“Dutch Safety Requirements for Nuclear Reactors:
Fundamental Safety Requirements”
19.3.2015

Contents

Scope of application

The "Dutch Safety Requirements for Nuclear Reactors" apply to facilities for the fission of nuclear fuels for the generation of electricity (nuclear power plants) and for research reactors. These requirements are applicable for stationary light water cooled nuclear reactors and apply to all lifetime phases of a nuclear reactor: site evaluation, design, construction, commissioning, operation, decommissioning, and dismantling. In principle the “Dutch Safety Requirements for Nuclear Reactors” were developed for licensing new build nuclear power plants and research reactors. Existing nuclear facilities shall apply these requirements as far as reasonable achievable with the objective to continuously improve nuclear safety.

Requirements are established for the structures, systems and components of nuclear reactors as well as for procedures important to safety, that are required to be met for safe operation and for preventing events that could compromise safety, or for mitigating the consequences of such events.

The technical requirements within this publication are substantiated by requirements on management and organisation established in another document. The “Dutch Safety Requirements for Nuclear Reactors” shall periodically come under scrutiny.

Annexes 1, 2, 3, and 4 contain supplementary requirements. Annex 1 provides postulated initiating events. Annex 2 describes the concept of protection against hazards and the corresponding provisions. The basic principles of the application of the single failure concept are provided in Annex 3, and Annex 4 contains supplementary requirements for the safety demonstration and documentation. Annex 6 describes the appropriate application to research reactors. The definitions of Annex 5 apply.

Requirements for items important to safety to be considered with regard to malevolent disruptive acts or other third party intervention are not dealt with in the “Dutch Safety Requirements for Nuclear Reactors”.

1 Fundamental objectives

The fundamental safety objective is to protect people and the environment from harmful effects of ionising radiation throughout the entire lifetime of a nuclear reactor: design, construction, commissioning, operation, decommissioning and dismantling.

Safety measures, security measures and measures for accounting for, and control of, nuclear material shall be designed and implemented in an integrated manner in such a way that they do not compromise one another.

2 Technical safety concept

2 (1) The radioactive materials present in the nuclear power plant shall be confined repeatedly by barriers and accordingly by retention functions (see Section 2.2) for compliance with the radiological safety objectives (s. Section 2.6). The radiation of the radioactive materials shall be sufficiently shielded. The effectiveness of barriers and retention functions shall be ensured by fulfilling the fundamental safety functions (see Section 2.3). A defence in depth safety concept shall be implemented that ensures the compliance of the fundamental safety functions and the protection of the barriers and retention functions on several consecutive levels of defence as well as in case of internal and external hazards (see Sections 2.1 and 2.5). The levels of defence in depth shall be independent as far as is practicable. The safety objectives for new power reactors recommended by the Western European Nuclear Regulators Association (WENRA) and presented in Table 2-1 are implemented in the technical safety concept, which is defined in the following subchapters.

Table 2-1 Technical safety concept

Levels of defence in depth	Associated plant condition categories	Objective	Essential means	Radiological consequences
Level 1	Normal operation	Prevention of abnormal operation and failures	Conservative design and high quality in construction and operation, control of main plant parameters inside defined limits	Regulatory operating limits for discharge
Level 2	Anticipated operational occurrences	Control of abnormal operation and failures	Control and limiting systems and other surveillance features	
Level 3[1]	Level 3.a Postulated single initiating events	Control of accident to limit radiological releases and prevent escalation to core melt conditions[2]	Reactor protection system, safety systems, accident procedures	No off-site radiological impact or only minor radiological impact
	Level 3.b Postulated multiple failure events		Additional safety features, accident procedures	
Level 4	Postulated core melt accidents (short and long term)	Control of accidents with core melt to limit off-site releases	Complementary safety features to mitigate core melt, Management of accidents with core melt (severe accidents)	Limited protective measures in area and time
Level 5	-	Mitigation of radiological consequences of significant releases of radioactive material	Off-site emergency response Intervention levels	Off-site radiological impact necessitating protective measures

According to "Position paper on the safety of new reactors in relation to safety objective O4", WENRA, RHWG, 03.02.2012

[1] Even though no new safety level of defence is suggested, a clear distinction between means and conditions for sub-levels 3.a and 3.b is lined out. The postulated multiple failure events are considered as a part of the Design Extension Conditions in IAEA Safety Standard No. SSR 2.1.

[2] Associated plant conditions being now considered at defence in depth level 3 are broader than those for existing reactors as they now include some of the accidents that were previously considered as "beyond design" (level 3.b). However, the associated acceptance criteria related to radiological consequences are the same as those required for postulated single initiating events for currently operating reactors. For level 3.b, analysis methods and boundary conditions, design and safety assessment rules may be defined according to a graded approach, also based on probabilistic insights. Best estimate methodology and less stringent rules than for level 3.a may be applied if appropriately justified.

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 emitted by these materials shall be ensured.

In order to achieve this objective, a safety concept shall be implemented in which inherent features, equipment and procedures are allocated to different levels of defence which are characterised by the following plant states:

- Level 1 of defence in depth: normal operation (normal operation)
- Level 2 of defence in depth: anticipated operational occurrences (abnormal operation)
- Level 3 of defence in depth:
  - Level 3a of defence in depth: postulated single initiating events
  - Level 3b of defence in depth: postulated multiple failure events
- Level 4 of defence in depth: postulated core melt accidents.

  Comprehensive and reliable protection against the radioactive materials within the plant shall be achieved by items important to safety and procedures to be installed on these levels of defence
- for quality assurance,
- the prevention of events,
- the control of events and core meltdown accidents as well as
- protection against internal and external hazards (see subsection 2.5).

2.1 (2) For accidents with core melt emergency measures shall be planned to support the disaster response forces 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 (level 5 of defence in depth).

2.1 (3a) Inherent features, equipment and procedures shall be provided which

at level 1 of defence in depth avert abnormal operation and failures,

at level 2 of defence in depth

a) control abnormal operation and failures,

b) avert escalation to accidents,

at level 3a of defence in depth

a) control postulated initiating events[3] to limit radiological releases,

b) prevent escalation to multiple failure events,

c) prevent escalation to core melt conditions,

at level 3b of defence in depth

a) control postulated multiple failure events[4] to limit radiological releases,

b) avert escalation to core melt conditions,

2.1 (3b) At level 4 of defence in depth, complementary safety features shall be provided

a) to practically eliminate situations that could lead to early or large releases of radioactive material,

b) to control accidents with core melt,

c) to achieve a long-term stable state.

2.1 (4) The defence in depth concept shall be implemented at the plant for all plant operational states of power operation as well as for low power and shutdown operation (see Annex 1, Section 4), with consideration of the respective representatively conservative plant state parameters.

[3] A list of postulating initiating events is provided in Annex 1

[4] A definition of multiple failure events is provided in Annex 5, a list of postulated multiple failure events is listed in Annex 1

2.1 (5a) The nuclear reactor shall be protected against hazards. Items important to safety shall be designed and located, considering other safety implications, to limit possible harmful consequences of their failures due to the hazards.

2.1 (5b) The design shall be such that items that are necessary to fulfil the fundamental safety functions are either capable of withstanding the effects of external events considered in the design or protected from such effects by other features such as passive barriers. At least the number of redundant trains and components to ensure the required degree of redundancy as specified in 3.1 (3) and 3.1 (4) shall be protected against external hazards.

2.1 (6) Independence between levels of defence in depth shall be implemented as far as practicable with a particular attention for levels 3 and 4 because of the enhanced severity of overall consequences if failures of these two levels occur simultaneously. –Inherent features and protection features shall be provided and arranged in a way that upon the failure of equipment at levels 1 and 2 of defence in depth the items important to safety and procedures on the subsequent level re-establish the required safety related condition independent of items important to safety and procedures of other levels of defence in depth.

All items important to safety that have to be effective at all or several levels of defence in depth shall be designed according to the requirements applying at the level of defence in depth with the respective most stringent safety requirements.

2.1 (7) The overriding safety related objective of the defence in depth concept is to ensure that a single technical failure or erroneous human action on one of the levels of defence will not jeopardise the effectiveness of the items important to safety on the next level.

2.1 (8) If using items important to safety and procedures provided at level 2 or 3a or 3b of defence in depth, to show that the requirements of previous levels of defence are met, it shall be demonstrated that

- other technical solutions are not reasonably achievable and

- adverse effects on the reliability and effectiveness of the items important to safety and procedures used for event control are excluded.

2.1 (9) The items important to safety and procedures at all four levels of defence in depth shall strictly be available in accordance with the respective operating phases. Any unavailability's of safety-relevant installations shall be restricted in time in dependence of the respective operating phases and their safety related consequences. The conditions to be fulfilled in this connection shall be specified.

2.1 (10) The reliability and quality of items important to safety shall be commensurate with their safety significance. The design of items important to safety shall be such as to ensure that the equipment can be qualified, procured, installed, commissioned, operated and maintained to be capable of withstanding, with sufficient reliability and effectiveness, all conditions specified in the design basis for the items.

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.

The design will prevent as far as practicable the failure of a barrier as a consequence of the failure of another barrier.

The barriers and retention functions shall be designed in such a way and maintained in such a condition over the entire plant operating lifetime that, in combination with the equipment and procedures of the respective levels of defence and the associated mechanical, thermal, chemical and radiation - induced impacts, the respective safety related acceptance targets and acceptance criteria (see Annex 1) as well as the radiological safety objectives according to Section 2.6 are met for all events or plant states on the different levels of defence.

The barriers and retention functions shall also be reliably effective in their entirety in all events resulting from internal and external hazards, so that the radiological safety objectives according to section 2.6 are met.

2.2 (2) If barriers are ineffective due to planned operational procedures, other equipment and procedures shall be available to achieve the radiological safety objectives (see subsection 2.6 (1)) which ensure an effective and reliable retention function according to the respective conditions.

2.2 (3) At levels 1 and 2 of defence in depth, 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,

2. the reactor coolant pressure boundary, unless the reactor coolant system is opened according to schedule, and

3. the containment, unless it is opened according to schedule. The opening of the containment according to schedule shall not be performed before reaching specified pressure and temperature conditions in the reactor coolant system. It shall be ensured that the barrier function of the containment is restored in due time to the necessary extent in the case of events with releases of radioactive materials within the containment. In case that this cannot be ensured, effective and reliable retention functions shall exist, so that an unacceptable release of radioactive materials from the containment is prevented or suppressed in due time.

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

1. during all operating phases (for definitions see Annex 1), the fuel rod cladding, as well as

2. the containment, unless it is opened according to schedule. If the containment is opened to schedule, it shall be ensured that the barrier function of the containment is restored in due time to the necessary extent in the case of events with releases of radioactive materials within the containment. In case that this cannot be ensured, effective and reliable retention functions shall exist, so that an unacceptable release of

radioactive materials from the containment is prevented or suppressed in due time.

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

2.2 (4) At level 3a and 3b of defence in depth, 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 is opened according to schedule or its failure is not postulated as initiating event,

3. the containment, unless it is opened according to schedule. If the containment is opened according to schedule, it shall be ensured that the barrier function of the containment is restored in due time to the necessary extent in the case of events with releases of radioactive materials within the containment. In case that this cannot be ensured, effective and reliable retention functions shall exist, so that an unacceptable release of radioactive materials from the containment is prevented or suppressed in due time.

b) for the handling and storage of fuel assemblies:

1. the fuel rod cladding, as well as

2. the containment, unless it is opened according to schedule. If the containment is opened according to schedule, 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 with releases of radioactive materials within the containment. In case that this cannot be ensured, effective and reliable retention functions shall exist, so that an unacceptable release of radioactive materials from the containment is prevented or suppressed in due time.

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

2.2 (5) At level 4 of defence in depth complementary safety features are provided to maintain the integrity of at least the containment for the confinement of radioactive materials. Core melt sequences involving containment failure and containment bypassing shall be practically eliminated. High pressure core melt situations must be prevented by design provisions. The design objective is to transfer high pressure core melt sequences to low pressure core melt sequences with a high reliability.

2.3 Concept of the fundamental safety functions

2.3 (1) By inherent features, equipment and procedures provided according to subsection 2.1 (3a) with consideration of the requirements of subsection 2.1 (5), the following fundamental safety functions (protection goals) 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) At levels 1 to 3b of defence in depth, the following requirements shall be fulfilled:

for reactivity control:

- reactivity changes shall be restricted to values that have been demonstrated as being admissible,
- it shall be possible to shut down the reactor core safely and keep it subcritical in the long term,
- upon the handling of fuel assemblies and in the storage for fresh fuel assemblies as well as in the spent fuel storage pool, subcriticality shall be ensured;

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 storage pool shall be ensured;

for the confinement of radioactive materials:

- the mechanical, thermal, chemical and radiation-induced impacts on the barriers and retention functions resulting on the different levels of defence shall be limited such that the effectiveness of the barriers and retention functions is maintained for the achievement of the radiological safety objectives according to Section 2.6.
- if the containment is opened according to schedule, 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 with releases of radioactive materials within the containment. In case that this cannot be ensured, effective and reliable retention functions shall exist, so that an unacceptable release of radioactive materials from the containment is prevented or suppressed in due time.

2.3 (3) At level 4 of defence in depth the integrity of at least the containment, to retain the radioactive materials and to reach a long-term controllable condition shall be maintained.

2.3 (4) At the design stage, special consideration shall be given to the incorporation of features that will facilitate the future waste management and decommissioning of the plant.

2.4 Evaluation of the site characteristics and potential effects of the nuclear reactor in the region

2.4 (1) A meteorological description of the region shall be developed, including descriptions of the basic meteorological parameters, regional orography and phenomena such as wind speed and direction, air temperature, precipitation, humidity, atmospheric stability parameters, and prolonged inversions.

2.4 (2) A programme for meteorological measurements shall be prepared and carried out at or near the site with the use of instrumentation capable of measuring and recording the main meteorological parameters at appropriate elevations and locations. Data from at least one full year shall be collected, together with any other relevant data that may be available from other sources. Relevant site specific data and data available from other sources shall be collected.

2.4 (3) On the basis of the data obtained from the investigation of the region, the atmospheric dispersion of radioactive material released shall be assessed with the use of appropriate models. These models shall include all significant site specific and regional topographic features and characteristics of the installation that may affect atmospheric dispersion.

2.4 (4) A description of the surface hydrological characteristics of the region shall be developed, including descriptions of the main characteristics of water bodies, both natural and artificial, the major structures for water control, the locations of water intake structures and information on water use in the region.

2.4 (5) A programme of investigation and measurements of the surface hydrology shall be carried out to determine to the extent necessary the dilution and dispersion characteristics for water bodies, the reconcentration ability of sediments and biota, and the determination of transfer mechanisms of radionuclides in the hydrosphere and of exposure pathways.

2.4 (6) An assessment of the potential impact of the contamination of surface water on the population shall be performed by using the collected data and information in a suitable model.

2.4 (7) A description of the groundwater hydrology of the region shall be developed, including descriptions of the main characteristics of the water bearing formations, their interaction with surface waters and data on the uses of groundwater in the region.

2.4 (8) A programme of hydrogeological investigations shall be carried out to permit the assessment of radionuclide movement in hydrogeological units.

This programme shall include investigations of the migration and retention characteristics of the soils, the dilution and dispersion characteristics of the aquifers, and the physical and physicochemical properties of underground materials, mainly related to transfer mechanisms of radionuclides in groundwater and their exposure pathways.

2.4 (9) An assessment of the potential impact of the contamination of groundwater on the population shall be performed by using the data and information collected in a suitable model.

2.4 (10) The distribution of the population within the region shall be determined.

2.4 (11) Information on existing and projected population distributions in the region, including resident populations and to the extent possible transient populations, shall be collected and kept up to date over the lifetime of the installation. The radius within which data are to be collected shall be chosen on the basis of national practices, with account taken of special situations. Special attention shall be paid to the population living in the immediate vicinity of the installation, to densely populated areas and population centres in the region, and to residential institutions such as schools, hospitals and prisons.

2.4 (12) Before commissioning of the nuclear installation the ambient radioactivity of the atmosphere, hydrosphere, lithosphere and biota in the region shall be assessed so as to be able to determine the effects of the nuclear reactor on radioactivity in the environment. The data obtained are intended for use as a baseline in future investigations.

2.4 (13) The total nuclear capacity to be installed on the site shall be determined as far as possible at the first stages of the siting process. If the installed nuclear capacity is significantly increased to a level greater than that previously determined to be acceptable, the suitability of the site shall be re-evaluated, as appropriate. For assessing the feasibility of the implementation of the emergency plans, all nuclear installations to be installed on the site shall be considered.

2.5 Concept of protection against internal and external hazards

2.5 (1) All items required for the safe shutdown of the nuclear reactor, for maintaining it in a shutdown state, for residual heat removal or the prevention of a release of radioactive materials shall be designed such and constantly kept in such a condition that they can fulfil their safety related tasks even in case of any internal hazard or relevant site specific external hazards (see Annex 2).

A site specific hazard analysis shall be performed to develop a hazard curve for each external hazard.

Specific requirements regarding compliance with radiological safety objectives are given in Annex 2.

2.5 (2) The different redundant sub-systems of systems important to safety shall be installed in physically separated plant areas or shall be protected such that in case of any internal hazard (such as fire or flooding) a failure of more than one redundant train will be reliably prevented.

2.5 (3) If due to the site characteristics no appropriate protection measures against the relevant external hazards can be developed (e. g. in case of a capable fault underneath the site), the site shall be deemed unsuitable or no longer suitable.

2.6 Radiological safety objectives

2.6 (1) At levels 1 of defence in depth (normal operation),

- radiation exposure of the personnel shall be kept as low as reasonably achievable for all activities, below the limits for normal circumstances as specified in the Radiation Protection Decree[5], taking into account all circumstances of individual cases,
- any radiation exposure or contamination of man and the environment by direct radiation from the plant as well as by the licensed discharge of radioactive materials shall be kept as low as reasonably achievable, taking into account all circumstances of individual cases,
- any licensed discharge of radioactive materials in air or water under normal circumstances shall be controlled via the therefore intended release paths; the releases shall be monitored as well as documented and specified according to their kind and activity.

At levels 2 and 3 of defence in depth (abnormal events and prevention of accidents; accidents without core melt

- there is no off-site radiological impact or only minor radiological impact,
- the maximum radiation exposure of personnel in connection with the planning of activities for the control of events, the mitigation of their effects, or the elimination of their consequences, shall be kept as low as reasonably achievable and shall not exceed the relevant limits for normal circumstances as specified in the Radiation Protection Decree[6], taking into account all circumstances of individual cases,
- any release shall only happen via the therefore intended release paths; the release shall be kept as low as reasonably achievable and shall not exceed the following limits for the public taking into account all circumstances of individual cases.:

[5] In Dutch: Besluit stralingsbescherming

Event frequency per year	Maximum allowable effective dose (over 70 years)
$F \geq 10^{-2}$	0,1 mSv
$10^{-2} > F \geq 10^{-3}$	1 mSv
$F < 10^{-3}$	10 mSv

- The release shall be monitored and documented and specified according to its kind and activity.

At level 4 of defence in depth, accidents with core melt

- The total probability of occurrence of accidents with core melts shall be as low as reasonably achievable, but shall not exceed 10^{-6} per year.
- accidents with core melt which would lead to early or large releases shall be practically eliminated,
- for accidents with core melt that cannot be practically eliminated only limited protective measures in area and time shall be needed for the public (no need for emergency evacuation outside the immediate vicinity of the plant, limited sheltering, no permanent relocation, no long term restrictions in food consumption) and sufficient time is available to implement these measures,
- the maximum radiation exposure of personnel in connection with the planning of activities for the control of postulated core melt accidents, the mitigation of their effects, or the elimination of their consequences, shall be kept as low as reasonably achievable and do not exceed the limits for intervention as is specified by the EURATOM when implementing ICRP103, taking into account all circumstances of individual cases,
- any release of radioactive materials from the plant shall be monitored and documented and specified according to their kind and activity.

The probability of occurrence that a person, located permanently and unprotected outside the facility, dies as a result of accident, shall not exceed 10-6 per year.

The probability of occurrence that a group of at least 10 persons would directly die as a result from an accident shall not exceed 10^{-5} per year, or for n times more fatalities a probability which is n^2 times smaller.

2.6 (2) All items important for safety 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, that they fulfil the safety related functions for meeting the requirements according to subsection 2.5 (1).

All structures, systems and components 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 limits for personnel for all necessary activities on levels of defence 1 and 2 and for the planning of activities for the control of events, the mitigation of their effects, or the elimination of their consequences, on levels of defence 3 and 4.

3 Technical requirements

3.1 Overall requirements

3.1 (1) In the design, manufacturing, construction and tests as well as during the operation and maintenance of the items important to safety, principles and procedures shall be applied to comply with the specific safety related requirements of nuclear technology. Upon the application of sound 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 case of application.

3.1 (2) Safety-enhancing design, manufacturing and operating principles shall be applied to the equipment and procedures at levels 1 to 3b of defence in depth with regard to all operating phases. In particular, the following shall be implemented:

a) safety margins in the design of components shall be justified according to the safety significance; here, established rules and standards may be applied with regard to the case of application;

b) preference of inherently safe acting mechanisms during design;

c) use of qualified materials and manufacturing and testing methods;

d) use of equipment that have been proven by operating experience or which have been sufficiently tested;

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

f) the ergonomic design of work places. The possibility of human error shall be taken into account in the design of the nuclear power plant and in the planning of its operation and maintenance. Human error or deviations from normal plant operation due to human error shall not endanger plant safety;

g) to ensure and maintain the quality features during manufacturing, construction and operation;

h) performance of regular in-service inspections to an extent that is necessary from a safety related of view;

i) reliable monitoring of the relevant operating conditions in the respective operating phases,

j) preparation of a monitoring concept with monitoring systems to detect and control service- and ageing-induced damage;

k) recording, evaluation and safety related use of the operating experience.

3.1 (3) In addition to subsection 3.1 (2), the following design principles shall be applied to the safety systems at level 3a of defence in depth to ensure sufficient reliability:

a) redundancy (degree of redundancy (n+2));

b) diversity;

c) segregation of redundant subsystems, unless it is conflicting with safety benefits;

d) physical separation of redundant subsystems;

e) safety-oriented system behaviour upon subsystem or plant component malfunctions (application of the fail-safe principle);

f) preference of passive over active safety systems;

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

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

3.1 (4) In addition to subsection 3.1 (2), the following design principles shall be applied to the additional safety features (level 3b of defence in depth) and complementary safety features (level 4 of defence in depth):

a) active parts of items important to safety at levels 3b or 4 of defence in depth shall be redundantly available (n+1);

b) physical separation of redundant subsystems;

c) for items performing safety functions a back-up on-site electrical supply shall be provided;

d) automation of the functions shall be provided in case of postulated multiples failure events if there is no sufficient time for manual actuation;

e) the operability of the items important to safety is ensured by maintenance and in-service inspections with respect to its reliability data.

3.1 (5)

All items important to safety shall be classified according to their safety significance. The requirements 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 environmental and effectiveness conditions, emergency power supply and long-term maintenance of quality.

Of highest safety significance and accordingly classified shall be:

a) items important to safety whose failure leads to event sequences that cannot be controlled,

b) safety systems (level 3a of defence in depth) that are necessary for effective and reliable accident control of postulated single initiating events, including the auxiliary and supply systems required for it and

Of less safety significance and accordingly classified shall be:

a) items important to safety of Level of defence 2 that are necessary to effectively and reliably avert accident escalation, including the auxiliary and supply systems required for it,

b) additional safety features (level 3b of defence in depth) that are necessary to control postulated multiple failure events

c) complementary safety features (level 4 of defence in depth) to control accidents with core melt

d) items important to safety for compliance with and monitoring of defined radiological limits, particularly by maintaining the required effectiveness of barriers and retention functions,

e) other items important to safety

The design shall take due account of the fact that the existence of multiple levels of defence is not a basis for continued operation in the absence of one level of defence. All levels of defence in depth shall be kept available at all times, and any relaxations shall be justified for specific modes of operation.

3.1 (6) A qualification programme for items important to safety shall be implemented to verify that items important to safety at a nuclear power plant are capable of performing their intended functions when necessary, and in the prevailing environmental conditions, throughout their design life, with due account taken of plant conditions during maintenance and testing.

a) The environmental conditions considered in the qualification programme for items important to safety at a nuclear power plant shall include the variations in ambient environmental conditions that are anticipated in the design basis for the plant.

b) The qualification programme for items important to safety shall include the consideration of ageing effects caused by environmental factors (such as conditions of vibration, irradiation, humidity or temperature) over the expected service life of the items important to safety. When the items important to safety are subject to natural external events and are required to perform a safety function during or following such an event, the qualification programme shall replicate as far as is practicable the conditions imposed on the items important to safety by the natural event, either by test or by analysis or by a combination of both.

c) Any environmental conditions that could reasonably be anticipated and that could arise in specific operational states, such as in periodic testing of the containment leak rate, shall be included in the qualification programme.

3.1 (7) The potentials for common-cause failures of items important to safety shall be analysed. Measures to reduce the incident probability of such failures shall be implemented, that with a high level of confidence multiple failure of items important to safety at level 3a of defence in depth does not have to be assumed. Thus, safety systems for which potentials for common-cause failures were identified shall be designed according to the principle of diversity as far as feasible and technically reasonable.

3.1 (8) The reliability and effectiveness of the safety functions at level 3a of defence in depth, including the safety system support features, shall be ensured by safety systems and procedures

- under all conditions to be assumed for the event sequences,
- in the case of event-induced consequential failures,
- in case of simultaneous or time-lag failure of the house load supply, and
- in the case of failures or unavailability according to the single-failure approach, see Annex 3.

3.1 (9) Safety systems to control postulated single initiating events at level 3a of defence in depth are redundantly designed in such a way that the safety functions are also sufficiently effective if it is postulated that, in the event of their required function,

- a failure of an item important to safety due to single failure with the most unfavourable effects occurs, and
- at the same time an item important to safety is in general assumed to be unavailable due to maintenance case with the most unfavourable effects in combination with a single failure.

Note: Detailed requirements for the application of the single failure concept are provided in Annex 3.

3.1 (10) In operating phases in which parts of the safety systems are scheduled to be unavailable according to the operating manual, reliable and effective control shall be ensured under these conditions for the events to be assumed in these phases.

3.1 (11) In case of external hazards, autarchy of the related emergency systems shall be ensured for at least 10 hours with respect to all cooling and operating agents necessary to take the plant to a controlled condition and maintain it in this condition.

3.1 (12) All items important to safety 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. Inspections and maintenance shall be possible 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 items important to safety shall be checked to the required extent under conditions that correspond to the case of demand as far as possible.

3.1 (12a) If for certain structures, systems and components 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. This shall be done in such a way, that during operation and in accordance with the state of the art in science and technology no safety relevant damages have to be assumed and that a documentation of the supplier is available from which no abnormality or deviation can be derived with respect to the specifications to be fulfilled.

3.1 (12b) Appropriate margins shall be provided in the design to take account of relevant ageing effects and potential ageing related degradation. Ageing effects

shall be taken into account for all operational states, including periods of maintenance and shutdown.

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

3.1 (13) Requirements for the design of the work environment, work equipment and content of work

a) In order to provide the prerequisites for required performance of personnel working at the plant all foreseen safety relevant tasks at levels 1 to 4 of defence in depth shall be designed in accordance with accepted Human Factors Engineering principles. The conditions of internal and external hazards shall be considered.

b) The requirement according to subsection 3.1 (13) a) shall be applied to the design of all work places where these tasks are performed, to all work equipment provided, and to the routes used by the personnel to reach the work place with all necessary work equipment.

Note: The work equipment comprises, among others: information sources, operating equipment and communication means, measuring and test equipment, tools and other work aids, means of transport, lifting equipment and attachment devices as well as documents with instructions and other information on activities to be performed.

c) While implementing the requirements according to subsection 3.1 (13) a) all impacts on those persons performing tasks at their work places and on the routes to their work places shall be taken into account. This comprises, among others, radiation exposure, room climate, illumination and exposure to sonic noise.

d) The requirement according to subsection 3.1 (13) a) shall be applied to the design of all work processes, the task distribution between man and technology and the task allocation to different task performers.

3.1 (14) In case of multiple unit sites, each unit shall have its own items important to safety to control and mitigate the anticipated operational occurrences and accidents considered for the design.

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

3.2 (1) The control of reactivity in the reactor core shall be ensured for normal operation, anticipated operational occurrences, postulated single initiating events, postulated multiple failure events as well as in the case of internal and external hazards.

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

- at level 1 of defence in depth the design limits, and
- at levels 2 to 3b of defence in depth the respective applicable safety related acceptance targets and acceptance criteria

are met.

3.2 (3) The reactor core shall be designed such that due to inherent reactor-physical feedback characteristics of the core 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 shutdown systems the applicable safety related acceptance targets and acceptance criteria are met on the respective levels of defence.

3.2 (4) The fuel elements, fuel assemblies and support structures shall be designed so that in normal operation, anticipated operational occurrences, postulated single initiating events and postulated multiple failure events a geometry is maintained, that allow for adequate cooling and does not impede the insertion of control rods.

3.2 (5) The reactor core shall be designed such that due to inherent reactor-physical feedback characteristics of the core anticipated transients without scram with postulated failure of the fast-acting shutdown system (reactor scram system) are controlled and that in combination with other measures and installations of the plant, being effective as specified, the safety related acceptance targets and acceptance criteria applicable for this event are met.

3.2 (6) The reactor shall have

- at least one system for fast shutdown (reactor scram system) by means of reactivity control devices, and
- at least one more shutdown system, being independent of it and diverse, for reaching and long-term maintenance of sub-criticality. For nuclear power plants systems to inject soluble neutron absorbers into the reactor coolant shall be implemented.

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

3.2 (7) Distributions of neutron flux that can arise in any state of the reactor core, including states arising after shutdown and during or after refuelling, and states arising from anticipated operational occurrences, postulated single initiating events and postulated multiple failure events shall be inherently stable. The demands made on the control system for maintaining the shapes, levels and stability of the neutron flux within specified design limits in all operational states shall be minimized.

3.2 (8) In the design of reactivity control devices, due account shall be taken of wear out and of the effects of irradiation, such as burnup, changes in physical properties and production of gas

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

- from each condition at levels 1 to 3b of defence in depth, even if it is postulated that the most reactivity-effective control rod assembly is ineffective, and
- in case of internal and external hazards

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

In case of postulated single initiating events and postulated multiple failure events, the postulated failure of the most reactivity effective control rod assembly may be treated as single failure according to subsection 3.1 (8) with regard to the sub-criticality to be maintained.

3.2 (10) It shall be possible to shut-down the reactor and to maintain a safe state at levels 1 to 3b of defence in depth as well as in the case of internal and external hazard conditions, even at the temperature, xenon concentration and the point in time of the cycle leading to the most unfavourable reactivity balance that is possible for the conditions and events to be considered.

For pressurized water reactors the systems for injecting soluble neutron absorbers into the coolant alone shall be able to provide the required amount of sub-criticality for the conditions and associated events at levels 1 to 3b of defence in depth as well as in the case of internal and external hazards.

For boiling water reactors each of the following items important to safety alone shall be able to provide the required amount of sub-criticality:

- Insertion of the control elements driven by electro motors in case of events at levels 1 to 3b of defence in depth as well as in case of internal and external hazards.
- In case of events at levels 1 and 2 of defence in depth the injection of soluble neutron absorbers into the coolant.

Note: In case long-term maintenance of sub-criticality at levels 1 to 3 of defence in depth is ensured by the control rods alone, failure of the most effective control rod is postulated. At level 3 of defence in depth, this may be treated as single failure according to subsection 3.1 (8).

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

3.3 (1) Fuel cooling (heat removal from the reactor core) shall be ensured for normal operation, anticipated operational occurrences, postulated single initiating events and postulated multiple failure events as well as in the case of internal and external hazards.

For this purpose, the heat produced in the fuel element shall be removed such that the safety related acceptance targets and acceptance criteria for the fuel assemblies and the other items important to safety applicable on the respective levels of defence are met during their entire operating life.

3.3 (2) Structures, systems and components shall be available by means of which during normal operation and anticipated operational occurrences

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

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

c) the inventory, temperature and pressure of the reactor coolant can be controlled to ensure that specified design limits are not exceeded, with due account taken of volumetric changes and leakage, and

d) adequate facilities shall be provided to clean up the reactor coolant by removing non-radioactive and radioactive substances, including activated corrosion products and fission products derived from the fuel.

3.3 (3) A reliable and redundant safety system for emergency core cooling (emergency core cooling system) in case of a loss-of-coolant accident shall be provided that ensures for the break sizes, break locations, operating conditions and accident-induced impacts on 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 (9),

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 safety system for reactor shutdown and residual-heat removal in case of accidents without loss of coolant 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 (9).

3.3 (5) Safety systems ensuring residual-heat removal shall be designed in such a way, that the 72 h self-sufficiency criterion is met. All necessary materials and supplies shall be available at the nuclear power plant and shall be protected against internal and external hazards.

3.3 (6) A diverse ultimate heat sink shall ensure residual heat removal for all operating conditions in case of an unavailability of the ultimate heat sink due to failures of the cooling water intake or discharge. If necessary efficient cooling capabilities shall be ensured by a combination of various heat sinks. The necessary items important to safety shall fulfil at least the requirements at level 3b of defence in depth. The effectiveness shall be demonstrated.
The availability of the diverse ultimate heat sink shall be ensured also in case of site specific external hazards.

3.4 Requirements for the reactor coolant pressure boundary and the pressure and activity retaining components of systems outside the reactor coolant pressure boundary (“external systems”)

3.4 (1) The reactor coolant pressure boundary shall be designed, arranged and operated such that the occurrence of rapidly propagating cracks and brittle fracture shall be practically eliminated.

3.4 (2) For this purpose, in the design an adequate safety margin shall be added to the determined values of impact according to the requirements of subsection 3.1 (2) to ensure that the design conditions of the reactor coolant pressure boundary are not exceeded.

3.4 (3) For the reactor coolant pressure boundary and the pressure-retaining walls of components of external systems with nominal diameter larger than

DN[6] 50, basic safety shall be ensured by fulfilment fulfilling the following requirements considering also the operating medium:

- use of high-quality materials, in particular with regard to ductility and corrosion resistance,
- conservative limitation of stresses,
- prevention of stress peaks by optimised design and construction, and
- application of optimised manufacturing and testing technologies.

This includes the awareness and assessment of possibly existing defects.

To ensure and assess the required quality of those components in operation a concept shall be arranged to maintain the integrity. Measures shall be defined and implemented to monitor possible causes and consequences of degradation mechanisms, in particular of leakages during operation.

3.4 (4) For the reactor coolant pressure boundary and the pressure-retaining walls of components of external systems, leak and break postulates shall be defined within the framework of the design concept on level of defence 3a. For piping systems and components of these systems for which catastrophic failure during plant operation can be safely prevented, these failures do not have to be postulated in the design concept, and limited leak and break sizes may be assumed in the safety analyses. A high level of confidence shall be ensured regarding the impacts on these components and piping systems at levels 1 to 3b of defence in depth as well as in the case of internal and external hazards.

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

3.4 (5a) Effective and reliable structures, systems and components for pressure limitation and overpressure protection shall be provided to prevent

[6] DN: *D*iameter *N*ominal, for definition see Annex 5

exceeding the admissible pressure in the reactor coolant pressure boundary (for pressurized water reactors including secondary side of steam generator).

Reliable opening and closure of the items important to safety for overpressure protection shall be assured under the conditions of anticipated operational occurrences, postulated single initiating events and postulated multiple failure events as well as in the case of internal and external hazard.

3.4 (5b) Structures, systems and components with a high degree of reliability for effective depressurisation of the reactor coolant system shall be provided to practically eliminate high pressure core melt scenarios.

3.4 (6) The nuclear power plant shall be operated such that the respective permissible values for impacts on the reactor coolant pressure boundary are not exceeded at levels 1 to 3b of defence in depth nor in the case of internal and external hazards. Here, the safety margins 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 of the external systems shall be arranged and installed such that, in case of postulated single initiating events and postulated multiple failure events initiated by failure of these components as well as in case of internal and external hazards, no consequential damages at other items important to safety can occur which may endanger the fulfilment of the safety function of these components.

3.5 Requirements for buildings

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

- ensuring load transfer of the systems and components during operation and in the event of accidents and / or internal or external hazards,
- ensuring protection against these hazards (see Annex 2),
- shielding of the ionising radiation and retention of radioactive materials,

commensurate to the safety classification of the structures, systems, and components located in the building.

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 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 radiological safety objectives specified for levels 1 to 4 of defence in depth are not exceeded (see subsection 2.6 (1)).

The containment shall fulfil its safety function in operating phases during which the containment is closed according to schedule under the conditions at levels 1 to 4 of defence in depth as well as in case of internal and external hazards.

In operating phases during which the containment may be open according to schedule, it shall be ensured that under the conditions of normal operation, anticipated operational occurrences, postulated single initiating events and postulated multiple failure events as well as in case of internal and external hazard, 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 located within a containment system unless an inadmissible release of radioactive materials into the environment can be prevented otherwise in a sufficiently reliable manner.

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

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 operating phases in which the containment is closed.

The containment and the systems and components affecting the leak-tightness of the containment system shall be designed and constructed in such a way, that the leak rate can be tested after all penetrations through the containment have been installed and during the operating lifetime of the plant. The leak rate shall be tested at the design pressure of the containment.

3.6 (4) To limit the number of leak paths, the number of penetrations should be kept as low as possible. The external extensions of the penetrations should be installed in a confined structure, at least until the first isolation valve, in order to collect and filter any leaks before a radioactive release occurs. Penetrations shall ensure structural integrity and leaktightness.

3.6 (5) The building surrounding the containment

- 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 considered for the plant.

3.6 (6a) The containment shall be protected by structural decoupling such that its stability is also maintained in case of human induced hazard conditions.

3.6 (6b) The support stability or integrity of internals and rooms shall be maintained as far as necessary in case of postulated single initiating events and postulated multiple failure events, including the effect of pressure differences.

3.6 (7) In case of postulated single initiating events and postulated multiple failure events, a long-term temperature or pressure increase in the containment shall be prevented.

3.6 (8) For postulated core melt accidents the following requirements apply:

- A long-term temperature or pressure increase in the containment shall be prevented by an effective and redundant system for removing the residual heat from the containment building. A filtered venting system shall be included in the design. The safety margins shall be such that filtered venting shall not be needed in the early phases of the core melt accident. In case of filtered venting the radiological safety objectives shall be fulfilled. It shall be ensured that no failure of the containment due to negative pressure occurs as a result of the filtered venting.

- Combustion processes of gases endangering the containment / building integrity shall be prevented by complementary safety features. All sources of combustible gas generation shall be taken into account in a representative manner.

- If severe fuel assembly damages in the spent fuel storage pool cannot be practically eliminated, combustion processes of gases endangering the integrity of the containment or the surrounding building shall be prevented by complementary safety features.

3.6 (9) For boiling water reactors impermissible leaks between drywell and wetwell, in particular during restart of the plant and after maintenance measures, shall be prevented. The containment, consisting of drywell and wetwell is designed such that the function of the wetwell regarding pressure suppression and relief is ensured without consideration of the suppression pool spray system. The tight sealing between drywell and wetwell is ensured.

3.6 (10) Coverings, thermal insulations and coatings for components and structures within the containment system shall be carefully selected and methods for their application shall be specified to ensure the fulfilment of their safety functions and to minimize interference with other safety functions in the event of deterioration of the coverings, thermal insulations and coatings.

3.6 (11) Airlocks are provided for introducing and removing materials and objects into or out of the containment as well as for entry and exit of persons.

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

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

Interlocks shall ensure that in the operating phases in which the locks shall be closed a hatch can only be opened when

- the other hatch is closed and sealed and
- pressure equalisation is finished.

Disengagement of the interlock is only permissible under conditions permissible from the safety point of view.

3.6 (12) Loops that are closed either inside or outside the containment envelope shall have at least one isolation valve outside the containment envelope at each penetration. Each containment isolation valve as such fully complies with the specified tightness conditions.

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

3.7 Requirements for instrumentation and control system (I&C)

3.7 (1) Instrumentation shall be provided for determining the values of all the main variables that can affect the fission process, the integrity of the reactor core, the reactor coolant systems and the containment at the nuclear power plant, for obtaining essential information on the plant that is necessary for its safe and reliable operation, for determining the status of the plant in accident conditions and for making decisions for the purposes of accident management.

3.7 (2) Appropriate and reliable control systems shall be provided at the nuclear power plant to maintain and limit the relevant process variables within the specified operating limits and conditions.

3.7 (3) Instrumentation and control equipment and systems with functions at level 1 of defence in depth shall be provided. These instrumentation and control equipment and systems shall be designed and operated in such a way that a stable operation of the plant is ensured without actuating instrumentation and control functions at level 2 of defence in depth.

3.7 (4) The nuclear power plant shall be equipped with instrumentation and control system with functions at level 2 of defence in depth that are suitable for avoiding an actuation of the protective actions at level 3a of defence in depth in case of anticipated operational occurrences.

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

The reactor protection system shall be designed according to the following principles:

- redundant design of components, subassemblies and subsystems,
- diversity,
- physical separation under consideration of the area of probable impacts of postulated initiating events,
- self-acting monitoring of the failures,
- adaptation of the components to the possible ambient conditions,
- software with an as simple as possible, traceable and testable structure,
- limitation of the functional scope of hardware and software to the necessary safety related extent, and

– use of fault-preventing, fault-detecting and fault-controlling measures and installations.

In the case that computer-based or programmable logic device (PLD) based reactor protection systems are applied for functions at level 3a of defence in depth, it shall be demonstrated for the entire life cycle that any manipulation of these systems are excluded by design or security measures.

3.7 (6) The reactor protection system of the nuclear power plant shall be designed

– to be capable of overriding unsafe actions of the control system and

– with fail-safe characteristics to achieve safe plant conditions in the event of failure of the reactor protection system.

The design

– shall prevent operator actions that could compromise the effectiveness of the reactor protection system in operational states and in accident conditions, but not counteract correct operator actions in accident conditions;

– shall automate various safety actions to actuate safety systems so that operator action is not necessary within a justified period of time from the onset of anticipated operational occurrences or accident conditions;

- shall make relevant information available to the operator for monitoring the effects of automatic actions.

3.7 (7) In the design of the instrumentation and control system fulfilling safety functions according to 3.7 (5) the potentials and effects of systematic failures of instrumentation and control systems on postulated single initiating events shall be analysed taking process engineering based requirements into account.

Provisions shall be made to minimise the incident probability of systematic failures in such a way, that with a high level of confidence its occurrence must not be postulated at level 3a of defence in depth.

3.7 (8) The results of the individual software development phases are fully verified by application of formal analysis methods and additional tests whether these requirements are fulfilled. For this purpose, tests are carried out at defined milestones. Following the installation of the software on the computers, the required behaviour of the hardware and software systems is validated. If validation is performed in several steps, the individual validation steps are designed to be overlapping. Verification and validation processes shall be carried out by teams independent of the designers and developers.

3.7 (9) Manual reactor scram shall be possible at any time during operating phases in which the availability of the reactor scram system is required, even in case of postulated systematic failure of software-based instrumentation and control including systematic software failure. Instrumentation and control systems dedicated for the manual actuation of safety functions shall be independently set up from automatic instrumentation and control systems.

3.7 (10) The instrumentation and control system (reactor protection system) according to 3.7 (5) shall be designed in such a way that even if the single failure to be postulated occurs in these installations, no actions will be triggered that could take the reactor to accident conditions or could have negative effects on the accident control.

3.7 (11) Monitoring and alarm installations shall be available at the nuclear power plant which at levels 1 and 2 of defence in depth allow at any time a sufficient overview of the safety related operating condition of the plant and the developing relevant processes and which are able to display and record all safety-relevant operating parameters. Control room alarms shall be clearly prioritized. The number of alarms, including alarm messages from process computers, shall be minimized for any analysed operational state, outage or accident condition of the plant.

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

3.7 (12) Specific accident instrumentation shall be available at the nuclear power plant for postulated single initiating events, postulated multiple failure events and postulated core melt accidents which

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) provides indications on the event sequence and allows its proper documentation,

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

d) is supplied with uninterrupted emergency power supply for at least 10 hours (even in case of a failure of the electrical power supply not backed-up by batteries),

e) performs redundant signal processing,

f) whose items for recording the necessary information are diverse and accident-proof, and

g) is protected against internal and external hazards.

3.7 (13) The functions to be performed by the instrumentation and control system shall be classified by their safety-significance according to subsection 3.1 (5). 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 sub-systems) of the instrumentation and control system shall be defined according to their safety related classification.

3.7 (14) Additional safety features (at level 3b of defence in depth) and complementary safety features (at level 4 of defence depth) may have priority over concurring actions at levels 1 to 3a of defence in depth. Manual interaction in systems at levels 1 to 3a of defence in depth is permitted if required for additional safety features (at level 3b of defence in depth) and complementary safety features (at level 4 of defence in depth).

3.7 (15) Unauthorised access to information systems and instrumentation and control systems (I&C) 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 and emergency response facilities

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

3.8 (2) A supplementary control room shall be provided outside the control room from where in case of an unavailability of the control 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 (3a) An on-site technical support centre, separate from both the plant control room and the supplementary control room, shall be provided and suitably equipped from which technical support can be provided to the control room operational personnel during accident conditions.

3.8 (3b) An emergency centre shall be provided and suitably equipped from which on-site emergency response as well as the interface to external response forces can be managed.

3.8 (3c) The emergency response facilities[7] mentioned in 3.8 (3a) (technical support centre) and 3.8 (3b) (emergency centre) shall operate as an integrated system in support of the control room / supplementary control room, without interfering in each other's functions.

Information on

- important plant parameters,
- radiological conditions on-site and
- radiological conditions in the immediate surroundings,

[7] Such emergency response facilities (technical support centre and emergency centre) may be colocated (i.e. these functions may be performed from a single emergency response facility or location) as long as it is ensured that they do not interfere with each other in performing their specified functions and that they are separated from the control rooms.

shall be available and

- means of communication with the control room, supplementary control room and other important locations on the plant site and
- means of communications with on-site and off-site emergency response organizations

shall be provided.

3.8 (4) The habitability and good condition of the control room, supplementary control room, technical support centre and emergency centre shall be maintained. Where the design of the plant foresees additional or local control rooms that are dedicated to the control of processes that could affect plant conditions, clear communication lines shall be developed for ensuring an adequate transfer of information to the operators in the main control room / supplementary control room.

3.8 (5) The control room and the supplementary control room shall be physically separated, independently power-supplied and protected against external hazards in such a manner that they cannot be disabled at the same time.

3.8 (6) The control room and the supplementary control room shall be designed under ergonomic aspects to establish the preconditions for the safety oriented behaviour of the personnel.

3.8 (7) The control room, supplementary control room, technical support centre and emergency centre shall remain operable, accessible and habitable for a protracted period of time in situations generated by accidents and conditions due to or resulting from hazards considered in the design of the plant.

3.8 (8) Appropriate alarm systems and communication systems shall be available so that all persons present at the nuclear power plant and on the site can be given warnings and instructions from at least one central point.

3.8 (9) For the on-site communication and the communication with off-site agencies technically appropriate and diverse systems shall be provided. These communication systems shall be functional in case of postulated multiple

failure events and postulated core melt accidents and under conditions due to or resulting from external hazards.

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, which execute safety functions, is ensured in compliance with their power supply conditions for all plant states as well as in case of internal and external hazards. The electrical power supply shall be designed of such reliability in order not to affect the unavailability of the supplied systems, whose failure can lead to adverse safety related effects.

3.9 (2) For this purpose, a minimum of two independent (offsite) electrical power sources shall be available. At least one of these power sources is a connection to the grid. The second power source is able to carry the same load as the grid connection. If there are two or more grid connections, these shall be functionally separated from each other and decoupled by protective circuits.

In case of an unavailability of the main grid connection the nuclear power plant shall be designed to switch to house load operation by utilizing the main generator ("load rejection to house load operation"). The plant shall have the capability to withstand this load rejection without undergoing a reactor trip or a main generator trip. For the separation of the nuclear power plant from the main grid and for the reduction of the reactor power equipment and automatic measures shall be implemented.

In case of an unavailability of the grid connection, the second (offsite) electrical power source and the main generator as well as in case of internal and external hazards reliable emergency power supply facilities shall be available ensuring the electrical power supply of items important to safety. Sufficient operating supplies supporting these emergency power supply facilities for at least 72 hours (72 h self-sufficiency criterion) shall be provided at the plant.

3.9 (3) Ensuring electrical power supply in case of a simultaneous failure of the offsite power supply, the main generator and the emergency power supply

facilities an alternate emergency power supply shall be provided. This alternate emergency power supply shall be independent, physically separated and diverse in design from the electrical power supply options of subsection 3.9 (2).

3.9 (4) The functionality of items important to safety at the nuclear power plant shall not be compromised by disturbances in the external grids, including anticipated variations in the voltage and frequency of the grid supplies.

3.9 (5) In the design of components, which contain electrical, electromechanical or electromagnetic component parts or analogue-electric subassemblies with a simple structure, the potential for systematic failures of these components shall be analysed. Provisions shall be taken to reduce the probability of occurrence of systematic failures in a way that a systematic failure no longer has to be postulated or else that its effects can be controlled.

In the design of components, which contain complex electronic subassemblies (programmable or non-programmable), fault-preventing and fault-controlling provision shall be taken on component level as well as if applicable fault-controlling provisions on system level, so that common cause failures on system-level in more than one redundancy are practically eliminated.

Note: "Simple" means, that the function as well as the failure behaviour of the components can be deterministically determined based on general electrical engineering judgement.
"Complex" means, that the function as well as the failure behaviour of the components cannot be deterministically determined based on general electrical engineering judgement.

3.9 (6) The necessary electrical power supply for the additional safety features (at level 3b of defence in depth) and the complementary safety features (at level 4 of defence in depth) shall be ensured for a period of 10 hours without any external support.

The restoration (e.g. switch-back of the main or standby grid, restart of the emergency diesel generators or connection of another electrical power supply option) of the electrical power supply shall be ensured after the electrical power supply, not provided by the batteries, has failed.

For long-term back-up of the electrical power supply, compensating measures ensuring electrical power supply after 72 hours, shall be provided. The associated necessary equipment within the plant site or in the immediate vicinity of the plant shall be protected against external hazards. For this equipement a minimum of two adequate external connections shall be provided.

The provided electrical power shall be sufficient to remove the residual heat in the particular operating state with the available items important to safety and to prevent unacceptable release of radioactive material.

3.9 (7) The emergency power supply facilities shall be constructed redundantly, physically separated, generally without structural interconnections, functionally independent of each other and protected from each other avoiding that any failure in an emergency power supply facility will lead to a loss of several redundancies of these emergency power supply facilities. The degree of redundancy of the emergency power supply facilities has to correspond at least to the degree of redundancy of the process-related plant component to be supplied.

Note: A structural interconnection of the individual redundancies of the emergency power supply facilities is acceptable in individual cases if it has been demonstrated that this will not unacceptable impaired the reliability of the emergency power system. Here, special care shall be taken that none of the possible failures to be considered must lead to the failure of more than one redundancy.

3.9 (8) Energy storage systems have sufficient capacity for at least 10 h in order to be able to execute necessary functions until the AC electrical power supply is restored.

3.10 Requirements for the handling and storage of the fuel assemblies

3.10 (1) Control of reactivity shall be ensured for all operating phases in case of normal operation, anticipated operational occurrences, postulated single initiating events, postulated multiple failure events as well as in the case of internal and external hazards.

3.10 (2) Procedures and items important to safety for the handling and storage of non-irradiated and irradiated nuclear fuel shall be provided such that a criticality event in the storage facilities is practically eliminated even under accident conditions as well as in the case of internal and external hazards.

3.10 (3) Fuel cooling (heat removal from the facilities for the storage of fuel assemblies) shall be ensured in all operating phases in case of normal operation, anticipated operational occurrences, postulated single initiating events, postulated multiple failure events as well as in the case of internal and external hazards. At level 1 of defence in depth the temperature of the pool water shall not exceed 45°C. (see also Tab. 3-4 in Annex 1). The safety systems ensuring residual-heat removal shall meet the 72 h self-sufficiency criterion.

3.10 (4) A diverse ultimate heat sink shall ensure residual heat removal for all operating conditions in case of an unavailability of the ultimate heat sink due to failures of the cooling water intake or discharge. If necessary efficient cooling capabilities shall be ensured by a combination of various heat sinks. The necessary items important to safety shall fulfil at least the requirements at level 3b of defence in depth. The effectiveness shall be demonstrated. The availability of the diverse ultimate heat sink shall be ensured also in case of site specific external hazards.

3.10 (5) Fuel handling and storage systems shall be provided at the nuclear power plant to ensure that the integrity and properties of the fuel are maintained at all times during fuel handling and storage.

a) The design of the plant shall incorporate appropriate features to facilitate the lifting, movement and handling of fresh fuel and spent fuel.

b) The fuel handling and storage systems for irradiated and non-irradiated fuel shall be designed:

- To permit inspection of the fuel;
- To permit maintenance, periodic inspection and testing of components important to safety;
- To prevent damage to the fuel;
- To prevent the dropping of fuel in transit;
- To provide for the identification of individual fuel assemblies;

- To provide proper means for meeting the relevant requirements for radiation protection;
- To ensure that adequate operating procedures and a system of accounting for, and control of, nuclear fuel can be implemented to prevent any loss of, or loss of control over, nuclear fuel.

c) In addition, the fuel handling and storage systems for irradiated fuel shall be designed:

- To permit adequate removal of heat from the fuel in operational states and in accident conditions;
- To prevent the dropping of spent fuel in transit;
- To prevent causing unacceptable handling stresses on fuel elements or fuel assemblies;
- To prevent the potentially damaging dropping on the fuel of heavy objects such as spent fuel casks, cranes or other objects;
- To permit safe keeping of suspect or damaged fuel elements or fuel assemblies;
- To control levels of soluble absorber if this is used for criticality safety;
- To facilitate maintenance and future decommissioning of fuel handling and storage facilities
- To facilitate decontamination of fuel handling and storage areas and equipment when necessary;
- To accommodate, with adequate margins, all the fuel removed from the reactor in accordance with the strategy for core management that is foreseen and the amount of fuel in the full reactor core;
- To facilitate the removal of fuel from storage and its preparation for off-site transport.

d) For reactors using a water pool system for fuel storage, the design of the plant shall include the following:

- Means for controlling the temperature, water chemistry and activity of any water in which irradiated fuel is handled or stored;
- Means for monitoring and controlling the water level in the fuel storage pool and means for detecting leakage;
- Means for preventing the uncovering of fuel assemblies in the pool in the event of a pipe break (i.e. anti-siphon measures).

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 in case of normal operation, anticipated operational occurrences, postulated single initiating events, postulated multiple failure events, postulated core melt accidents and in the case of internal and external hazards to the necessary extent.

3.11 (4) Procedures and items important to safety 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 materials. These procedures and items important to safety shall be designed in such a way that neither any inadmissible radiation exposure nor any inadmissible release of radioactive material into the environment needs to be assumed. Proper arrangement and shielding of the items important to safety shall be considered in the design phase. During the operation phase the items important to safety shall be kept in such a condition that neither inadmissible radiation exposure nor any inadmissible release of radioactive material into the environment needs to be assumed.

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 individual cases.

3.11 (5) 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.

3.11 (6) Characteristics of the natural environment and meteorological conditions in the region of the plant shall be determined for investigating potential radiological impacts in operational states and accident conditions. Potential radiological impacts that could lead to emergency measures limited in area and time shall be evaluated with due consideration of the relevant factors, including population distribution, dietary habits, use of land and water, and the radiological impacts of any other releases of radioactive material in the region. All these characteristics shall be observed and monitored throughout the lifetime of the installation.

3.11 (7) Materials used in the manufacture of structures, systems and components shall be selected to minimize activation of the material as far as is reasonably practicable.

3.11 (8) Facilities shall be provided for the decontamination of operating personnel and plant equipment.

3.12 Waste Management

3.12 (1) Careful planning has to be applied to the siting, design, construction, commissioning, operation, shutdown and decommissioning of facilities in which waste is generated, to keep the volume and the radioactive content of the waste arising to the minimum practicable. The measures to control radioactive waste generation are generally applied in the following order:

- reduce waste generation,
- reuse items as originally intended,
- recycle materials and,
- consider disposal as waste.

4 Postulated operating conditions and events

4.1 Operating conditions, anticipated operational occurrences and accidents (associated levels 1 to 3a of defence in depth)

4.1 (1) The design of the structures, systems and components to be realised according to subsection 2.1 (3a) at levels 1 to 3a of defence in depth shall be based on:

- the operating conditions to be expected during normal operation, including testing conditions,
- the events whose occurrence is anticipated during the operating lifetime of the plant (anticipated operational occurrences), and
- a comprehensive spectrum of events whose occurrence is not to be expected during the operating lifetime of the plant due to the reliability and effectiveness of the items important to safety provided, but which shall be postulated (postulated single initiating events).

4.1 (2) The respective items important to safety 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 1) are met, also considering specified boundary conditions.

4.1 (3) The completeness and the comprehensive character of the events to be considered shall be ensured plant-specifically. Especially, the specific characteristics of the reactor type resulting in new kind of events have to be considered in the determination of the plant specific event list (see Annex 1 also).

4.2 Events involving multiple failures of safety systems (associated to level 3b of defence in depth)

4.2 (1) A list of multiple failure events shall be derived by

- postulating common cause failures of items important to safety needed to fulfil a safety function to control anticipated operational occurrences or postulated single initiating events,
- postulating common cause failures of items important to safety needed to fulfil the fundamental safety functions in normal operation, or
- postulating random failures that affect simultaneously several safety (or safety related) systems, if such a combination has to be assumed due to its probability indicated by probabilistic safety analyses.

4.2 (2) From this list the representative event sequences, which present the greatest challenge to the acceptance criteria and which define the performance parameters for safety related equipment, shall be selected based on the results from the deterministic and probabilistic safety analysis, operating experience feedback, engineering judgement as well as results of reactor safety research and international recommendations.

Note: Here, accident sequences shall be considered which according to the results of probabilistic safety analyses make a dominant contribution to the core meltdown frequency and furthermore especially those that may lead to an instantaneous release of radioactive materials into the environment. Events are listed in tables 4-1 (pressurized water reactors) and 4-2 (boiling water reactors) of Annex 1.

4.2 (3) Additional safety systems at level 3b of defence in depth for restoring and maintaining fuel assembly cooling in the spent fuel storage pool shall be designed in particular to control the following postulated multiple failure events:

- total loss of residual heat removal systems of the spent fuel storage pool, and
- loss of coolant from the spent fuel storage pool with decrease of filling level below the minimum level required for cooling.

4.2 (4) Internal and external events with the potential to cause multiple failures of safety systems shall be taken into account.

4.3 Accidents with core melt (associated to level 4 of defence in depth)

4.3 (1) For the design of complementary safety features at level 4 of defence in depth, a spectrum of events shall be postulated that takes the relevant phenomena of accidents with core melt into account for the respective plant type.

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

4.4 Internal and external hazards

4.4 (1) The protection of structures, systems and components against internal and external hazards according to subsection 2.5 shall be based on the following:

a) the relevant internal and external hazards and

b) other external hazards to be postulated at the site under consideration;

c) the special characteristics of external hazards of long duration;

d) combinations of several natural or human induced external hazards (e.g. earthquake, flooding, storm, lightning, fire, human-induced hazards) or combinations of these hazards with plant internal events (e.g. pipe break, loss of offsite power) or internal hazards (e.g. internal fires, internal flooding). These combinations shall be considered if the combined events or hazards are related or if their simultaneous occurrence has to be assumed due to their probability and degree of damage.

4.4 (2) All structures, systems and components shall be classified according to their safety significance in case of internal or external hazards. The classification shall take into account all possible effects of internal and external hazards, the role of the respective structures, systems and components in

ensuring the safety functions, their location, and possible interactions with items important to safety. For each specified class the requirements for the level of protection applicable to the items in this class shall be defined in a way to ensure that the requirements of subsection 2.5, 2.1 (5a) and 2.1 (5b) are met.

4.4 (3) Changes in site characteristics over time with respect to external hazards shall be taken into account.

5 Requirements for the safety demonstration

5 (1) The licensee/applicant shall be in the position to provide documentary evidence on plant safety covering all the stages during the lifetime of the plant. The safety demonstrations shall be documented in the Safety Analysis Report. The Safety Analysis Report shall be complete, comprehensible and verifiable. The Safety Analysis Report shall be updated whenever necessary to document the actual status of plant safety.

Note: Specifications of the Safety Analysis Report are presented in IAEA Safety Standards.

5 (2) The safety assessment shall be independently verified by the operating organisation before it is used by the operating organization or submitted to the regulatory body. This verification shall be performed by a group different from those carried out the safety assessment. The independent verification shall be performed by suitably qualified and experienced individuals.

5 (3) The safety assessment shall demonstrate, that

- the site characteristics have been properly analysed;
- all possible radiation risks associated with the nuclear power plant have been identified;
- the items important to safety can reliably fulfill the fundamental safety functions;
- defence in depth has been adequately implemented and that sufficient safety margins have been provided in the design and operation of the nuclear power plant;
- adequate measure for radiation protection have been implemented;
- all items important to safety are based on a robust and proven design;
- human interactions with the nuclear power plant are assessed with respect to nuclear safety.

5 (4) Assessments of the effects of natural hazards exceeding the design basis events of the plant shall be undertaken. Analysis shall, as far as practicable, include:

a) determining the severity of the event at which fundamental safety functions cease to be available;

b) demonstration of sufficient margins to “cliff-edge effects”;

c) identification and assessment of the most resilient means for ensuring the fundamental safety functions;

d) consideration that events could simultaneously challenge redundant or multiple SSCs, several units at multi-unit sites, site and regional infrastructure, external supplies and other countermeasures;

e) on-site verification (typically by walk-down methods).

5 (5) The following deterministic and probabilistic methods shall be applied to demonstrate that the technical safety requirements are fulfilled:

The methods comprise

a) the computational analysis of events and conditions,

b) the measurement and experiment,

c) the engineering judgement, and

d) the probabilistic analysis.

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

a) an up-to-date compilation of safety-relevant information about the current condition of the respective items important to safety affected and

b) documentation, that the condition of the items important to safety affected are in agreement with the currently valid requirements.

5 (7) For the analysis of events (a generic list of events for nuclear power plants is provided in Annex 1 and for research reactors in Annex 6) and conditions,

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

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

5 (8a) To supplement the deterministic safety analyses, the balance of the safety related design shall be verified by probabilistic safety analyses in order to identify potential weak points. Probabilistic safety analysis of level 1, level 2 and level 3 shall be performed for all operational states.

5 (8b) To supplement the deterministic safety demonstrations, probabilistic safety analyses shall be applied to assess the safety significance

- of modifications of procedures,
- of modifications of structures, systems and components or
- modifications of the operating mode of the plant, as well as
- new findings,

for which a significant influence on the probabilistic safety analysis results cannot clearly be excluded.

5 (8c) The relevant parameter of the probabilistic safety analysis of level 1 is the average core damage frequency for all operating phases of power operation and low-power and shutdown conditions, all plant-internal events as well as all internal and external hazards. The relevant information from the probabilistic safety analysis of level 2 is the confirmation that large early releases are prevented and the overall remaining release frequency. In addition the probabilistic safety analysis of level 2 shall provide the source term to be used in the probabilistic safety analysis of level 3. The probabilistic safety analysis of level 3 analysis is used to confirm that with the expected releases the radiological safety objectives are met.

5 (9) Where a new design, feature or engineering practice is introduced it shall be ensured that the quality and reliability is commensurate with the safety significance as required in 3.1 (5). Before implementation of such a design, feature or engineering practice the transferability of

a) results from precedent research and development programs,

b) performance tests with specific acceptance criteria and

c) examination of operational experience from similar applications

d) on the expected conditions in a nuclear power plant shall be demonstrated.

After implementation of a new design, feature or engineering practice a procedure shall be established to verify that the plant can be safely operated within specified operational limits and conditions.

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

a) the applicability of the experimental conditions to the plant conditions of the respective application context has been qualified, and

b) the uncertainties associated with the measurement have been quantified.

5 (11) Engineering judgement may be used for the safety demonstration if acceptance criteria exist that are scientifically/technically comprehensible.

5 (12) The accomplishment of requirements shall be demonstrated by accepted and verified investigation and evaluation methods. The verification process shall be repeated periodically.

5 (13) A periodic safety review shall be performed every 10 years.

5 (14) The scope of the review shall be clearly defined and justified. Each area shall be reviewed and their findings compared to the licensing requirements as well as to the current safety standards and the current state of the art of science and technology. The safety significance of all findings shall be evaluated using deterministic and probabilistic methods as appropriate. For all findings, a list of proposed safety improvements shall be prepared, or if no safety improvement can be identified that is reasonable and practicable, a justification shall be given.

5 (15) The scope shall be as comprehensive as reasonably practical with regard to significant safety aspects during all phases of operations and – as a minimum – the following areas shall be covered by the review:

- Plant design as built and actual condition of systems, structures and components (including ageing management and equipment qualification);
- Site characteristics and the protection against external hazards;
- Reassessment of the internal hazards;
- Safety analyses and their use;
- Operating experience and relevant research findings during the review period and the effectiveness of the system used for experience feed-back;
- Organisation, human factors, management system and safety culture
- Relevant procedures;
- Emergency preparedness;
- Radiation protection of the workers and the public as well as the radiological impact on the environment;
- Interactions between units at sites with more than one unit (e.g. hazards, possible common SSCs, organisation and management system, procedures, emergency preparedness)

6 Requirements for the operating rules

Note: Specifications in this respect are presented in Annex 4.

6 (1) Written instructions shall exist for normal operation, anticipated operational occurrences and accident conditions, in which the following is specified:

a) A sufficiently complete set of provisions whose compliance ensures that the operation of the plant fulfils the safety requirements and conditions of the licence. The provisions shall comprise, in particular, the process-related and plant conditions, effectiveness, availability and relevant boundary conditions of safety-relevant plant components to be observed (operational limits and conditions).
The specification of the operational limits and conditions shall be based on the plant design, the safety analyses, the licensing conditions and the experiences from commissioning and operation. The specification of the operating limits and conditions shall comprise all operating phases.

b) Instructions for the case of deviations from the operational limits and conditions.

c) The provisions to be fulfilled to prevent or control anticipated operational occurrences, postulated single initiating events, postulated multiple failure events and postulated core melt accidents. Both event based approaches and symptom based approaches shall be used, as appropriate.

d) The necessary in-service inspections of items important to safety.

e) The organisational regulations relevant for ensuring safe plant operation (structural and procedural organisation).

f) The minimum requirements for the number and qualification of the personnel and the minimum availability of personnel at the plant for ensuring safe plant operation and control of anticipated operational occurrences, postulated single initiating events, postulated multiple failure events and postulated core melt accidents; here postulated initiating

events or consequential events of internal or external hazards and occupational accidents, shall also be considered.

g) Written procedures shall exist describing the interaction with notification points in case of emergencies.

6 (2) The documents according to subsection 6 (1) shall be directly accessible to the personnel in the control room and the documents according to 6 (1) a) to d) shall be directly accessible to the personnel in the supplementary control room.

All documents needed for the work of the disaster response team shall be kept available in the emergency control centre.

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

6 (4) The design basis for each item important to safety shall be systematically justified and documented. For all items important to safety design codes, material specifications, assembly instructions and test codes as well as operating instructions and maintenance standards shall be provided or be in place 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 installations that are necessary for assessing quality shall be accessible until dismantling of the equipment.

6 (5) The provisions and operational limits and conditions required in 6 (1) a) shall include:

(a) Safety limits;

(b) Limiting settings for safety systems;

(c) Operational limits and conditions for operational states;

(d) Control system constraints and procedural constraints on process variables and other important parameters;

(e) Requirements for surveillance, maintenance, testing and inspection of the plant to ensure that structures, systems and components function as intended in the design, to comply with the requirement for optimization by keeping radiation risks as low as reasonably achievable;

(f) Specified operational configurations, including operational restrictions in the event of the unavailability of safety systems or safety related systems;

(g) Action statements, including completion times for actions in response to deviations from the operational limits and conditions.

7 Requirements for the documentation

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

Note: Details are provided in Annex 4

Annex 1:
Postulated Events
19.3.2015

Contents

1 Objectives and scope

1 (1) For the events presented in the following generic event lists for pressurized water reactors (PWR) and boiling water reactors (BWR) (hereinafter referred to as event lists), it shall be demonstrated by means of computational analyses that the criteria specified in the “Safety Requirements for Nuclear Power Plants” have been met. Especially for these events it shall be demonstrated in accordance with the “Annex 4 of the Safety Requirements for Nuclear Power Plants: Requirements for the 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.

Note: In the event lists, the events are classified according to the respective fundamental safety functions

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

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

For each protection goal, the acceptance targets and criteria assigned to the levels of defence 2 to 3b are presented in the Tables 3-3 for the reactor plant and in Table 3-4 for fuel assembly storage and handling, for the radiological safety objective in Table 3-5.

1 (2) No events were defined for level 4 of defence in depth. A spectrum of events shall be postulated that takes the relevant phenomena of accidents with core melt into account for the respective plant type (see 4.3 (1) of “Dutch Safety Requirements for Nuclear Reactors”). In accordance with the protection goals defined in the "Dutch Safety Requirements for Nuclear Reactors" Section 2.1 (3b), proof has to be furnished with respect to the postulated phenomena. To prevent any large-scale and early releases, the following conditions have to be practically excluded:

- core melt under high pressure and direct containment heating
- fast reactivity accidents

- steam explosions (in-vessel and ex-vessel phenomena)
- hydrogen detonation
- core melt sequences involving containment bypass leading to early and large releases
- fuel melt in fuel pool

As for controlling core meltdown accidents at low pressure, it has to be demonstrated that the core melt can be cooled sufficiently and that the containment can be maintained as a barrier.

The Safety demonstration shall be based on deterministic and probabilistic methods as required in Section 5 of the “Safety Requirements for Nuclear Power Plants”.

1 (3) The fulfilment of the criteria according to 1 (1) shall be demonstrated on the basis of the operating phases defined in Table 1-1 (for pressurized water reactors) and Table 1-2 (for boiling water reactors).

Table 1-1 Definition of the operating phases for pressurized water reactors (PWR)

Operating phase	Definition	System states (normal operation)	k_{eff} [8]
A	Nuclear power and startup operation	- power state as well as hot or intermediate shutdown state with all the automatic reactor protection functions available	≥ 0,99
B	Subcritical hot	- residual heat removal system not connected	< 0,99
C	Subcritical cold Primary circuit pressure-tight	- intermediate and cold shutdown, with the residual heat removal system in operation and - the primary coolant system closed	< 0,99[9]
D	Subcritical cold Primary circuit not pressure-tight	- cold shutdown with the primary coolant system open	< 0,95[2]
E	Refuelling	- cold shutdown with the reactor cavity flooded	< 0,95[2]
F	Fuel assembly storage	- cold shutdown with the reactor core totally unloaded - Cooling of the fuel assemblies via the spent fuel pool cooling systems	< 0,95

[8] The safety demonstration with respect to the control of events on levels of defence 2 and 3 may result in further requirements for the k_{eff} values required according to the operating procedures (margin for event sequences to be controlled).

[9] With the control elements withdrawn from the reactor core.

Table 1-2 Definition of the operating phases for boiling water reactors (BWR)

Operating phase	Definition	System states (normal operation)	k_{eff} [10]
A	Nuclear power and start-up operation	Power state or start-up operation (beginning of withdrawal of control elements)	≥ 0,99
B[11]	Subcritical hot	- All control elements completely inserted - Residual heat removal system not connected	< 0,99
C	Subcritical cold Primary circuit pressure-tight	- intermediate and cold shutdown, with the residual heat removal system in operation and - the primary coolant system closed	< 0,99[12]
D	Subcritical cold Primary circuit not pressure-tight	- cold shutdown with the primary coolant system open and reactor cavity not completely flooded	< 0,99
E	Refuelling	- cold shutdown with the reactor cavity flooded - fuel elements in reactor and in spent fuel storage pool	< 0,99[13] in reactor < 0,95 in pool
F[14]	Fuel assembly storage	- cold shutdown with the reactor core totally unloaded - Cooling of the fuel assemblies via the spent fuel pool cooling systems	< 0,95

[10] The safety demonstration with respect to the control of events on levels of defence 2 and 3 may result in further requirements for the k_{eff} values required according to the operating procedures (margin for event sequences to be controlled).

[11] Upon start-up of the BWR, there is a direct transition from Phase C to Phase A, due to the nuclear heat-up caused by the withdrawal of the control elements.

[12] In zero-load inspections, only the number of control elements is withdrawn that will ensure that criticality is avoided.

[13] Not during function or subcriticality tests nor during the shutdown safety test; here, however, 2 control elements at the most not inserted.

[14] In a BWR, operating Phase F generally only occurs in special cases (e.g. pressure test of the reactor pressure vessel).

2 General requirements for safety demonstration

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

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

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

2 (4) The specific characteristics of the reactor type resulting in new kind of events have to be considered in the determination of the plant specific event list.

2 (5) 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 2 to 3b of defence in depth 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 periodic safety reviews with the events summarised in the generic event lists (Tables 4-1 to 4-3).

b) Verification of the representative character of the event lists and -where required- plant-specific supplementation and adjustment of the lists.

c) As far as appropriate for level 2 to 3b of defence in depth, condensing of the event lists prepared according to b) under the aspect of the representative character of individual events. Condensing is justified in a detailed and comprehensible manner.

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

3 Acceptance targets and acceptance criteria

Table 3-1 Safety-related acceptance targets and acceptance criteria of levels of defence 2 to 3b for the reactor plant and the fundamental safety function "control of reactivity"

Level of defence	**2**	**3a**	**3b**
fundamental safety function	**Control of reactivity (R)**		
Acceptance targets	**Power adjustments or reactor shutdown[15]**	**Reactor shutdown[8]**	
Acceptance criteria	Also see "Cooling of the fuel assemblies" (Tab. 3-2) and "Confinement of radioactive material" (Tab. 3-3)		
Acceptance target	**Ensuring sub-criticality**		
Acceptance criteria[16] „Amount of shutdown reactivity"	≥ 1 %	≥ 1 %	sub-criticality k_{eff} < 0,999

[15] Only operating phase A

[16] Acceptance criteria for the effectiveness of reactor scram (only operating phase A as well as, for boiling water reactors (BWRs), also temporarily in operating phase E during refuelling) and shutdown in the long term (all operating phases). The boundary conditions specified in the "Safety Requirements for Nuclear Power Plants", subsections 3.2 (6) and 3.2 (7) have been met. During refuelling (operating phase E), the failure of the most effective control element to insert fast need not be postulated.

Table 3-2 Safety-related acceptance targets and acceptance criteria of levels of defence 2 to 4 for the reactor plant and the fundamental safety function "cooling of the fuel assemblies"

Level of defence	2	3a and 3b	4
fundamental safety function	Cooling of the fuel assemblies (K)		
Acceptance targets	Unrestricted reuse of the fuel assemblies	Possibility of shutdown and cooling of the reactor core	
Acceptance criteria	- For anticipated operational occurrences with respect to cooling of fuel elements there shall be 95 % probability at 95 % confidence level that departure from nucleate boiling or dry-out will be avoided. - No internal melting of the fuel	- $T_{Cladding} < 1.200$ °C - Shutdown and coolability in the short and long term	- Removal of the residual heat in the long term

Table 3-3 Safety-related acceptance targets and acceptance criteria of levels of defence 2 to 3b for the reactor plant and the fundamental safety function "confinement of radioactive material"

Level of defence	2	3a	3b
fundamental safety function	**Confinement of radioactive material (B)**		
Acceptance target	**To maintain barrier integrity**		
Acceptance criteria	– pressure increase in containment below limits of the reactor protection system – BWR: Keeping of specified temperatures in the pressure-suppression pool – pressure in the primary system below design pressure – pressure in the primary systembelow pressure limits for opening of safety valves – no PCI[17] – For anticipated operational occurrences with respect to cooling of fuel elements there shall be 95 % probability at 95 % confidence level that departure from nucleate boiling or dry-out will be avoided.	– pressure in the containment below design pressure of the containment – BWR: Keeping of specified temperatures in the pressure-suppression pool – pressure in the primary system below 1.1 times the design pressure[4] – hydrogen concentration everywhere inside the containment below ignition limit – maximum cladding oxidation must remain lower than 17 % of the cladding thickness – leakage ≤ 0.1 A: integrity of the fuel rods – leakage > 0.1 A: number of damaged fuel rods ≤ 10 % – less than1 % of the total available Zirconium inventory is allowed to react with water	– pressure in the containment below design pressure of the containment – boiling water reactors (BWR): Keeping of specified temperatures in the pressure-suppression pool – pressure in the primary system below 1.3 times the design pressure[12]

[17] Only operating phases A and B (PCI: Pellet Cladding Interaction)

Table 3-4 Safety-related acceptance targets and criteria of level of defence 2 to 3b for fuel assembly storage and handling

Level of defence	2	3a	3b
Fundamental safety function	**Control of reactivity (R)**		
Acceptance target	Ensuring sub-criticality		
Acceptance criteria "neutron multiplication factor k_{eff}"	< 0,95[18]	< 0,95[13]	< 0,999[13]
fundamental safety function	**Cooling of the fuel assemblies (K)**		
Acceptance targets	Limitation of the pool water temperatures to values which ensure accessibility of the pool area with customary measures	Limitation of the pool water temperatures to values below the design temperature of the pool to ensure the integrity of the pool	Limitation of the pool water temperatures to values which ensure pool integrity
	Sufficient water coverage for ensuring the required inlet condition for the pool pumps	Sufficient water coverage for ensuring fuel assembly cooling	Sufficient water coverage for ensuring spill or evaporation cooling (maintenance of fuel rod integrity)
Acceptance criteria	pool water temperature ≤ 60°C	pool water temperature ≤ 60°C	pool water temperature ≤ 80°C
fundamental safety function	**Confinement of radioactive material (B)**		
Acceptance targets	see Table 3-3		
Acceptance target	**Maintenance of the retention function of buildings and systems**		
Acceptance criteria	see Table 3-5		

[18] A coolant density that leads to the largest neutron multiplication factor and being possible under the given circumstances shall be assumed. The demonstration of criticality safety shall be based on the assumption that the coolant is pure water.

Table 3-5 Deleted

Table 3-6 Radiological safety objectives of levels of defence 4 for the reactor plant and fuel assembly storage and handling

Measure	Evacuation Zone (< 3 km)	Sheltering Zone (< 5 km)	Beyond Sheltering Zone
Permanent Relocation	No	No	No
Evacuation	May be needed	No	No
Sheltering	May be needed	May be needed	No
Iodine Prophylaxis	May be needed	May be needed	No

4 Generic event lists

The generic event lists comprise for power operation and low-power and shutdown operation of pressurized water reactors and boiling water reactors the levels 2 to 3b of defence in depth and for the spent fuel pool (of pressurized water reactors and boiling water reactors) the levels 2 to 3b of defence in depth according to the "Dutch Safety Requirements for Nuclear Reactors". For levels 2 to 3b of defence in depth, comprehensive event spectra are available. In the plant-specific review, this list may be condensed to representative events if a documented justification according to number 2 (4) is provided.

Accidents with core melt are developed from events at level 3b of defence in depth if the foreseen preventive accident management measures fail.

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

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

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

For the pressurized water reactor (PWR) the event categories are:

- change of secondary-site heat removal,
- secondary-site heat removal - leakages,
- 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,
- internal event,
- anticipated transient without scram (ATWS),
- loss of component cooling,
- loss of secondary site heat removal, and

For the boiling water reactor (BWR) the event categories are:

- main-steam or feedwater-site 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,
- internal event,
- anticipated transient without scram (ATWS),
- loss of component cooling and

For the fuel pool of pressurized water reactors (PWR) and boiling water reactors (BWR), the following event categories are applicable:

- Reduced heat removal from the fuel pool,
- loss of coolant from the fuel pool,
- loss of energy supply,
- reactivity changes in the fuel pool, and
- events during handling and storage of fuel assemblies and heavy loads.

The first column of the event lists gives the number of the event. For numbering the general listing Xy-x; for X is used: D is applied for pressurized water reactors, S for boiling water reactors and B for fuel pool, y stands for the level of defence, and x represents the consecutive number of the events on the respective level or in the respective table. This is followed by a description of the events in the next column. There then follow columns for the fundamental safety functions affected, the relevant operating phases, additional explanations regarding the acceptance criteria and, if necessary, detailed information about supplementary boundary conditions or notes specific to the event.

The labels in the "fundamental safety functions affected" column indicate for each event those fundamental safety functions (R for “control of reactivity”, K for “cooling of the fuel assemblies”, B for “confinement of radioactive material” for the fundamental safety functions, and in addition the radiological safety objective S for “Protection of man and environment against harmful effects of ionizing radiation” to mark events that are relevant regarding the release of radionuclides) for which the effectiveness of the inherent features, equipment, and procedures has to be demonstrated. The acceptance criteria generally applying to the individual fundamental safety functions are contained in Section 3, for power operation (operating phase A) and low-power and shutdown operation (operating phases B-F) of pressurized water reactor and boiling water reactor as well as for the spent fuel storage pool. Here, the acceptance criteria for the different levels of defence and operating phases are specified.

In the right-hand column, event-specific boundary conditions are put more precisely if need be, and detailed event-specific explanations are given.

The "operating phase" column refers to those phases of power plant operation in which the respective event may occur and be relevant.

The structure of the lines of the lists starts with the designation of the level of defence. The line that follows refers to the event category from which the subsequently listed events are derived. For leaks and breaks, the maximum flow cross-section considered depends on whether or not break preclusion has been demonstrated for the piping section in question.

Note: For the definition of the terms “leakages” and “leak” see Annex 5.

Table 4-1 Event list power operation and low-power and shutdown operation of pressurized water reactors (PWR)

No.	Events PWR	Fundamental safety function concerned	Operating phase	Additionally considered 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 or primary circuit	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 increase in the steam generator or primary circuit.	K	A-B	Note: E.g. turbine control faults, partially inadvertent closure of main steam isolation valves.
D2-03	Inadvertent closure of valves leading to significant changes in main steam or feedwater flow rate.	K, B	A-B	
D2-04	Turbine trip with opening of the bypass station	R, K, B	A	
D2-05	Turbine trip with delayed failure of the bypass station or without opening of the bypass station	R, K, B	A	

No.	Events PWR	Fundamental safety function concerned	Operating phase	Additionally considered comments, boundary conditions and notes
D2-06	Loss of main heat sink	R, K, B	A-B	
D2-07	Load rejection to auxiliary power	R, K, B	A	Additional boundary condition: With and without switching to off-site power supply.
D2-08	Failure of a main feedwater pump without actuation of the standby pump	R, K	A	
D2-09	Failure of all operating main feedwater pumps with and without actuation of the 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	Note: Coastdown behaviour as per design of the reactor coolant pumps is assumed.
Pressure change in the primary circuit				
D2-12	Pressure drop due to inadvertent pressuriser spraying actuation or inadvertent valve opening	K	A-B	

No.	Events PWR	Fundamental safety function concerned	Operating phase	Additionally considered comments, boundary conditions and notes
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 operating phases B and C are considered.
D2-16	Malfunction in the volume 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: The successful prevention of the failure of the residual-heat removal pumps caused by the level drop has to be demonstrated.
D2-18	Leaks in the pressuriser steam space	K	A-B	Note: Without automatic actuation of the safety system.
Loss of residual-heat removal				
D2-19	Loss of a train in operation of the residual-heat removal system including cooling	K, B	C-E	Additional boundary condition: Single failure is not postulated

No.	Events PWR	Fundamental safety function concerned	Operating phase	Additionally considered comments, boundary conditions and notes
	chain			
D2-20	Loss of all residual-heat removal trains due to inadvertently triggered signals (short term)	K, B	C-E	Additional boundary condition: The limit values for taking the residual-heat removal system into operation are not 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 failure of the limitation systems	R, K	A-B	
D2-23	Inadvertent drop or insertion of one or more control elements	R, K	A	
D2-24	Inadvertent injection from a system carrying deionised water or low-borated coolant (external boron dilution; homogeneous and heterogeneous)	R	A-E	
D2-25	Most unfavourable misloading of the most reactive fuel assembly	R, K	E, A	Additional boundary condition: Reactor startup with misloaded fuel assembly is analysed regarding protection goal K in operating phase A. Comment: - Fundamental safety function R (subcriticality) in operating phase E - Fundamental safety function K in operating phase A

No.	Events PWR	Fundamental safety function concerned	Operating phase	Additionally considered comments, boundary conditions and notes
D2-26	Non-compliance with the actuation conditions upon the start-up of a main coolant pump following 3-loop operation	R, K	A	
D2-27	Cold water injection into the reactor coolant system from a connected system (e.g. bypass of the recuperative heat exchanger of the volume control system)	R	A-B	
Loss of energy supply				
D2-28	Loss of offsite power for less than 10 hours	R, K, B	A-E	Additional boundary condition: The restoration of the external electrical power supply has to be analysed as well.
Level of defence 3				
Level of defence 3a				

No.	Events PWR	Fundamental safety function concerned	Operating phase	Additionally considered comments, boundary conditions and notes
Change of the secondary-side heat removal				
D3a-01	Major malfunction in the main steam system or in the feedwater supply system, leading to an unplanned temperature or pressure reduction in the steam generator or in the primary circuit	R, B, S	A-C	Additional boundary condition: Operationally permissible steam generator tube defects are considered. Note: E.g. inadvertent complete opening of main steam bypass valve, inadvertent opening of main steam safety and main steam relief valves. Relevant with regard to radiology (since no N16 detection) in phase B or in phase A at low power. Inadvertent opening in phase B more probable than in phase A due to performance of tests.
D3a-02	Major malfunction in the main steam system or in the feedwater supply system, leading to an unplanned temperature or pressure increase in the steam generator or in the primary circuit	K, B, S	A-B	Additional boundary condition: Operationally permissible steam generator tube damage has to be taken into account. Cases to be considered: e.g. inadvertent closing of two up to all main steam isolation valves.
D3a-03	Loss of feedwater supply	K	A-B	Note: This is to be understood as the loss of the main feedwater supply as well as of the installations used during startup and shutdown (startup and shutdown system or emergency feedwater system in operating mode).

No.	Events PWR	Fundamental safety function concerned	Operating phase	Additionally considered comments, boundary conditions and notes
D3a-04	Malfunction in the feedwater supply, leading to an impermissible increase of the coolant level in the steam generator	K	A-B	
Secondary-side heat removal – leaks				
D3a-05	Secondary-side leak or secondary-side break within the containment	R, K, B	A-C	Additional boundary condition: At low secondary circuit pressures, the effectiveness of the actuation due to dp/dt and / or containment pressure difference at the respective leak spectrum has to be considered.
D3a-06	Leak/break in main steam or feedwater system or other high-energy piping systems in the annulus and in the valve compartment	R, K, B, S	A-B	Additional boundary condition: Operationally permissible steam generator tube defects are considered for leak/break in the main steam and feedwater system. Special consideration of: the integrity of the containment, humidity, pressure build-up, differential pressures, temperature, jet and reaction forces, etc. with impacts affecting more than one redundancy, the integrity of safety-relevant structures of the reactor building and the valve compartment.
	Leak/break in the main steam or feedwater system downstream of the main steam isolation valve and upstream of the feedwater isolation valve	R, K, B, S	A-C	Additional boundary condition: Operationally permissible steam generator tube defects are considered for leak/break of the main steam line.
D3a-08	Main steam line rupture after first isolation with maximum 2A break of a steam generator tube	R, K, B, S	A-B	Additional boundary condition: The accidental steam generator tube rupture can be considered as a random failure.
D3a-09	Inadvertent opening of a main steam safe-	R, K, B, S	A-B	Additional boundary condition: The accidental steam generator tube rupture can be considered as a

No.	Events PWR	Fundamental safety function concerned	Operating phase	Additionally considered comments, boundary conditions and notes
	ty valve with consequential 2A break of a steam generator tube			random failure.
D3a-10	Inadvertent opening of a steam generator safety valve		A-B	
Change of flow rate in the primary circuit				
D3a-11	Forced decrease of reactor coolant flow (all pumps)	R, K, B	A-B	Note: Fast coastdown of the main coolant pumps (see also D2-13)
D3a-12	Reactor coolant pump seizure (blocked rotor)	R, K, B	A-B	
D3a-13	Reactor coolant pump shaft break	R, K, B	A-B	
Increase of reactor coolant inventory				
D3a-14	Inadvertent injection by operational systems or safety systems in case of ineffectiveness of limitation measures provided	K, B	A-C	
Decrease of reactor coolant inventory				
D3a-15	Inadvertent level drop during mid-loop operation with consequential loss of residual-heat removal pumps	R, K, B	C-D	- Fundamental safety function R affected due to reflux condenser mode in Phase C. - Fundamental safety function B is relevant for operating phase C (primary circuit closed)
Loss of residual-heat removal				

No.	Events PWR	Fundamental safety function concerned	Operating phase	Additionally considered comments, boundary conditions and notes
D3a-16	Loss of a train in operation of the residual heat-removal system including cooling chain	K, B	C-E	Additional boundary condition: In contrast to event D2-19, here with consideration of the single failure criterion.
D3a-17	Shutdown of all residual-heat removal trains by inadvertently triggered signals	K, B	C-E	Additional boundary condition: The analysis has to take the ineffectiveness of operator actions required at short notice into account (see event D2-20)
Change of reactivity and power distribution				
D3a-18	Inadvertent withdrawal of the most effective control element or control element group with loss of limitation systems	R, K	A-B	
D3a-19	Ejection of the most effective control element	R, K	A-B	
D3a-20	Misloading of the reactor core with more than one fuel assembly	R	E	
D3a-21	Drop of a fuel assembly on the reactor core	R	E	Additional boundary condition: Verification of subcriticality for fuel assembly on the core
D3a-22	Inadvertent injection from a system carrying deionised water or low-borated coolant with loss of limitation systems or preceding procedures (external boron dilu-	R, K	A-E	Additional boundary condition: The following is considered: - all possibilities and amount of an influx of demineralised water, - operator error or . inadvertent filling of tanks,

No.	Events PWR	Fundamental safety function concerned	Operating phase	Additionally considered comments, boundary conditions and notes
	tion; homogeneous and heterogeneous)			- input from connected systems via heat exchanger tubes, seals and / or valve seat leakages, and - 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 ionised 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 Table 3.1c and - for an initially subcritical reactor the amount of shutdown reactivity required according to Table 3.1a are complied with.
D3a-23	Formation of low-borated areas in the primary circuit (internal boron dilution)	R, K	A-C	<u>Additional boundary condition:</u> Potential sources of formation of low-borated areas shall be investigated. Causes may be, e.g., - reflux condenser operation after small LOCA under consideration of the inserted control elements (under consideration of “Safety requirements for Nuclear Power Plants” subsection 3.2 (6)) and the time-dependent xenon concentration, and - shutdown with three circuits and secondary-side isolated steam generator and injection of low-borated coolant after restart of natural circulation. - It shall be demonstrated that reactivity changes due to injection of ionised water into the reactor coolant system remain limited to such values where for an initially subcritical reactor the amount of shutdown reactivity required according to Table 3.1a is complied with.

No.	Events PWR	Fundamental safety function concerned	Operating phase	Additionally considered comments, boundary conditions and notes
D3a-24	Subcooling transients due to leak or break of main steam or feedwater line	R, K	A-B	Specification of the acceptance criteria: - Recriticality is only permissible in the case of leaks in the main steam line with high and rapid cooldown of the primary circuit if the criteria for fuel assembly cooling are fulfilled. - The leak size leading to the highest degree of subcooling has to be ~~postulated~~ identified.
Loss of coolant within the containment				
D3a-25	Small leak within the containment	R, K, B, S	A-B	Additional boundary condition: Reflux condenser mode shall be considered (see D3a-23). Note: Characteristic feature: Secondary-side heat removal necessary for the control of this postulated single initiating events
D3a-26	Medium leak within the containment (leak cross section ≤ 0.1 A)	R, K, B, S	A-B	Note: Characteristic feature of the medium leak: Heat removal via leak sufficient => secondary-side heat removal for control of this postulated single initiating event not generally necessary.
D3a-27	Large leak within the containment (leak cross section > 0.1 A)	R, K, B, S	A-B	Additional boundary condition: The double-ended break of a main coolant line (“2A break“) determines the dimensioning of the emergency core cooling and residual-heat removal system, the pressure design of the containment, the design of the pump flywheels against failure due to overspeed and the failure resistance of all safety-relevant components in the containment required for the control of accidents. Specification of the acceptance criteria: Subcriticality in the short term without taking the control elements into account unless effectiveness of the control elements has been demonstrated, and in the long term without taking the control elements into account.

No.	Events PWR	Fundamental safety function concerned	Operating phase	Additionally considered comments, boundary conditions and notes
D3a-28	Leak in the pressuriser steam space without reaching the containment pressure criterion	R, K, B, S	A-B	Note: With automatic actuation of the safety system.
D3a-29	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 practically eliminated. - The consequences of an event regarding sufficient coverage of sump suction lines with coolant in case of considered dead volumes of the reactor cavity shall be considered.
D3a-30	"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.
D3a-31	Leak in RPV closure head area	R, K, B, S	A-B	Additional boundary condition: In connection with the control of this event, it also has to be demonstrated in particular that the sufficient draining of the coolant into the containment sump is ensured, also considering the routine operational processes during and after plant standstills, i.e. a sufficiently dimensioned connection between the reactor cavity and the sump in operating phases A and B must be ensured.
D3a-32	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-

No.	Events PWR	Fundamental safety function concerned	Operating phase	Additionally considered comments, boundary conditions and notes
				holes). - The analysis shall consider that in case of an incident a fuel assembly is transported in the most unfavourable position. Here, the acceptance criterion is to maintain the cladding tube integrity. - Requirement for emergency cooling effectiveness; limited availability of safety systems (e.g. reactor protection) shall be considered.
D3a-33	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 systems (e.g. reactor protection) is considered.
D3a-34	Failure of a steam generator tube (larger than operationally permissible leakages and up to max. 2A)	K, B, S	A-B	Additional boundary condition: The event 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.
D3a-35	small leak loss of coolant accident in external systems (up to 50 mm diameter)	R, K, B, S	C-E	
D3a-36	intermediate break and large break loss of coolant accident (up to the surge line break in states A and B)	R, K, B, S	A-B	
D3a-37	Rupture of two steam generator tubes in one steam generator	K, B, S	A-B	Additional boundary condition: Leak size: up to 2A of an exchanger tube.
Loss of coolant outside the containment				

No.	Events PWR	Fundamental safety function concerned	Operating phase	Additionally considered comments, boundary conditions and notes
D3a-38	Leak in residual-heat removal system in rooms between containment and surrounding building during residual-heat removal operation	K, B, S	C-E	Additional boundary condition: Spiking effect shall be considered.
D3a-39	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.
D3a-40	Loss of coolant from the containment via systems connected to the reactor coolant pressure boundary	K, B, S	A-C	
D3a-41	Leaks in systems with flooding potential in the rooms between containment and surrounding building	K, B, S	A-E	Additional boundary condition: All relevant sources from leaks and containment failure of systems and devices in the annulus, in particular the containment sump suction line, shall be considered.
Release of radioactive material from nuclear auxiliary systems				
D3a-42	Leak in the volume control system outside the containment	S	A-F	Additional boundary condition: Spiking effect shall be considered.
D3a-43	Rupture of a line carrying primary coolant outside of the containment (e.g. sampling line)	S	A-F	
D3a-44	Leak/break in a pipe or break of a filter in the off-gas or gas treatment system	S	A-F	
D3a-45	Leak in container with active medium	S	A-F	Additional boundary condition:

No.	Events PWR	Fundamental safety function concerned	Operating phase	Additionally considered comments, boundary conditions and notes
				- The container with the largest radiological hazard potential shall be identified. - Analysis also has to cover container failure due to an earthquake.
Loss of energy supply				
D3a-46	long term loss of offsite power (> 10h)	R, K, B, S	A-C	Additional boundary condition: Operationally permissible steam generator tube leakages shall be considered.
Internal event				
D3a-47	Potential activity release as a result of plant-internal fires (including filter fires) or explosions	S	A-F	Additional boundary condition: Fires and explosions affecting components and in system areas with high activity release potential have to be considered.
D3a-48	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 damages of neighbouring drives occur that impair the functional safety of other control elements. If consequential damage cannot be practically eliminated, it shall be demonstrated that the acceptance criteria are also fulfilled.
Level of defence 3b				
Anticipated transient without scram (ATWS)				

No.	Events PWR	Fundamental safety function concerned	Operating phase	Additionally considered comments, boundary conditions and notes
D3b-01	Loss of main heat sink, e.g. by loss of condenser vacuum or closure of the main steam isolation valve with available house load supply	R, K, B	A	
D3b-02	Loss of main heat sink with unavailable house load supply	R, K, B	A	
D3b-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	
D3b-04	Total loss of main feedwater supply	R, K, B	A	
D3b-05	Maximum reduction of the coolant flow rate	R, K, B	A	
D3b-06	Maximum reactivity insertion by withdrawal of control elements or control element groups on the basis of the operating conditions “full load” and “hot subcritical”	R, K, B	A	
D3b-07	Depressurisation due to inadvertent opening of a pressuriser safety valve	R, K, B	A	
D3b-08	Maximum reduction of the reactor inlet temperature caused by a fault in an active component of the feedwater supply	R, K, B	A	
Loss of energy supply				

No.	Events PWR	Fundamental safety function concerned	Operating phase	Additionally considered comments, boundary conditions and notes
D3b-09	Loss of offsite power cumulated with the failure of all emergency diesel generators	R, K, B	A-F	Remark: mid-loop operation in state C or D DC power supply and back-up AC power supply available
D3b-10	Loss of offsite power and all onsite AC power sources	R,K,B	A-F	Remark: DC power supply available
Loss of component cooling				
D3b-11	loss of the component cooling water system	R, K, B	A-F	Remark: - mid-loop operation in state C or D - essential service water system cooling chains
Loss of secondary site heat removal				
D3b-12	total loss of feedwater		A	Remark: loss of the main feedwater, startup and shutdown, emergency feedwater systems
Loss of coolant accidents				
D3b-13	small break loss of coolant accident (up to 50 mm diameter) and loss of the medium head safety injection trains	R, K, B	A+C	
D3b-14	small break loss of coolant accident (up to 50 mm diameter) and loss of the low head safety injection trains	R, K, B	A+C	

No.	Events PWR	Fundamental safety function concerned	Operating phase	Additionally considered comments, boundary conditions and notes
D3b-15	small break loss of coolant accident and simultaneous loss of the component cooling water system/essential service water	R, K, B	A	
D3b-16	rupture of several steam generator tubes	R, K, B	A	Remark: up to 10 tubes in one steam generator
D3b-17	steam line break and simultaneous steam generator tube rupture	R, K, B	A	Remark: up to one tube in the affected steam generator
D3b-18	steam generator tube rupture with a main steam relief train stuck open at the affected steam generator	R, K, B	A	Remark: – one steam generator tube ruptured – leak size: up to 2A of an exchanger tube.

Table 4-2 Event list power operation and low-power and shutdown operation of boiling water reactors (BWR)

No.	Events BWR	Fundamental safety functions	Operating phase	Additionally considered 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 which lead to an unplanned temperature or pressure decrease in the reactor coolant system	R, K	A-B	Additional boundary condition: Impact on stability of the core is considered. Note: E.g. control fault, loss of high-pressure preheater, inadvertent actuation of a main steam turbine bypass, inadvertent actuation of auxiliary steam supply or of S&R valves.
S2-02	Malfunctions in the main steam system or in the feedwater supply system which lead to an unplanned temperature/pressure increase in the reactor coolant system	R, K, B	A-B	Note: – e.g. malfunction of turbine control, inadvertent closure of individual valves. – Relevant for pressure control, in particular of the main steam bypass
S2-03	Turbine trip with opening of the turbine bypass	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	

No.	Events BWR	Fundamental safety functions	Operating phase	Additionally considered comments, boundary conditions and notes
S2-06	Load rejection to auxiliary power	R, K B	A	Additional boundary condition: With and without switch-over to offsite power supply.
S2-07	Loss of a main feedwater pump without connection of standby pump	R, K	A-B	
S2-08	Loss of all main feedwater pumps with and without connection of standby pump	R, K	A-B	
Change of flow rate in the reactor coolant system				
S2-09	Loss of individual / several / all reactor re-circulation pumps	R, K	A-B	Additional boundary condition: Effect on neutron-physical thermal hydraulic stability of the core has to be considered.
Increase of reactor coolant inventory				
S2-10	Malfunction in the coolant level control or removal of excess water or inadvertent in-jection 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 a train of the emergency core cooling systems	- - -	D	Additional boundary condition: - Relevant for procedures. - Only relevant in operating phase D due to overfilling of reactor pressure vessel in case of not installed reactor cavity seal liner. Specification of the acceptance criteria:

No.	Events BWR	Fundamental safety functions	Operating phase	Additionally considered comments, boundary conditions and notes
				Ensuring coolant inventory in the long term.
Decrease of reactor coolant inventory				
S2-12	Leakage from RPV bottom resulting from maintenance work	K	E	Note: - Relevant for procedures. - Limit: leakage can be overfed by operational systems.
Loss of residual heat removal				
S2-13	Loss of a train, in operation or in demand, of the residual-heat removal system	K, B	C-E	Additional boundary condition: Single failure is not postulated.
S2-14	Shutdown of all active 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 the most effective control ele-	R, K	A, C, E	

No.	Events BWR	Fundamental safety functions	Operating phase	Additionally considered comments, boundary conditions and notes
	ment group			
S2-16	Inadvertent fast rod insertion or inadvertent insertion of a control rod	R, K	A	
S2-17	Inadvertent insertion of all control rods 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: Effect on neutron-physical thermal hydraulic stability of the core has to be considered.
S2-19	Malfunction in the reactor power control	R, K	A	

No.	Events BWR	Fundamental safety functions	Operating phase	Additionally considered comments, boundary conditions and notes
S2-20	Most unfavourable misloading of the most reactive fuel assembly	R, K	E, A	Additional boundary conditions: Reactor startup with misloaded fuel assembly shall be analysed regarding fundamental safety function K in operating phase A.. Comment: - Fundamental safety function R (subcriticality) in operating phase E - Fundamental safety function K in operating phase A
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 for 10 hours or less	R, K, B	A-E	Additional boundary condition: The restoration of the external power supply also has to be analysed.
Level of defence 3				
Level of defence 3a				

No.	Events BWR	Fundamental safety functions	Operating phase	Additionally considered comments, boundary conditions and notes
Main-steam or feedwater-side change of heat removal				
S3a-01	Major malfunction in the main steam system or in the feedwater supply system which leads to a temperature or pressure decrease in the reactor coolant system.	R, K	A-B	Note: In contrast to S2-01, in this case simultaneous inadvertent opening of several valves, e.g. inadvertent complete opening of main-steam bypass station, inadvertent opening of safety and relief valves.
S3a-02	Major malfunction in the main steam system or in the feedwater supply system which leads to a 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.
S3a-03	Loss of all main feedwater pumps without addition of standby pump	R, K	A	Additional boundary condition: In contrast to event S2-08, here with consideration of the single failure criterion
Increase of reactor coolant inventory				
S3a-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: In contrast to event S2-10, here with consideration of the single failure criterion.

No.	Events BWR	Fundamental safety functions	Operating phase	Additionally considered comments, boundary conditions and notes
Loss of residual-heat removal				
S3a-05	Loss of a train, in operation or in demand, of the residual-heat removal system	K, B	C-E	Additional boundary condition: In contrast to event S2-13, here with consideration of the single failure criterion
S3a-06	Shutdown of all residual-heat removal trains due to pressure increase or coolant level decrease	K, B	C-D	Additional boundary condition: In contrast to event S2-14, here with consideration of the single failure criterion
Change of reactivity and power distribution				
S3a-07	Inadvertent reactivity insertion due to loss of high-pressure preheater and unavailability of limitation systems	R, K	A	
S3a-08	Withdrawal of the most effective control element or control element group with loss of limitation systems	R, K	A, B, D	
S3a-09	Ejection of the most effective control rod	R, K	A	

No.	Events BWR	Fundamental safety functions	Operating phase	Additionally considered comments, boundary conditions and notes
S3a-10	Drop out of the most effective control rod	R, K	A	Additional boundary condition: Drop out over the length of a latch distance.
S3a-11	Drop of a fuel assembly into the reactor core during refueling	R, K	E	
S3a-12	Drop of a fuel assembly onto the reactor core	R	E	Additional boundary condition: Verification of subcriticality for fuel assembly on the core.
S3a-13	Inadvertent withdrawal of control rods during loading	R, K	E	
S3a-14	Inadvertent withdrawal of a control rod during zero-power test or shutdown safety test	R, K	C, E	
S3a-15	Misloading of the reactor core with more than one fuel assembly	R	E	
S3a-16	Nuclear-thermal hydraulic instability	R, K	A	Additional boundary condition: The boundary conditions of the possible initiating events have to be considered. Without consideration of limiting measures. In-phase and out-of-phase oscillations have to be analysed. The effectiveness of reactor protection actions for the timely detection of neutron flux oscillations and reactor shutdown has to be demonstrated.
S3a-17	Inadvertent speed increase of the reactor	R, K	A	Additional boundary condition: Increase of pump speed from minimum speed with maximum speed gra-

No.	Events BWR	Fundamental safety functions	Operating phase	Additionally considered comments, boundary conditions and notes
	recirculation pumps			dient without limitations.
Loss of coolant within the containment, not isolable				
S3a-18	Leak/break within the containment (leak cross section ≤ 0.1 A of the respective line considered)	R, K, B, S	A-B	<u>Additional boundary condition:</u> In-addition to main steam and feedwater lines, all other coolant-retaining systems shall be considered.
S3a-19	Leak/break within the containment (leak cross section > 0.1 A of the respective line considered)	R, K, B, S	A-B	Additional boundary control: In-addition to main steam and feedwater lines, all other coolant-retaining systems shall be considered. The double-ended break of the main-steam line (2A break) has to be analysed for the design of the pressure suppression system, the reactor pressure vessel internals necessary for cooldown and core cooling, as well as the pressure design of the containment and the accident resistance of all safety-relevant systems and components necessary for accident control.
S3a-20	80 cm^2 leak in RPV bottom	R, K, B, S	A-B	
S3a-21	Leak due to faulty maintenance or switching failures at the reactor coolant system	K	C-E	<u>Additional boundary condition:</u> A maximum leak resulting from faulty maintenance or switching failures is postulated. The leak size is determined by the largest free cross section in the lines connected with the reactor coolant system The analysis considers that in case of an incident a fuel assembly is

No.	Events BWR	Fundamental safety functions	Operating phase	Additionally considered comments, boundary conditions and notes
				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).
S3a-22	Leak in the reactor cavity seal liner	K, S	D-E	Additional boundary condition: The constructively possible leak cross section in case of seal failure is postulated. Note: Relevant for establishment of the sump function and procedures.
S3a-23	Leak in RPV bottom due to - inadvertent pulling of a pump shaft, or - work on control rod drives or detector assemblies	K, S	E	Note: Where applicable, temporary requirement for the sump function of the containment until reliable function of the isolating equipment has been verified (locks included).
S3a-24	Leak in the blow-off pipe of a safety and relief valve within the gas space of the pressure suppression pool	K, B, S	A-B	

No.	Events BWR	Fundamental safety functions	Operating phase	Additionally considered comments, boundary conditions and notes
Loss of coolant outside the containment				
S3a-25	Leak/break in the main steam or feedwater system and other high-energy piping systems between containment and first isolation possibility outside the containment	R, K, B, S	A-B	Additional boundary condition: Special consideration of: the integrity of the containment, humidity, pressure build-up, differential pressures, temperature, jet and reaction forces, etc. with impacts affecting more than one redundancy, and the integrity of safety-relevant structures of the reactor building.
S3a-26	Leak/break in the main steam or feedwater system within the turbine building	R, K, B, S	A-B	
S3a-27	Leak/break in an instrumentation line carrying coolant, in the reactor building	S	A-C	Additional boundary condition: 2A break of an instrumentation line in the reactor building that cannot be isolated for 30 min. The most unfavourable operating phase is analysed with regard to radiology (spiking effect).
S3a-28	Leak/break in the reactor water cleanup system in the reactor building	S	A-E	Additional boundary condition: The Spiking-effect shall be considered.
S3a-29	Leak/break in coolers, carrying reactor coolant, in case of demand	B, S	A-E	

No.	Events BWR	Fundamental safety functions	Operating phase	Additionally considered comments, boundary conditions and notes
S3a-30	Leakage from the wetwell	K	A-B	Additional boundary condition: The event is relevant for the transition to residual-heat removal via RHR train from RPV and flooding of reactor building
S3a-31	Leak/break in reactor scram system in the reactor building	R	A	Note: Relevant for the design of the reactor scram system.
S3a-32	Leak in residual-heat removal system in the reactor building during residual-heat removal operation	K, B, S	C-E	Additional boundary condition: - The Spiking-effect shall be considered.
S3a-33	Loss of coolant from the containment via systems connected to the reactor coolant pressure boundary	K, B, S	A-C	
Release of radioactive material from nuclear auxiliary systems				
S3a-34	Leak/break in a pipe or break of a filter in the off-gas or gas treatment system	S	A-F	
S3a-35	Leak in container with active medium	S	A-F	Note: – The container with the largest radiological hazard potential shall be identified. – Analysis also has to cover container failure due to earthquake.

No.	Events BWR	Fundamental safety functions	Operating phase	Additionally considered comments, boundary conditions and notes
Loss of energy supply				
S3a-36	Longterm loss of offsite power (> 10 hours)	R, K, B, S	A-E	Additional boundary condition: Cooldown under emergency power conditions also has to be analysed.
Internal event				
S3a-37	Potential activity release as a result of internal fires (including filter fires) or explosions	S	A-F	Additional boundary condition: Fires and explosions on components and in system areas with great activity release potential have to be analysed.
S3a-38	Break of a control rod nozzle with control rod 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 rod does not lead to an impermissible damage of the containment. Further, it shall be demonstrated that no consequential damages of neighbouring drives occur that impair the functional safety of other control rods. If consequential damage cannot be excluded, it shall be demonstrated that the acceptance criteria are also fulfilled.

No.	Events BWR	Fundamental safety functions	Operating phase	Additionally considered comments, boundary conditions and notes
Level of defence 3b				
Anticipated transient without scram (ATWS)				
S3b-01	Loss of main heat sink, e.g. by loss of condenser vacuum or closure of the main steam bypass valve with available house load supply.	R, K, B	A	Note: For ATWS it is postulated that the nut follow-up movement (if available) for the control rods is effective.
S3b-02	Loss of main heat sink with unavailable house load supply	R, K, B	A	
S3b-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	
S3b-04	Total loss of main feedwater supply	R, K, B	A	

No.	Events BWR	Fundamental safety functions	Operating phase	Additionally considered comments, boundary conditions and notes
S3b-05	Maximum reactivity insertion by withdrawal of control rods or control element rods on the basis of the operating conditions “full load” and “hot zero power condition”	R, K, B	A	
S3b-06	Maximum decrease of the feedwater temperature.	R, K, B	A	
S3b-07	Steam line isolation with available house load supply	R, K, B	A	
S3b-08	Steam line isolation with unavailable house load supply	R, K, B	A	
S3b-09	Maximum increase of feedwater flow rate	R, K, B	A	
S3b-10	Startup of the recirculation pumps with maximum speed gradient	R, K, B	A	
Loss of energy supply				
S3b-11	Loss of offsite power cumulated with the failure of all emergency diesel generators	R, K, B	A-F	Additional boundary condition: DC power supply and back-up AC power supply available

No.	Events BWR	Fundamental safety functions	Operating phase	Additionally considered comments, boundary conditions and notes
S3b-12	Loss of offsite power and all onsite AC power sources	R, K, B	A-F	Additional boundary condition: DC power supply available
Loss of component cooling				
S3b-13	Loss of component cooling water system	R, K, B	A-F	
Loss of coolant accidents				
S3b-14	Small break loss of coolant accident and simultaneous loss of the component cooling water system/essential service water	R, K, B	A	
S3b-15	Loss-of-coolant accident with failure to shut off emergency cooling after flooding of the core and failure of steam line isolation	R, K, B	A	
Loss of residual-heat removal				
S3b-16	Transient with simultaneous complete loss of emergency cooling	R, K, B	A	

Table 4-3 Event list spent fuel pool of pressurized water reactors (PWR) and boiling water reactors (BWR)

No.	Events spent fuel pool of PWR and BWR	Fundamental safety functions	Operating phase	Additionally considered comments, boundary conditions and notes
Level of defence 2				
Reduced heat removal from the fuel pool				
B2-01	Loss of a train in operation or unplanned short-term (max. 30 min) interruption of heat removal	K	A-F	
Loss of coolant from fuel pool				
B2-02	Leakage from the spent fuel pool or loss of water from via connecting pipes (corresponding as a maximum to a cross-sectional area of NB25)	K	A-F	
Loss of Energy supply				
B2-03	Loss of offsite power for 10 hours or less	K	A-F	
Reactivity changes in the fuel pool				
B2-03	Disturbances in the boron concentration	R	A-F	

No.	Events spent fuel pool of PWR and BWR	Fundamental safety functions	Operating phase	Additionally considered comments, boundary conditions and notes	
B2-04	Most unfavourable misloading of the fuel pool or transport and storage cask with a most reactive fuel assembly	R	A-F		
Level of defence 3					
Level of defence 3a					
Reduced heat removal from the fuel pool					
B3a-01	Loss of two trains of the fuel pool cooling system for a longer period (> 30 min.)	K	A-F		Additional boundary condition: For the safety demonstrations, grace times and repair possibilities can be taken into account.
Loss of coolant from fuel pool					
B3a-02	Loss of coolant from the spent fuel pool throgh leaks in the pool or via connecting pipes (corresponding to a cross-sectional area of > NB25)	K, B	A-F		Additional boundary condition: Maximum leak cross-sectional area: area of the largest connecting pipe.
B3a-03	Leak in the reactor cavity or the setdown pond for steam separators at opened re fueling slot gate	K, B	E		Additional boundary condition: Effects of leaks that may occur in the reactor coolant system during refuelling also have to be considered.

No.	Events spent fuel pool of PWR and BWR	Fundamental safety functions	Operating phase	Additionally considered comments, boundary conditions and notes	
B3a-05	Internal leak in heat exchangers of the fuel pool carrying coolant	K, B, S	A-F		
B3a-06	small leak loss of coolant accident in external systems (up to 50 mm diameter)	B,S	A-F		
Reactivity changes in the fuel pool					
B3a-07	Water/steam ingress in the spent fuel dry storage facility	R	A-F		Specification of the demonstration criteria $k_{eff} < 0.98$
B3a-08	Geometry changes due to earthquake (fuel pool, spent-fuel dry storage facility)	R, K, B	A-F		
B3a-09	Drop of a fuel assembly into the 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.	Events spent fuel pool of PWR and BWR	Fundamental safety functions	Operating phase	Additionally considered comments, boundary conditions and notes	
B3a-10	Misloading of the fuel pool or the transport and storage cask with more than one fuel assembly	R	A-F		
B3a-11	Boron dilution in the fuel pool	R	A-F		
Events during handling and storage of fuel assemblies and heavy loads					
B3a-12	Fuel assembly damage during handling	S	A-F		Additional boundary condition: Damage of all fuel rods at exterior side of a fuel assembly is postulated. Note: The analysis serves to verify that the release into the environment resulting from the release of radionuclides in the containment without loss of coolant is sufficiently limited.
Loss of energy supply					
B3a-13	Long term loss of offsite power (> 10 h)	R, K, B	A-F		

No.	Events spent fuel pool of PWR and BWR	Fundamental safety functions	Operating phase	Additionally considered comments, boundary conditions and notes	
Level of defence 3b					
B3b-01	total loss of the spent fuel pool cooling system	S	A-F		
B3b-02	Loss of offsite power cumulated with the failure of all emergency diesel generators	R, K, B	A-F		Additional boundary condition: DC power supply and back-up AC power supply available
B3b-03	Loss of offsite power and all onsite AC power sources	R, K, B	A-F		Additional boundary condition: DC power supply available

Annex 2
Requirements for provisions and protection against hazards
19.3.2015

Contents

1 Basic Requirements on Protection Concepts for Plant Internal and External Hazards

1 (1) All items required for safe shutdown of the nuclear reactor, for maintaining it in a shutdown state, for removing residual heat or for prevention of the release of radioactive materials shall be designed such and constantly kept in such a condition that they can fulfil their safety related tasks even in case of any internal hazard or relevant site specific external hazards.

Note: Requirements for these items important to safety to be considered with regard to malevolent disruptive acts or other third party intervention are not covered by the "Dutch Safety Requirements for Nuclear Reactors".

A site specific hazard analysis shall be performed to develop a hazard curve for each external hazard. The hazard assessment shall take due account of the uncertainties involved in the analyses.

1 (2) Items important to safety shall be designed and located, considering other safety implications, to limit their exposure to hazards and possible harmful consequences of their failures.

Preventive and mitigative measures shall be possible even in case of internal and external hazards.

1 (3) The design of systems, structures and components against internal and external hazards shall be based on

a) those natural hazards with the most severe consequences or other external hazards to be postulated at the site under consideration;

b) the special characteristics of external hazards of long duration;

c) combinations of several natural or human induced external hazards (e.g. earthquake, flooding, storm, lightning, fire, human induced hazards) or combinations of these hazards with plant internal events (e.g. pipe break, loss of offsite power) or internal hazards (e.g. internal fires, internal flooding). These combinations shall be considered if the com-

bined events or hazards show a causal relationship or if their simultaneous occurrence has to be assumed according to its probability and the expected degree of damage.

1 (4) Preventive measures shall ensure that internal or external hazards inadmissibly impairing the required function of items important to safety shall be,

- either reliably prevented
- or sufficiently limited in their effects (see “Dutch Safety Requirements for Nuclear Reactors“ 2.1 (5))

1 (5) The effectiveness and reliability of a preventive measure shall be commensurate to the occurrence frequency and the potential effects of the hazard against which the respective measure provides protection.

1 (6) If preventive measures as described in Sections 3 and 4 are in place, analyses of event sequences due to the corresponding internal and external hazards are not required in general. In this case, the safety demonstration focuses on compliance with the requirements for effectiveness and reliability of the preventive measures.

However, the requirements according to Annex 1 of the “Dutch Safety Requirements for Nuclear Reactors” do apply for analyses of event sequences that have to be postulated notwithstanding existing preventive measures and for event sequences for which preventive measures only limit the effects according to 1 (3) .

1 (7) Radiological consequences shall be determined for hazards originating from internal and / or external hazards leading to a radiological representative event at levels 3 or 4 of defence in depth.

Note: Radiological representative events on level 3 of defence-in-depth are listed in Annex 1 of the “Dutch Safety Requirements for Nuclear Reactors”.

1 (8) In case the control room is not operable as a result of internal and/or external hazards, it shall be ensured that the plant is brought into a controlled condition without any manual intervention and can remain in this condition

for at least 10 hours. Moreover, the plant shall be brought into a condition which ensures subsequent residual heat removal in the long-term. Measures need not be automated if sufficient lead time is available or administrative measures are in place for their actuation. For long-term control of emergency conditions resulting from internal and/or external hazards on-site supporting measures can be taken.

In case that the control room is not operable, a supplementary control room shall be available according to Section 3.8 of the “Dutch Safety Requirements for Nuclear Reactors”.

1 (9) For items important to safety necessary for the control of event sequences due to external hazards the following requirements do apply:

a) Components and sub-systems shall be protected against the postulated external hazards.

b) The required function shall not be inadmissibly impaired by damage in plant areas which are not protected against the hazard under consideration. This does not apply only to mechanical systems and components but also to energy supply systems and I&C equipment.

c) Unauthorised interventions or operating errors in the control room or in other plant areas which are not specifically protected shall not lead to any inadmissible impact on the required function.

1 (10) In case of external hazards cooling of the fuel assemblies in the core and in the spent fuel pool shall be ensured in the long-term. Maintenance and repair measures at those items important to safety required in the long-term, shall be performed in due time, if required.

The accessibility of areas where operations might have to be performed shall be ensured as well as the communication with the personnel working in these areas.

2 Requirements for Preventive Measures

2 (1) Reliability and effectiveness of preventive measures shall be such that the requirements according to subsection 1 (2) are met.

2 (2) Preventive measures shall be mainly based on passive means. If inadmissible consequences cannot be reliably prevented by passive means, reliable active measures shall be provided. If administrative measures are taken, their reliability shall be demonstrated according to Subsection 2 (6). If preventive measures are exclusively based on administrative measures, their reliability shall be thoroughly justified.

2 (3) The effectiveness of preventive measures shall be ensured even if the single failure concept is applied (see Annex 3 of the “Dutch Safety Requirements for Nuclear Reactors”).

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

2 (5) Postulated malfunction of or damage to preventive measures as well as their faulty operation or human error in the execution of preventive measures shall not impair the operability of items important to safety.

2 (6) If administrative measures and related operator actions are part of preventive 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 execution and check of preventive measures. The personnel responsible for the performance and checking of preventive measures shall be specifically qualified in accordance with the safety significance of the preventive measures.

- Distinct procedures and instructions for execution and check of preventive measures shall be in place. Type and number of the checks shall be defined in accordance with requirements regarding reliability of the respective preventive measure. Distinct, measurable and quantifiable criteria shall be specified for the check. Anysafety implications of identified deviations from these requirements shall be assessed.

- The performance of the verification and the results achieved shall be fully documented. The persons involved shall be nominated.

- Sufficient time for the performance and checking of preventive measures shall be available.

- The environmental conditions shall not impair the performance and checking of the preventive measures.

- The boundary conditions under which the persons in charge perform the measures shall be such that the prerequisites for failure-free behaviour are ensured to the extent possible. Ergonomic criteria shall be considered. Potential failures and their consequences shall be considered in the training of the personnel.

2 (7) Validity of the boundary conditions for the efficiency and reliability of preventive measures has to be ensured over the whole operational life of the plant.

3 Requirements for Internal Hazards

3.1 Basic Requirements

3.1 (1) Plant specifically postulated internal hazards and their possible combinations or their combinations with other external hazards that may occur due to the plant-specific conditions shall be fully considered.

Note: Sections 2.5 and 4.2 of the "Dutch Safety Requirements for Nuclear Reactors" and subsections 3.2.1 (3) and (4) in Annex 4 of the "Dutch Safety Requirements for Nuclear Reactors" shall be considered.

3.1 (2) For each hazard or combination of hazards according to subsection 3.1 (1), the safety related impacts on the plant 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 level,
- 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.
- Collapse of structures and non-structural elements

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

3.1 (4) Adequate protection features and/or measures 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 Hazard Specific Requirements

3.2.1 Plant Internal Fire

3.2.1 (1) Protection features and/or measures for the protection against internal fires and their consequences shall both be provided 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 shall be planned and implemented such that defence in depth is realised:

- Appropriate protection features and/or measures shall be in place to prevent the occurrence of incipient fires.
- Fires which have nevertheless occurred shall be quickly detected and extinguished.
- The propagation of any fire neither extinguished nor self-extinguished shall be limited.

3.2.1 (3) A fire protection concept/strategy 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/strategy shall be assessed and, if necessary, enhanced.

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 feature and/or measure 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 and in case of any incident to be assumed (incl. 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 needed for plant operation fire loads, which cannot be avoided due to plant operational reasons, shall be sufficiently physically separated from these ignition sources at any location, where permitted by design and the requirements for 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) Items of the redundant safety trains shall be separated by sufficiently rated fire barriers to exclude 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 features and/or measures 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. This excludes control and lubrication fluids as well as other combustible materials unavoidable for operational reasons.

3.2.1 (13) In principle, wires and cables shall be routed separated from heated pipes or pipes carrying combustible media. In principle, power cables shall be sufficiently separated from signal and control cables.

In case of unavoidable crossings of instrumentation and control wires and cables with pipes or pipes carrying combustible media or with power cables, particular protection features and/or measures shall be in place.

Adequate protection features and / or measures shall ensure that special measures and / or items important to safety shall ensure that even in case of fire cables for power supply or instrumentation and control 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 case of fire, particularly in plant areas with items important to safety and in controlled areas, adequate protection features and/or measures 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) Escape and rescue routes shall be provided within the buildings. These shall be protected against fire effects for an appropriate time period allowed for self-rescue, rescue of persons, fire extinguishing as well as for personnel actions required for safety reasons.

3.2.1 (18) 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 (19) 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 impair the required func-

tion of items of the safety trains nor of structural elements for physical separation of fire compartments.

3.2.1 (20) 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 (21) 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 (22) It shall be ensured that all measures required for controlling postulated single initiating events, postulated multiple failure events and postulated core melt accidents can also be taken in case of fire suppression.

3.2.2 Plant Internal Flooding

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

- High quality design of the medium containing components,
- Precise specifications for maintenance measures on medium containing components, in particular those with high flooding potential,
- High reliability of stationary automatic fire extinguishing systems with respect to inadvertent/spurious 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 hitting of loads, start-up of systems after maintenance measures or plant modifications with isolation devices inad-

vertently not installed). It is possible to define an enveloping hazard as design basis for protection means.

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 the 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 shall be provided. 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. retention ponds, barriers) around items important to safety,
- Guard pipe (i.e. concentric pipe-in-pipe system) design,

- Bars or equivalent installations for preventing spread of water, in particular into adjacent redundant trains,
- Active or passive drainage features,
- Organisational means in case of a flooding event.

3.2.2 (10) If maintenance measures are performed on means for prevention of flooding hazards, their function shall either be ensured during the maintenance period or fully compensated by other measures.

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 items important to safety cannot be prevented, precautions shall be provided for the protection of these items important to safety.

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

3.2.3 (3) The required function of items important to safety shall be ensured in case of impacts resulting from a postulated component failure, e.g.:

- Direct mechanical impacts (reaction forces, whipping pipes),

- High energy fragments,
- Jet forces,
- Internal flooding,
- Increased humidity,
- Physical or chemical impacts,
- Pressure differences (static and dynamic)
- Increased or decreased 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 these hazards.

3.2.3 (5) The following protection features and/or measures 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 items important to safety identified as potential targets of fragments,
- Selection of building arrangement such that items important to safety are 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 items important for safety due to pipe whip shall be prevented by structural means for the pipes.

3.2.3 (7) If safety-relevant impacts are to be postulated in case of failure of rotating components,

- Reliable items important to safety for limiting the speed and
- Vibration monitoring for identification of damages (initiated by unbalances)

shall be provided.

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

3.2.3 (9) Structural means 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 provisions during impact of the high energy fragments.

3.2.3 (10) In case of a postulated double-ended rupture of a high energy pipe , measures for the protection against impacts on items important to safety caused by jet and reaction forces shall be taken under consideration of 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 impacts in case of impact on other components.

3.2.4 Leak/break in main steam or feedwater system and other high-energy piping systems in the annulus and in the valve compartments (pressur-

ized water reactor) and between containment and first isolation possibility outside the containment (boiling water reactor).

3.2.4 (1) The impacts of leaks

- in the annulus and in the valve compartments (pressurized water reactor) in piping systems carrying main steam or feedwater,
- in the area between containment and the first external isolation possibility (boiling water reactor) in piping systems carrying main steam or feedwater,
- in a steam generator blowdown line (pressurized water reactor),
- on another high-energy pipe

shall not lead to impairment of the containment, including the penetrations, as well as of items important to safety in the area between containment and the reactor building (annulus) and the valve compartments (pressurized water reactor).

3.2.4 (2) Inadmissible impacts shall be prevented by appropriate design of the pipes in this area.

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 safely prevented.

3.2.6 Electromagnetic Interferences

3.2.6.1 Protection against electromagnetic interference.

3.2.6.1 (1) Items important to safety shall be reliable effective in their electromagnetic environment.

3.2.6.1 (2) The electromagnetic compatibility shall be demonstrated by analysis. It comprises the electromagnetic interference radiation, the disturbance resistance of the components, the own disturbance resistance and the necessary tests.

3.2.6.1 (3) During the lifecycle of the plant, both the presence of new sources and the change of existing sources of interference shall be monitored and analysed. The protection of items important to safety against electromagnetic interferences shall be adapted to changed environmental conditions, if 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 influence on the items important to safety cannot be precluded, shall be identified and possible influences from these sources shall be assessed. Enveloping (Covering) sources of interference shall be analysed to the extent possible. The environmental conditions resulting by operation of the electromagnetic interference sources shall be determined at the location of items important to safety.

3.2.6.2 (2) Electromagnetic interference shall be limited such that proper functioning of the electrical installations important to safety is ensured.

3.2.6.2 (3) For limitation of electromagnetic influences from plant internal sources, the administrative and technical measures shall be provided for protection instrumentation and control equipment according to their safety significance (e.g. shielding, decoupling, grounding, physical separation).

3.2.6.2 (4) Temporarily existing potential sources of electromagnetic interference, as for example 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 items with regard to the protection against inadmissible electromagnetic impacts

3.2.6.3 (1) Items important to safety shall be qualified with regard to the protection against inadmissible electromagnetic impacts.

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

3.2.7 (1) Safety related systems, structures and components at the plant site 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 Mutual influence between multi-unit plants and neighbouring plants

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 function of plant components important to safety shall be ensured by suitable protection means for explosion protection.

3.2.9.1 (2) Appropriate protection features and / or measures inside and outside of buildings shall be provided for the prevention of chemical explosions, ex-

plosions of steam-gas mixtures and physical explosions as far as the initiating materials are stored or handled in the area of the plant in relevant amounts or if they can be produced there.

3.2.9.1 (3) The explosion protection procedures shall be planned and designed such that defence in depth is realised. The items important to safety and procedures shall

- prevent the generation of an explosive gas mixture,
- prevent the ignition of an explosive atmosphere generated 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 formation of explosive gas mixtures cannot be safely prevented, protection features and/or measures shall be provided to ensure that items important to safety are not inadmissibly impaired. These include:

- Minimization of the amounts of explosive gas mixtures
- Eliminating all potential ignition sources, encapsulation of ignition sources, if necessary, (exception: items important to safety for reduction of explosive gas mixtures),
- Adequate ventilation, and
- Use of features 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 appropriate and reliable protection features and/or measures, e.g.:

- Pressure relief systems,
- Compliance with safety distances to items important to safety, and
- Protective measures such as (sealing) walls.

3.2.9.1 (6) All postulated explosions shall be assessed regarding their impacts on items important to safety.

3.2.9.1 (7) If it is necessary to keep explosive materials available on the plant site, the following principles shall be applied:

- The amount of explosive materials shall be minimized.
- Proper storage shall be ensured.
- Sufficient distance to potential ignition sources shall be kept.
- Fire and gas alarm systems and automatic extinguishing systems shall be provided at the storage location.

3.2.9.1 (8) Pressure waves not resulting from an explosion shall also be considered.

Note: These are, for example, pressure waves resulting from electric arcs in medium and high voltage switchgears/breakers.

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

Note: The following criteria 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 provided.

3.2.9.2 (2) The protection means to be provided 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 modes, 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.

3.2.9.3 (4) If radiolysis gas accumulations cannot be excluded for process related reasons, enveloping radiolysis gas accumulations and reactions shall be postulated for the determination of precautions to be taken. The reaction pres-

sure and the impacts on items important to safety by fragments and blast waves as well as by loss of coolant, jet forces, increased radiation level, reaction forces, temperature and humidity shall be determined.

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

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

Prevention of explosive hydrogen mixtures in the containment

3.2.9.2.1 General Requirements

3.2.9.3.1 (1) A measuring system shall be available which ensures reliable determination of the hydrogen distribution within the primarily loaded areas of the containment even under the conditions to be expected after a loss-of-coolant accident.

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

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

3.2.9.2.2 Prevention of explosive hydrogen mixtures in the containment after loss-of-coolant accidents

3.2.9.3.2 (1) The following principles apply to protection features and / or measures for the 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 areas of the containment, items important to safety shall be provided which ensure sufficient forced flow mixing of the containment atmosphere.

– If the calculation of the integral hydrogen concentration reveals that reaching the ignition limit cannot be excluded in the long-term without hydrogen removal procedures, the following shall apply:

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

(ii) The design of the recombiners shall ensure the reliable availability and operability even under the conditions prevailing within the containment at the moment of necessary activation. It shall be demonstrated that the fission product load of the recombiners determined under conservative boundary conditions will not unduly impair their function under radiological aspects and aspects important to safety by airborne halogens and volatile solids and the resulting 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 rooms outside of 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 undue radioactive releases through possible leaks. The pipes shall be shielded accordingly.

3.2.9.3.2 (2) It shall be possible to put active measures in place before a postulated hydrogen concentration of 4 % volume content has been reached.

3.2.9.3.2 (3) Flushing of the containment (injection and discharge from the containment) shall not be planned for the reduction of the integral hydrogen concentration.

4 Requirements for External Hazards

4.1 Basic Requirements

4.1 (1) The site specific external natural as well as human induced hazards shall be identified, monitored and checked regularly for any possible change. The hazard assessment shall be based on all relevant site and regional data. Particular attention shall be given to extending the data available to include beyond recorded and historical data.

Note: See on this point also Sections 2.5 and 4.2 in the "Dutch Safety Requirements for Nuclear Reactors" as well as Subsections 3.2.1 (3) and (4) in Annex 4 of the "Dutch Safety Requirements for Nuclear Reactors".

4.1 (2) It shall be ensured that all hazards identified according to subsection 4.1 (1) are included in the analysis. State-of-the-art methods shall be used for this analysis. If one hazard also covers other hazards, this shall be clearly indicated. Following a change of the protection measures for a covering hazard, the covering character of the protection measures shall be re-evaluated.

4.1 (3) Based on the site specific hazard assessment, design basis events associated with an exceedance probabilitiy of 10^{-4} 1/a shall be defined. The relevant load and engineering parameters associated with these design basis events shall be clearly specified. Consideration shall be given to the fact that one hazard might involve different types of loads acting at the same time (e. g. high water levels and mechanical loads due to wave action).

4.1 (4) A protection concept shall be established to provide a basis for the design of suitable permanent protection measures. 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 pres-

sure wave brought on by the bursting of vessels with high energy content in the turbine building during an earthquake).

4.1 (5) The protection concept provided for external hazards shall be documented in reviewable form. The documentation shall be kept up to date. The documentation shall contain at least a list of the hazards considered as well as the proof of the suitability and sufficient reliability of the protection measures.

4.1 (6) External hazards and resulting loads shall generally be combined with the specified permanent and variable loads acting on the respective plant components. For temporary loads and plant states that do not reoccur often, this approach need not necessarily be followed unless their simultaneous occurrence has to be postulated according to its probability and the expected extent of damage.

4.1 (7) It shall be ensured that external hazards do not impair access to the plant.

4.1 (8) It shall be ensured that external hazards do not impair access to safety related buildings and the feasibility of safety-relevant measures, 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 of the further development of the parameters relevant for safety shall be monitored and considered with foresight (e.g. water level and temperature of the ultimate heat sink).

4.1 (10) If applicable, limit values and intervention values (preceding the limit values) shall be defined, an exceedance of which will trigger the timely initiation of safety related measures.

4.1 (11) Following a hazard that has caused the exceedance of an intervention value, it shall be checked whether any inadmissible consequences for items important to safety have occurred.

4.1 (12) During hazards of long duration, safety related checks 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 loads shall be determined for the site based on site specific deterministic and probabilistic seismic hazard assessments. 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 assessment, at least a peak ground acceleration of 0.1g in combination with a generic response spectrum (according to IAEA NS-G-1.6) has to be applied as a design basis.

4.2.1.1 (2) All items important to safety shall be designed and remain lastingly in such a condition that they will fulfil the necessary safety functions during and after a design basis earthquake.

4.2.1.1 (3) Apart from the vibratory excitation of plant structures, systems and components, changes in the subsoil, (e.g. soil liquefaction or subsidence) have to be considered.

4.2.1.1 (4) The design of the plant shall ensure that the failure of items not designed against earthquakes will not have any inadmissible effects on items important to safety that are needed for controlling the design basis earthquake and its effects, i.e. that the required effectiveness and reliability of these items important to safety remains ensured.

Note: Regarding the consequential events to be considered in connection with the design earthquake, see in particular the events D3a-45, S3a36, B3a-07 in Annex 1 of the "Dutch Safety Requirements for Nuclear Reactors".

4.2.1.1 (5) For the reactor coolant pressure boundary and for the external systems that are needed to fulfil fundamental safety functions, the behaviour during the design basis earthquake shall be assessed by means of a structure-dynamics analysis. The availability of the fundamental safety functions shall be demonstrated. A simultaneous occurrence of a design basis earthquake and a leak in the pressure boundary need not be assumed due to design and implementation of the pressure boundary. A simultaneous occurrence of a leak in external systems need not be assumed if these are designed to withstand earthquake loads.

4.2.1.1 (6) Demonstrating that long-term sub-criticality is ensured after a design basis earthquake, it is acceptable in the case of pressurized water reactors to factor in not only borating systems with seismic design but also the effectiveness of the reactor scram system. In this 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 3 of defence in depth are met.

Note: For safety objectives of level of defence 3 see "Dutch Safety Requirements for Nuclear Reactors" paragraph 2.5 (1).

4.2.1.1 (8) Seismic instrumentation shall be installed by 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. It 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, examination of the plant condition) shall be initiated. It

shall be ensured that the operating personnel has access to the relevant values from the seismic instrumentation and that there is a corresponding alarm if the defined limit values are exceeded.

4.2.1.2External Flooding

4.2.1.2 (1) The possible causes of external flooding shall be determined site specifically. For flooding hazards a design basis flood shall be defined. Furthermore, heavy rainfall hazards at the plant site shall be considered.

A suitable meteorological and hydrological model shall be developed with account taken of all known past changes in relevant characteristics of the region. From this model the hazards for the site due to flooding shall be derived.

4.2.1.2 (2) External flooding shall not inadmissibly impair the safety of the plant. The functional performance of items important to safety and the efficiency of items important to safety shall be ensured.

4.2.1.2 (3) Permanent protection measures shall be used for flood control, taking the regulations in Subsections 4.1 (3) and 4.1 (4) into consideration.

4.2.1.2 (4) Apart from the static impact by water pressure, possible dynamic effects (e.g. wave action or impact of flotsam) shall also be considered.

4.2.1.2 (5) high water levels of long duration shall also be considered.

4.2.1.2 (6) The potential for instability of the coastal area or river channel due to erosion or sedimentation shall be investigated.

4.2.1.3Extreme meteorological conditions

4.2.1.3 (1) Depending on the site specific conditions, in particular the following extreme meteorological conditions shall be considered:

- high or low ambient air or cooling water temperatures,

- droughts of long duration and their effects on cooling water supply,
- storms including tornados,
- high or low atmospheric humidity,
- snowfall,
- icing,
- heavy rainfall, hail,
- lightning,
- 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) It shall be ensured by suitable protection measures 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 values are exceeded.

4.2.1.3 (4) Suitable protection measures shall be provided in particular against icing in the area of safety related systems, structures, and components such as circulating water intake, ventilation systems, or main-steam relief valves.

4.2.1.3 (5) Regarding the protection against storms, in particular the following aspects shall be considered:

- wind speed,
- gustiness,
- suction effects,
- duration of the event,
- interaction of adjacent structures,

– wind-related water levels in nearby water bodies (in particular the ultimate heat sink).

The hazards associated with tornadoes shall be derived and expressed in terms of parameters such as rotational wind speed, translational wind speed, radius of maximum rotational wind speed, pressure differentials and rate of change of pressure.

– Missiles that could be associated with storms (including tornadoes) shall also be considered.

4.2.1.3 (6) Regarding the protection against heavy rainfall, in particular the following aspects shall be considered:

– water level on the plant premises,

– ingress of water into buildings,

– ingress of water via the drainage system.

4.2.1.3 (7) Roofs of safety related buildings shall be designed to withstand the static loads induced by heavy rainfall and snow.

4.2.1.4Biological Hazards

4.2.1.4 (1) Depending on the site specific conditions, in particular the following biological hazards shall be considered:

– mussel growth,

– accumulation of larger amounts of algae, jellyfish or fish,

– accumulation of larger amounts of leaves or grass as flotsam,

– accumulation of larger amounts of biological flotsam due to flooding,

– microbiological corrosion.

4.2.1.4 (2) It shall be ensured by suitable protection measures that biological hazards will not inadmissibly impair the safety of the plant. In particular, the clogging of cooling water and ventilation systems shall be prevented.

4.2.1.4 (3) Safety related cooling water and ventilation systems shall be easy to clean and to maintain.

4.2.1.4 (4) The necessary cleaning equipment shall be available on-site.

4.2.1.4 (5) The ultimate heat sink shall be checked regularly for any changes regarding the biological conditions.

4.2.1.5Geotechnical Hazards

4.2.1.5 (1) Depending on the site specific conditions, in particular the following geotechnical hazards shall be considered:

- slope instability,
- collapse, subsidence or uplift of the site surface,
- soil liquefaction,

4.2.1.5 (2) The geotechnical characteristics of the subsurface materials, including the stability of the foundation material under static and seismic loading, the groundwater regime, and the chemical properties of the groundwater, shall be investigated and a soil profile for the site shall be determined.

4.2.1.5 (3) To identify potential sources for collapse, subsidence or uplift of the site surface, geological maps and other appropriate information for the region shall be examined for the existence of natural features such as caverns, karstic formations and human made features such as mines, water wells and oil wells. Based on this assessment, a detailed description of subsurface conditions shall be developed.

4.2.2 Human Induced Hazards

4.2.2.1 Aircraft Crash

4.2.2.1 (1) It shall be ensured by suitable protection measures that the safety of the plant will not be inadmissibly impaired by an accidental aircraft crash of both commercial and military aircraft with account taken of present and future characteristics of air traffic.

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 fire on the plant premises,
- kerosene explosion outside of structures,
- fire or explosion of (liquid or vaporous) kerosene that has entered into buildings through openings that are either permanent or have been caused by the crash,
- ingress of combustion products and intake of air with reduced oxygen concentration into ventilation systems potentially affecting operator actions, electrical installations and the emergency diesel generator supply air systems,
- debris / missile trajectories that may ensue from the breaking-up of the aircraft,

4.2.2.1 (4) Impacts (e.g. debris / missiles and fires) due to aircraft crashes near the plant shall also be considered.

4.2.2.1 (5) Load-time functions shall be provided for the design

4.2.2.1 (6) Structures shall be designed to provide full protection if safety related components needed to control the impacts and consequences of an aircraft

crash are either located inside the structure or behind it. The protection shall ensure that the components are not damaged by fragments and debris/missiles to such a degree that it can no longer be ensured that the plant can be brought into a safe state.

Permanent openings of buildings in which items important to safety are located shall be arranged and protected such that no kerosene can enter into these buildings in the event of an aircraft crash.

If the ingress of kerosene cannot be reliably prevented by the arrangement of and the protection provided for permanent openings, these are to be arranged and protected at least in such a way that the items important to safety that are necessary according to the regulations will not be inadmissibly impaired.

4.2.2.1 (7) The ion exchangers of the coolant purification system, associated spent-resin tanks and other components and system containing similarly high activity levels in principally flammable form shall be protected against damage by dedicated structural measures and fire protection measures in order to avoid any significant release of radioactive materials due to kerosene fires.

4.2.2.2Plant External Explosion

4.2.2.2 (1) It shall be ensured by suitable protection means that external explosions which have to be postulated due to the site specific conditions will not inadmissibly impair the safety of the plant. Apart from chemical explosions, explosions of vapour or gas clouds, deflagration-to-detonation transition and physical explosions shall be considered.

4.2.2.2 (2) Local and large-scale effects of explosions shall be considered.

4.2.2.2 (3) Suitable protection measures against the effects of plant external explosions are in particular the design of structural plant components and the adherence to safety distances.

4.2.2.2 (4) In the structural design, the following impacts shall be considered in particular:

- direct, reflected and focused pressure waves,
- time history of overpressure and negative pressure,
- debris,
- vibrations of soil and structures ,
- thermal impacts.

4.2.2.2 (5) For structural design, a conservative pressure curve shall be determined.

4.2.2.2 (6) Safety-relevant ventilation systems shall not be inadmissibly impaired by the effects of an explosion.

4.2.2.3Hazardous Materials

4.2.2.3 (1) The following shall be understood as hazardous materials:

a) materials that might lead to loss of safety related systems, structures, and components (due to immediate or long-term effects). These are:

- potentially explosive materials,
- easily flammable or flammable materials,
- materials displacing or consuming the oxygen in emergency diesel supply air,
- clogging materials or
- corrosive materials.

d) materials upon whose impact the ability of the safety relevant personnel to act is no longer sufficiently ensured. These are:

- toxic,
- narcotic,
- corrosive,
- oxygen-displacing,

- oxygen-consuming or
- potentially explosive materials and

e) radioactive materials.

4.2.2.3 (2) It shall be ensured by suitable protection measures that hazardous materials will not inadmissibly impair the safety of the plant and the ability of the personnel to act.

- In this context, the following aspects are relevant:
- site specific presence of hazardous materials (fixed or on transport routes),
- possibilities of their ingress into buildings,
- 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, if necessary and possible, protection features shall be provided.

4.2.2.3 (4) Depending on the nature of the hazardous materials, the following protection measures shall in particular be considered apart from the necessary system design (e.g. physical separation of the supply apertures for redundant subsystems):

Plant-specifically:

a) for hazardous materials with short-term effects
   - interruption of the media supply (e.g. ventilation isolation),
   - switch-over of operating modes (e.g. supply air/exhaust air operating mode to recirculating mode),

b) for hazardous materials with long-term effects
   - inspection of protection means and potentially impaired components, including recurrent testing as well as
   - cleaning.

Organisational:

- training of the personnel,
- protection of the shift personnel by e.g. provision of breathing apparatus, establishment of areas of independent media processing (e.g. air conditioning/regeneration).

Additional:

- detection devices for the respective hazardous materials in the intakes, in the control room and supplementary control room, on the power plant premises and possibly in the vicinity of parts of the plants that are 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) During the impact of hazardous materials, accessibility and habitability of the main control room or the supplementary control room shall also be ensured to the necessary extent by the provision of protective equipment.

4.2.2.4Flotsam, Dam Failures and Ship Accidents

4.2.2.4 (1) Depending on the site specific conditions, the essential service water supply shall also be ensured in case of

- an impact of flotsam,
- a loss of cooling water caused by a failure of a downstream dam,
- consequences of ship accidents and
- collisions of ships with cooling water intake structures.

4.2.2.4 (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.

4.2.2.5External Fire

4.2.2.5 (1) It shall be ensured by suitable protection measures that external fires will not inadmissibly impair the safety of the plant.

4.2.2.5 (2) Apart from thermal impact, combustion products such as aerosols and toxic and/or corrosive materials shall also be considered.

4.2.2.5 (3) The effects of external fires on ventilation systems and the intake air of the emergency diesel generators as well as the possible ingress of combustion products into structures shall be considered.

4.2.2.5 (4) Ground-level ducts and openings of underground supply installations or buildings shall be protected against the entry of flammable liquids in accordance with the safety related requirements pertaining to them.

4.2.2.6Electromagnetic impacts (except lightning)

4.2.2.6 (1) Electromagnetic sources of disturbance outside the plant whose influence on safety-relevant equipment cannot be excluded shall be comprehensively identified and their possible effects shall be assessed. The definition of covering events is acceptable. An analysis of the electromagnetic compatibility shall be carried out to the extent necessary and presented for review.

4.2.2.6 (2) If electromagnetic disturbances from outside the plant can impair the function of items important to safety, suitable measures shall be provided for the protection of their instrumentation and control systems in accordance with their safety-significance.

4.2.2.6 (3) During the entire operating lifetime of the plant, the protection of safety related installations against electromagnetic disturbances shall, if necessary, be adapted to the changes in electromagnetic sources outside the plant.

4.2.2.6 (4) Electromagnetic compatibility in their operating environment shall be demonstrated by appropriate tests / inspections (demonstration of electro-

magnetic compatibility) for items important to safety that may be impaired by electromagnetic impacts from outside the plant.

Annex 3

Basic principles of the application of the single failure criterion and for maintenance

19.3.2015

Contents

1 Single failure concept – Basic principles of the application of the single failure criterion

Objective of the single failure criterion

1 (1) The single failure concept is a deterministic concept for the design of items important to safety in nuclear power plants. Postulating a single failure as well as maintenance in case of actuating an item important to safety shall ensure sufficient redundancy.

1 (2) The degree of redundancy of items important to safety for ensuring the reliability of a safety function depends on its safety significance within the defence-in-depth concept and in case of internal and external hazards. Requirements concerning this matter are provided in Section 2.

1 (3) If an item important to safety is designed according to the single failure concept it can be assumed with a high level of confidence that its operability is not dependent on the coincidental failure of any particular component of the installation or in case of maintenance. The design shall take into account all components of the item important to safety as well as the necessary supply, control, and auxiliary systems.

1 (4) Postulating a single failure in passive structures, systems, and components aims for the segregation of redundant structures, systems, and components. The segregation shall prevent that a passive single failure will lead to a redundancy wide failure of items important to safety.

1(5) In connection with the single failure concept the time period of an unavailability of an item important to safety in case of maintenance is relevant, due to its influence on the total reliability of the safety function affected. To ensure an adequate reliability within the framework of the single failure concept the admissible time of unavailability due to maintenance and its implication on the safety of the plant shall be determined. Requirements concerning this matter are provided in Section 3.

2 Requirements for the application of the single failure concept

2.1 General Requirements

2.1 (1) If a single failure of an item important to safety has to be postulated then it will be generally postulated for active as well as passive items. Exceptions and requirements for specific systems and components are provided in Section 2.5. Further exceptions shall be justified.

2.1 (2) A single failure in one redundant train of a safety system, additional safety feature or complementary safety feature shall not lead to safety relevant failures in other redundant trains.

2.1 (3) In the framework of demonstrating the fulfilling of the acceptance criteria the most unfavourable single failure shall be chosen or the most unfavourable combination with a maintenance case if it has to be assumed. The selection shall be justified.

2.1 (4) If several items important to safety have to fulfil their tasks simultaneously or subsequently for controlling a postulated case of demand, occurrence of a single failure is postulated for the total of the systems but not in several of the installations required at the same time.

2.2 Redundancy requirements for items important to safety for operating phases A and B

2.2.1 Requirements for level 1 of defence in depth

For items at level 1 of defence in depth, there is no requirement for redundant design (degree of redundancy n+0).

2.2.2 Requirements for level 2 of defence in depth

For items important to safety for the control of anticipated operational occurrences, neither a single failure nor an unavailability of a redundancy due to maintenance (maintenance case) shall be postulated (degree of redundancy (n+0)).

For items important to safety for instrumentation and control systems executing instrumentation and control functions at level 2 of defence in depth a single failure shall be postulated (degree of redundancy (n+1)).

Note: In case of actuating safety systems to control events on level of defence 2 (e.g. "loss of main heat sink" and "loss of off-site power ≤10 h") single failure and maintenance case are postulated for the items important to safety on level 3a of defence in depth.

2.2.3 Requirements for level 3a of defence in depth

For active safety systems to control postulated single initiating events at level 3a of defence in depth a single failure and a maintenance case shall be generally postulated in case of actuation (degree if redundancy (n+2)). Exemptions are given below.

If for a items important to safety ensuring containment isolation a redundancy degree of only (n+1) is realised, maintenance shall only be performed if during the maintenance-induced unavailability of such an item, its safety-related function is reliably ensured otherwise by substitute procedures (e.g. closure of the 2nd isolation valve as a precaution) or the maintenance is limited in time and the permissible unavailability is specified in the operating manual.

For the maintenance cases, all maintenance procedures that are permitted and can be performed during the relevant operating phases shall be considered. Details on the permissibility of maintenance procedures in the respective operating phases are provided in Section 3.

Notes: The postulated failure of the most reactivity effective control element or control rod may be treated as single failure according to subsection 3.2 (6) and (7) of the

"Safety requirements for nuclear power plants" with regard to the subcriticality to be maintained.

In the analysis of all postulated single initiating events a single failure and a maintenance case according to subsection 3.2.4 (1) of Annex 4 shall be assumed to occur simultaneously in active components of the safety system.

2.2.4 Requirements for level 3b of defence in depth

For active components of additional safety features to control postulated multiple failure events a single failure shall be postulated (degree of redundancy (n+1)).

2.2.5 Requirements for level 4 of defence in depth

Active components of supplementary safety features for controlling postulated core melt accidents (level 4 of defence in depth) shall fulfil the single failure criterion (degree of redundancy (n+1)).

2.3 Redundancy requirements for items important to safety for operating phases C to F

2.3 (1) For the periods of scheduled maintenance work during operating phases C to F (inspection or shutdown) on safety systems at level 3a of defence in depth required for these operating phases, a single failure but no additional maintenance case is postulated (degree of redundancy (n+1)).

2.3 (2) A degree of redundancy n+0 is permissible in the operating phases E and F if in case of failure of the item important to safety, the time until non-fulfilment of the acceptance criteria is more than 10 hours and the active item important to safety failed or being under maintenance can be made available within 10 hours.

Note: The different operating phases are presented in Table 1-1 and 1-2 in Annex 1.

2.4 System and component specific requirements for the application of the single failure criterion

Passive structures, systems and components

2.4 (1) Within the framework of the single failure concept no failure has to be postulated for passive systems, structures and components without active components, if it has been demonstrated, that these structures, systems and components are designed with sufficient safety margins for all postulated cases of demand. The maximum expected loads shall be considered, taking into account the changes of the material properties during lifetime of the plant. A suitable material shall be chosen according to the planned application of the structure, system and component and shall be constructed, mounted, tested and operated with a comprehensive quality assurance to ensure an adequate reliability. The applicable procedures and safety margins shall be determined according to the safety significance of the item important to safety.

2.4 (2) The required safety demonstration in 2.4 (1) is proved, if the requirements regarding design, construction, material selection, manufacturing and testability of structures, systems and components according to regulations is fulfilled, taking the significance for nuclear safety into account.

2.4 (3) A single failure shall be postulated if the passive system relies on a passive process initiated by active components in case of demand.

Valves

2.4 (4) For check-valves a single failure shall be postulated if, when demanded, they have to change their initial position for fulfilment of the safety function.

2.4 (5) For self-medium-operated safety valves, relief valves and isolation valves of the reactor coolant system and the main steam system a single failure shall be postulated in the pilot control.

3 Maintenance and modification

3.1 General Requirement for maintenance

3.1 (1) Maintenance procedures which could lead to an unavailability of an item important to safety without procedures replacing its function or supersede its functional stand-by (e.g. shutdown, power reduction, fall-back on other procedures) are only permitted, if for the time period of maintenance the requirements of the single failure concept are fulfilled.

This requirement shall be applied for other procedures, which could lead to an unavailability of items important to safety, e.g. in case of modification or changes of the operating modes.

3.1 (2) For the re-establishment of the function of an item important to safety the permitted downtimes of these items shall be defined for each operating phase in the operational limits and conditions.

3.1 (3) Furthermore, the conditions to perform a preventive maintenance during operation, in particular for power operation (operating phase A) shall be defined in the operational limits and conditions. Details are provided in Section 3.3.

3.2 Maintenance procedures for achieving the specified normal condition of a safety-relevant installation (repair)

3.2.1 Procedures in case of deficiencies identified at items important to safety

3.2.1 (1) In case of deficiencies identified in items important to safety that could lead to the unavailability of the item when demanded, procedures for identifying the cause of the deficiency and for removing the deficiency are initiated immediately. In particular it shall be clarified whether the identified damage mechanism is of systematic nature.

3.2.1 (2) Necessary plant specific procedures (e.g. power reduction, shutdown) shall be initiated according to the operating manual. These procedures shall be identified and determined according to section 3.1.

3.2.1 (3) In case the time needed for the remedy of the deviation is not in accordance with the time period specified in the operational limits and conditions, the plant shall be transferred into an operating condition defined in the operating manual.

3.2.1 (4) If in case of an identified deficiency in an item important to safety, for which the permissible repair times are specified in the operational limits and conditions, it can be foreseen that repair cannot be performed within the permissible time, the procedures provided according to section 3.1 shall be initiated immediately.

3.2.1 (5) In cases where the operational limits and conditions do not include explicit specifications on permissible repair times for items important to safety the plant shall be immediately brought into an operating condition in which the availability of this item important to safety is not required or only to a limited extent.

3.2.2 Specification of allowable periods of inoperability

3.2.2. (1) The allowable periods of inoperability of items important to safety for the control of events on levels of defence 2 to 3b shall be determined and specified in the operational limits and conditions. Findings from reliability analyses and operational experience shall be taken into account.

3.2.2 (2) These specifications shall include at least the following information:

- Allowable periods of inoperability of one or more of these items important to safety and their minimum availability for each operating phase.
- Clear description of the procedures to be initiated when reaching the allowable periods of inoperability (e.g. power restriction or plant condition to be reached, procedures for reducing the occurrence probability of events).

3.2.2. (3) For those cases, not explicitly described in the operating manual (e.g. simultaneous failure of several items important to safety), the operating manual shall contain instructions to determine a suitable plant condition, i.e. a condition where the availability of the item important to safety is not required or is only required to a limited extent.

3.3 Preventive maintenance of items important to safety

3.3.1 General requirements for preventive maintenance

3.3.1 (1) Preventive maintenance resulting in unavailability of items important to safety shall be performed in general during operational phases 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 operating phases A and B, preventive maintenance measures are only permissible to a limited extent and only in compliance with the requirements of subsection 3.3.3.

3.3.1 (3) The requirements for preventive maintenance during operation of items important to safety are appropriately applicable for other planned procedures, which could lead to an unavailability of an item important to safety (e.g. modification of the plant). Deviations shall be justified.

3.3.2 In-service inspection

If in-service inspection is required for ensuring the functional operability of items important to safety, these can always be performed in all operating phases under the following conditions:

- The in-service inspection only leads to unavailability times of the item important to safety of less than 8 hours, and
- the item important to safety can be brought back to functionality in short time in case of a necessary demand, this shall also be possible under accident conditions, and
- the work remains restricted to one redundancy and all other redundancies remain fully available during this period, and
- in-service inspections during start-up and shut-down of the plant (operating phase B) is limited to unavoidable cases.

3.3.3 Permissibility of preventive maintenance during operating phases A and B

3.3.3 (1) The duration and the boundary conditions under which preventive maintenance during operation of items important to safety for the control of events on levels of defence 2 to 3b in the operating phases A and B and events due to hazards is permissible shall be specified in the operational limits and conditions under consideration of the safety significance.

3.3.3 (2) Regarding the specifications of subsection 3.3.3 (1), the following requirements shall be fulfilled:

- Preventive maintenance during operation of items important to safety at level 2 of defence in depth with a degree of redundancy of (n+1) is only admissible if an assessment of the item important to safety under consideration of the relevant cases of demand was performed and an adequate reliability was demonstrated.

- For safety systems with a degree of redundancy (n+2) the time of unavailability due to preventive maintenance shall be restricted under consideration of the reliability requirements for the respective item important to safety. Without a detailed safety demonstration, the duration of unavailability of an item important to safety with a degree of redundancy (n+2) shall not exceed 7 days per redundancy and year. For longer periods, plant-specific safety analysis shall be presented showing that unavailability of this items important to safety over a longer period does not raise any safety concern.

- Preventive maintenance during operation of items important to safety at level 3a of defence in depth with a degree of redundancy less than (n+2) are generally inadmissible.

- Preventive maintenance of additional safety features (at level 3b of defence in depth) and complementary safety features (at level 4 of defence in depth) during operation is only admissible, if an assessment of the item important to safety under consideration of the relevant cases of demand was performed and an adequate reliability was demonstrated.

3.3.3 (3) Preventive maintenance during operation are only permissible if the following boundary conditions are fulfilled:

- The preventive maintenance during operation shall not lead to a noteworthy increase of probability for anticipated operational occurrences, postulated single initiating events and postulated multiple failure events.

- Preventive maintenance during operation shall not be performed in several redundancies at the same time and shall be limited to one redundancy. Furthermore it shall be ensured that the availability of the remaining redundancies is not limited due to other activities (e.g. modification measures). This does not apply to necessary repair activities on items important to safety if those had failed coincidentally.

- The preventive maintenance during operation shall not lead to loss of functions, especially not due to common-cause failures of items important to safety not being affected.

- The fulfilment of the maintenance requirements in case of preventive maintenance during operation shall also be ensured under the conditions of operating phases A and B (e.g. requested post maintenance testing not affected).

- During start-up and shut-down of the plant and related test periods, no preventive maintenance during operation shall be performed.

- The integrity of the two barriers reactor coolant pressure boundary and containment, as well as the reliability of their active safety functions shall not be impaired by preventive maintenance during operation in an undue manner. If only two isolation devices (degree of redundancy n+1) are available as barriers, preventive maintenance during operation on these isolation devices are acceptable if the cooling circuit is depressurized.

4 Ensuring the functional standby of items important to safety

4 (1) The functional standby of items important to safety shall be periodically tested with a sufficient extent taking into account the conditions in case of demand .

4 (2) If possible, the entire functional sequence of the respective items important to safety as happens in case of demand shall be subjected to a functional test, e.g. also switching of emergency power supply to the consumers. If

subtests are necessary for process-related reasons, valid overlapping of the various subtests shall be ensured.

4 (3) The performance of functional tests shall not lead to a noteworthy increase of occurrence probability for anticipated operational occurrences, postulated single initiating events and postulated multiple failure events.

4 (4) Functional standby of the installations shall be maintained during the functional test as far as possible. Where applicable, downtimes due to tests performed shall be considered in the reliability analysis.

4 (5) It shall be ensured that test-induced deviations from the standby state of an item important to safety can be removed in due time, in case of demand.

4 (6) Functional standby of an item important to safety shall be ensured. Scheduled or fault-induced unavailability of individual components leading to an unavailability of the item important to safety shall be easily identifiable for the operating personnel (e.g. deviation from a clear standby state, unavailability due to maintenance, failure in I&C systems, changes in the water levels induced by anticipated operational occurrences, etc.).

4 (7) Erroneous positioning of valves shall be prevented as far as possible by reliable technical items (e.g. alarms in case of deviations from the standby state, valve locks) and where necessary by reliable administrative procedures.

4 (8) Deviations from parameter values specified in the plant operating manual for ensuring safe plant operation shall be indicated to the operating personnel by optic and acoustic signals at the control room.

4 (9) It is ensured that for a case of demand all information necessary for the assessment of the functional standby and effectiveness of items required in case of demand shall be available to the operating personnel at the control room or the supplementary control room or can be easily and rapidly determined by the information available at the control room or the supplementary control room.

4 (10) Functional standby and the function of items important to safety according to the requirements shall be ensured after completed maintenance by qualified functional tests.

Annex 4
Requirements on safety demonstration and documentation
19.3.2015

Contents

1 Objective and scope

1 (1) This Annex contains requirements for safety demonstration and documentation.

Suitable demonstration methods are applied to verify fulfilment of the requirements specified in the “Dutch Safety Requirements for Nuclear Reactors”.

1 (2) For safety demonstration according to the “Dutch Safety Requirements for Nuclear Reactors”, number 5 (4), both deterministic and probabilistic methods are applied.

1 (3) The safety demonstrations are documented in the form of demonstration documents. These are complete and comprehensible as well as verifiable.

2 Fundamental requirements for system assessment

2 (1) The main purpose of the system assessment shall be to determine whether an adequate level of safety has been achieved. The system assessment shall demonstrate that the required effectiveness and reliability of inherent features, equipment and procedures are met and whether their relevant quality characteristics are fulfilled. It shall be demonstrated that all safety requirements on the design of the plant are met throughout the entire lifetime of the plant. It shall be confirmed that the design, as delivered, meets the requirements for manufacture, construction, and as built, as operated and as modified. Here, the conditions ensuing from the calculatory analysis of events or operational states shall be taken into account.

2 (2) The performance of a system assessment requires an up-to-date compilation of safety-relevant information on the actual conditions of the plant.

For each item important to safety the following information shall be provided:

- Description of the intended safety functions to be performed on the respective level of defence
- Description of the layout, assembly and design
- Description of the actual valid operational limits and conditions to ensure the effectiveness of the considered item important to safety
- Description of the actual condition of the considered item important to safety

Planned modifications shall be considered in the system assessment if those modifications are either accepted by the regulatory body or documented in a verifiable form.

2 (3) If relevant to the circumstances to be analysed from a safety point of view, the results of the evaluation of operating experience shall be included in the system assessment.

3 Fundamental requirements for the deterministic analysis of events and conditions

3 (1) It shall be shown by the analysis of events or conditions that all (quantitative and qualitative) assessment criteria postulated in the “Dutch Safety Requirements for Nuclear Reactors” are fulfilled.

3 (2) If safety demonstration is done by analysing events and conditions,

a) up-to-date compilation of safety-relevant information on the prevailing condition of the procedures and items important to safety concerned shall be consulted. For existing installations, planned modifications shall be taken into account where applicable,

b) validated analysis methods according to the criteria in Section 3.1 shall be used for the respective areas of application;

c) the analyses regarding selected initial and boundary conditions shall be based on the requirements listed in Section 3.2;

d) the uncertainties in connection with levels of defence 1 – 3 that are associated with the respective analysis results for the corresponding acceptance criteria shall be quantified and taken into account in their entirety according to Section 3.3 or shall be taken into account according to Section 3.4;

e) operator actions as described in the operating manual as well as in the emergency operating procedures shall be considered in the analyses;

f) the uncertainties in connection with level of defence 4 analysis shall be assessed with regard to the acceptance target.

3 (3) If safety demonstration is done by analysing events or conditions, the following shall be documented in particular:

a) the relevant data used; unless plant-specific data are used, applicability has to be justified;

b) the justification of the choice of the underlying impacts, events, operating phases and operating conditions with regard to the fulfilment of the respective acceptance criterion;

c) in the case of statistical methods being used for determining the uncertainty of the analysis results: the distributions used in the analysis for the relevant input parameters, their derivation and, if relevant, their dependencies according to subsection 3.3 (1).

3.1 Validation of analysis methods

3.1.1 Objective

3.1.1 (1) Analysis methods that are used for safety demonstration of the fulfilment of the acceptance criteria for all levels of defence in depth and for the effectiveness of mitigative measures at level 4 of defence in depth must be validated for their respective scope of application.

3.1.1 (2) The validation of an analysis method must comprise the examination of the scope of application of the method and of the agreement of the results that

can be obtained by application of this method with comparative values obtained from

- experiments, plant operation, plant transients or other events,
- exact analytical solutions, or
- other validated analysis methods, provided the validation of that method is available to the user.

3.1.1 (3) An analysis method may be considered 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 particularly the case if the results obtained with the method lie within the bandwidths of experimentally obtained results (see subsection 3.1.2 (2)).

3.1.2 Performance

3.1.2 (1) 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 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 justified by for example engineering judgement.

3.1.3 Documentation

3.1.3 (1) The documentation regarding validation shall contain:

- data relating to the comparative values used (according to subsection 3.1.1 (3)), for experiments, plant transients or other events, including data on the accuracy of the comparative values referred to,

- data on the validated scope of application of the analysis method,
- descriptions of the calculation methods and models used as well as of the input data.

3.2 Specifications regarding initial and boundary conditions as well as the scope of safety demonstration

3.2.1 Criteria regarding the different levels of defence in depth

3.2.1 (1) For the demonstration of the stability of parts of physical structures / buildings, whose collapse could lead to safety-relevant impacts, the static and dynamic, mechanical, chemical and thermal impacts shall be considered.

a) Impacts due to assumed conditions, events and defined operational states on level of defence 1 to 3a as well as impacts resulting from internal and external hazards, shall be taken into account or superimposed in such a manner, that all consequences are considered conservatively.

b) impacts resulting from postulated events and conditions at levels 3b and 4 of defence in depth shall be realistically taken into account.

3.2.1 (2) For the demonstration of the integrity and stability of components, static and dynamic, mechanical, chemical, thermal and radiation-induced impacts shall be considered.

a) Impacts due to assumed conditions, events and defined operational states at levels 1 to 3a of defence in depth as well as impacts resulting from internal and external hazards, shall be taken into account or superimposed in such a manner, that all consequences on load bearing cross sections with respect to the covering failure mechanism are considered conservatively.

b) impacts resulting from postulated events and conditions at levels 3b and 4 of defence in depth shall be realistically taken into account and the condition of the component shall be accordingly analysed.

3.2.1 (3) Combinations of several external hazards or combinations of these hazards with internal events and hazards shall be postulated in accordance with the “Dutch Safety Requirements for Nuclear Reactors”.

The accidental impacts and the impacts resulting from the accident consequences are combined with the “normal external operational loads” (incl. snow and wind loads) and the “forced reactions under normal operational loads”. Consideration of the time-dependent progression of events is admissible for these combinations.

3.2.1 (4) The following shall be considered as possible consequential events occurring as a result of external hazards, unless the corresponding plant components have been designed to withstand these events:

a) impacts from pressure blast waves upon the failure of vessels with high energy content;

b) consequential mechanical damage upon the failure of plant equipment;

c) flooding due to a failure of plant equipment and

d) fires

and the following shall be taken into account:

e) malfunctions of structures, systems and components in plant areas that are not correspondingly designed, with consideration of instrumentation and control installations, and

f) the occurrence of a loss of offsite power.

3.2.1 (5) The protection of structures, systems and components in the case of internal events, postulated internal and external hazards shall be demonstrated on the basis of specified load assumptions. Here, induced vibrations of structures, systems and components shall also be considered.

3.2.1 (6) Safety demonstration at levels 2 to 3b of defence in depth shall be performed at least from the onset of an event until a controlled plant condition has been achieved in which the plant can permanently remain.

The analyses of the effectiveness of procedures and items important to safety provided at level 4 of defence in depth shall be carried out up to the moment when the condition relevant for the analysis has been reached.

3.2.1 (7) In the quantification of the uncertainties of the results according to subsection 3.3, measuring and calibration errors can be taken into account statistically. In conservative safety demonstrations according to subsection 3.4, the maximum measuring and calibration errors shall be covered by the initial and boundary conditions.

3.2.2 Level 1 of defence in depth (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 shall be considered, taking into account the possible changes and oscillations during normal operation.

3.2.3 Level 2 of defence in depth (anticipated operational occurrences)

3.2.3 (1) Adverse initial conditions lying within the range of realistic operating conditions shall be postulated for the different operating phases with regard to the respective acceptance criteria.

3.2.3 (2) All procedures and items important to safety allocated at level 2 of defence in depth and demanded according to the specifications can be assumed as being available for safety demonstration unless they are to be assumed to have failed due to the postulated event.

3.2.3 (3) A simultaneous failure in addition to loss of off-site power that is independent of the event need not be assumed.

3.2.4 Level 3 of defence in depth

3.2.4 (1) For demonstration of the effectiveness of safety systems at level 3a of defence in depth, the single-failure concept shall be applied.

The postulated failures according to the “Dutch Safety Requirements for Nuclear Reactors”, subsections 3.1 (8), 3.2 (6) and 3.2 (7), as well as according to Annex 3 of the “Dutch Safety Requirements for Nuclear Reactors” shall be taken into account.

In the analysis of events at level 3 of defence in depth, it shall be assumed that no credit can be taken of the first actuation of the reactor protection system or the first actuation of reactor scram unless only one actuation criterion is available for physical and technical reasons.

In the analysis of all postulated single initiating events a single failure and a maintenance case shall be assumed to occur simultaneously in active components of the safety system.

3.2.4 (2) Depending on the kind of event, a simultaneous or delayed loss of the house load supply shall also be postulated for all items important to safety and procedures 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 program of the equipment units supplied with emergency power.

3.2.4 (3) In addition to the assumed failures of the single-failure concept, safety demonstration shall also take into account accident-induced consequential failures of measures and installations with an adverse effect on the accident sequence as defined by the acceptance target.

In the event that this results in relevant adverse influences on the event sequence, it shall be postulated that the procedures and items important to safety will become operative as specified.

3.2.4 (4) The source term for radiological safety demonstrations at level 3 of defence in depth shall be determined up until the end of the release. If necessary, suitable termination criteria shall be specified for defining the end of the re-

lease. The radiological safety demonstrations shall be provided in accordance with the national requirements.

3.2.4.1 Level 3a of defence in depth (postulated single initiating events)

3.2.4.1 (1) The postulated initial conditions shall

- in the case of safety demonstration according to subsection 3.4 be covered by the initial operating conditions of normal operation that are worst for the respective operating phases with regard to the acceptance criterion that is the most difficult to meet, or
- in the case of safety demonstration according to subsection 3.3 be covered by means of realistic parameter values, also applying their uncertainty ranges.

3.2.4.1 (2) Regarding loss-of-coolant accidents, the respective worst leak/break location is determined and postulated for the spectrum of the leak/break sizes to be considered for the respective individual safety demonstrations when determining the effects of

- the pressure and temperature build-up in the containment,
- the pressure differences in the containment,
- missiles, jet forces and reaction forces, and
- pressure blast waves within the reactor coolant pressure boundary.

as well as

- when demonstrating the effectiveness of the emergency cooling installations and the support stability of installations (especially large components) and rooms.

3.2.4.2 Level 3b of defence in depth (postulated multiples failures events)

3.2.4.2 (1) In the analysis of the effectiveness of measures and items important to safety at level 3b of defence in depth, realistic models and realistic initial

and boundary conditions can be applied for the postulated event sequences.

3.2.4.2 (2) For the assessment of multiple failures events, all systems can be deemed available, except those which are assumed to have failed in the multiple failures events combination. No additional failure and no unavailability due to maintenance have to be deterministically postulated in the systems needed to reach the final state, in which the fundamental safety objectives are achieved (Dutch Safety Requirements for Nuclear Reactors 2.3).

3.2.4.2 (3) The safety assessment of multiple failures events has to include an assessment of the overpressure protection of the primary and in case of pressurized water reactors also of the secondary circuits with adequate specific criteria (s. Dutch Safety Requirements for Nuclear Reactors, Annex 1).

3.2.4.2 (4) The calculated radiological consequences must be consistent for multiple failures events with the radiological safety objectives set in 2.5 of “Dutch Safety Requirements for Nuclear Reactors” and in Annex 1 Table 3-5. Uncertainties of the results shall be considered when assessing the fulfilment of regulatory limits.

3.2.5 Level 4 of defence in depth (postulated core melt accidents)

3.2.5 (1) The uncertainties related to the relevant phenomena which could occur during postulated core melt accidents have to be applied in various scenarios and sensitivity studies.

3.2.5 (2) To demonstrate the achievement of the radiological safety objectives calculations of potential radiological consequences shall take into account realistic assumptions and parameters. Uncertainties of the results shall be considered when assessing the fulfilment of regulatory limits.

3.3 Quantification of the uncertainties of results

3.3 (1) When using statistical methods, the overall uncertainty of the corresponding analysis result shall be quantified according to subsection 3 (2) d). For this purpose,

a) the parameters (initial and boundary conditions as well as model parameters) and models that have a considerable influence on the uncertainties of the results 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 shall 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 unilateral 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% shown for the fulfilment of the acceptance criterion.

3.3 (4) The 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 which are added to the analysis result, or

c) if with regard to the corresponding acceptance criterion

- worst parameter combinations lying within realistic conditions are used, or if
- worst values of the individual parameters of the uncertainty range are combined such 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 for a comparable case that the uncertainties quantified according to subsection 3.3 are covered with regard to the respective acceptance criterion.

4 Fundamental requirements on safety demonstration by measurements

4 (1) Prior to the performance of measurements and experiments, the demonstration subject shall be specified and the measuring or experimental procedure planned in detail. If measurements or tests are to be performed within the nuclear power plant, the effects of the measurements or tests on the plant's safety shall be checked and set forth in writing. Safety-relevant adverse effects shall be prevented.

4 (2) If measurements or experiments are to be performed not within the plant or facility to be assessed but e.g. on component prototypes or test facilities, applicability to the components, systems or system functions to be assessed 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 measuring uncertainties into account.

4 (4) The demonstration subject, the measuring or experimental procedure and the results shall be documented in a comprehensible manner.

5 Fundamental requirements on engineering judgement

5 (1) Results from engineering judgement 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 shall 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 assessment criteria developed according to subsection 5 (1) a) is documented in a comprehensible manner.

5 (2) There are the following requirements on the performance of engineering judgement:

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 assessments are documented completely and in a comprehensible manner,

c) if applied to interdisciplinary and complex issues, the engineering assessment shall be performed by a team composed in an appropriate manner.

5 (3) For ergonomic analyses of personnel actions, the tasks assigned to the personnel shall 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 criteria.

The task analysis shall consider the aspects:

- required and available information for the person acting,
- required processes of information processing,

- required decisions and individual actions,
- time-dependent and spatial boundary conditions of the tasks.

6 Fundamental requirements on probabilistic safety analyses

6 (1) The fundamental methods and boundary conditions for the preparation of probabilistic safety analyses are described in regulatory provisions.

6 (2) In probabilistic safety analyses for assessments according to the "Dutch Safety Requirements for Nuclear Reactors " numbers 5 (8a) and 5 (8b), up-do-date methods, models and data have to be used. The up-to-dateness of the probabilistic safety analysis shall consider in particular the following aspects:

- safety-relevant modifications to procedures, items important to safety, or the operating mode performed in the plant,
- safety-relevant events or effects having become known, and
- the plant-specific evaluation of operating experience with regard to reliability parameters of components or occurrence frequencies of initiating events.

6 (3) For the probabilistic safety analysis, plant-specific data have to be used. If no sufficiently plant-specific database from operating experience is available, generic data may be used. The applicability of the generic data shall be justified.

6 (4) Probabilistic safety analyses shall be carried out by competent applicant or licensee staff. Support by external personnel is admissible.

6 (5) The respective scope and degree of detail as well as the scope of documentation of the probabilistic safety analysis results shall be defined case by case.

7 Fundamental requirements on documentation

7 (1) All documents used during the planning, construction and operation of the plant for the licensing and supervisory procedure shall be documented in a systematic and comprehensible manner. The degree of detail of the documentation shall be adapted to the safety-related significance of the contents of the documents.

7 (2) The documentation shall fulfil the following requirements:

- application of a clearance/licensing procedure that is commensurate with the relevance of the respective document,
- clear identification of documents,
- timely updating of documents, in particular in case of plant modifications,
- identification of modifications and of the revision status of documents,
- assurance of the availability of applicable documents at the respective equipment locations,
- timely adaptation of documentation required for operation management to the current plant condition and keeping it available in the control room,
- assurance of legibility and visual clarity,
- clear and unambiguous specification of safety-relevant operative instructions,
- identification and distribution of external documents to the respective equipment locations,
- prevention of the use of outdated documents or documents that are no longer applicable.

7 (3) The documentation shall be maintained and archived according to defined rules.

7 (4) Stipulations for the different kinds of document, documentation, document management, archiving, responsibilities and examination shall be specified in a documentation system.

Annex 5

Definitions

19.3.2015

All words printed in italics are explained in the definitions

A

Abnormal operation

Operational processes that develop in the event of malfunctions of installations or human errors whose occurrence is frequently to be expected over the service life of the plant concerned from operating experience and for which there are no safety-related reasons against a continuation of operation or the activity (level 2 of of defence in depth).

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 fulfilment of *acceptance criteria.*

Accident

Event or event sequence which is not expected to occur during the service life of the plant, however the plant is designed such that the design principles, *acceptance targets* and *acceptance criteria at level 3 and 4 of defence in depth* are fulfilled, and in case of its occurrence operation of the plant or the action cannot be continued due to safety reasons. Accidents comprise the following event sequences:

- Postulated single initiating events (level 3a of defence in depth)
- Postulated multiple failure events (level 3b of defence in depth)
- Postulated core melt accidents (level 4 of defence in depth)

Accident analysis

Analysis of the sequence of an event *on level of defence 3* (accident).

Accident instrumentation

Equipment which monitors, displays and records information on the condition of the plant before, during and after an event at levels 3 and 4 of defence in depth.

Accident procedure

Accident procedures or emergency operating procedures are plant specific procedures containing instructions for operating staff to implement preventive measures for managing accidents. These procedures typically contain all preventive measures for accident conditions.

Additional safety features

Engineered safety features to control postulated multiple failure events and avert escalation to core melt accidents.

Ageing

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

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

Ageing management

The entirety of all *measures* and *installations* to be provided by the *licensee* to control the *ageing* phenomena that is relevant with regard to the safety of a nuclear power plant.

Alarm system

Instrumentation and control installation signalling the necessity of a *measure* by optical or acoustic means.

Alternate emergency power supply

An electrical power supply that that is dedicated to supply power during station black-out and other accidents more severe than postulated single initiating events, i.e. during postulated multiple failure events and postulated core melt accidents.

Anticipated operational occurrence

Event or event sequence which is expected to occur frequently during the service life of the plant, and upon whose occurrence the operation of the plant or the activity can be continued, and for which the plant is designed or for which, with regard to an activity, *measures* and *installations* are provided as a precaution (*level 2 of defence in depth*). Synonyms: *abnormal operation*

Auxiliary and supply systems

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

Autarchy

The plant is able to bring itself into a safe state without human support and maintain this condition for at least 10 hours.

to avert

Events or event sequences can be averted, if items important to safety and procedures are designed with a higher reliability on a higher level of defence in depth *to prevent* such events or event sequences with the required reliability and effectiveness. It shall be achieved, that such events or event sequences at level 3a of defence in depth during the lifetime of the plant has not to be expected. For safety demonstration, such events have to be postulated.

B

Basic safety

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

Boron dilution, heterogeneous

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

Boron dilution, homogeneous

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

C

Cladding damage

Cladding damage is the degradation or breaching of the fuel rod cladding leading to a loss of this barrier for confinement of radioactive materials. It can contribute to increasing plant background radiation and / or can contribute to the release of radioactive fission products to the environment.

Common Cause Failure

A common cause failure is a failure of two or more redundant structures, systems and components due to a single specific *event* or cause.

Competence of persons

Synonym of *qualification of persons.*

Complementary safety features

Engineered safety features to control postulated core melt accidents and to achieve a long term stable state.

Component

See *structures, systems and components*.

Component part

Part of an *installation* or the smallest part of a *subassembly* manufactured from product forms. A component part is an item, which cannot operate alone.

Component, passive

A component whose functioning does not depend on an external input such as actuation, mechanical movement or supply of power.

Computer-based system

Plant component in which the functions of the system are achieved through an embedded computer system.

Conservative

The way of proceeding in safety assessments under consideration of the most unfavourable values from a safety point of view under the given circumstances.

Containment

Leaktight barrier to fulfil confinement function. The containment is part of the *containment system*.

Containment penetrations

Design 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.

to control

An event or event sequence is controlled, if it could be demonstrated that specified acceptance criteria are fulfilled.

Radiological representative postulated events are controlled, if it could be demonstrated that the radiological criteria are fulfilled.

Control room

The central location from which the operation of a nuclear power plant unit is monitored and controlled. Parts of the main control room are the actual control room and the adjoining rooms.

Coolability

Condition of the reactor core in case of which the removal of the heat produced and stored can be ensured.

Cooling water

Water which during *normal operation* is not contaminated with radioactive materials and which has the function of heat transfer to the main heat sink (e.g. receiving water, cooling tower).

Core damage, severe

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

D

Decay heat

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

Decommissioning

All steps leading to the release of a nuclear facility from regulatory control. These steps include the processes of decontamination and dismantling.

Defence-in-depth concept

Concept to protect people and environment from harmful effects of ionizing radiation by compensating potential component failures as well as human errors and by maintaining the efficiency of the barriers by averting damage to the facilities and to the barriers themselves.

A hierarchical deployment of different levels of diverse equipment and procedures to prevent the escalation of anticipated operational occurrences and to maintain the effectiveness of physical barriers placed between a radiation source or radioactive material and workers, members of the public or the environment, in operational states and, for some barriers, in accident conditions.

Degree of redundancy

Degree of redundancy n + x: n is the number of the *redundants* at least needed for controlling an event, with n possibly having different values depending on the different *operating phases* or *operating conditions*; x refers to the number of the *redundants* to be provided additional 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

The range of conditions, events and hazards taken explicitly into account in the design of a nuclear reactor, according to established criteria, such that the nuclear reactor can withstand them without exceeding authorized limits by the planned operation of items important to safety.

Design basis earthquake

A design basis earthquake is an earthquake considered in the design of a nuclear reactor for which safe shutdown of the nuclear reactor is ensured and a safe state can be maintained. The design basis earthquake is sometimes called a safe shutdown earthquake (SL-2).

In contrast to the design basis earthquake the operating base earthquake (SL-1) is less severe and more probable than the design base event without the need to shut down the nuclear reactor. An operating base earthquake corresponds to a level with a probability of being exceeded of 10^{-2} (mean value) per reactor per year.

Design basis event

A design basis event is a general term for a hazard considered in the *design basis*. A design basis event could be e.g. a *design basis earthquake* or a design basis flood.

Design limit

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

Design, inherently safe

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

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.

Diameter Nominal (DN)

Defines the pipe size by a non-dimensional number in the order of the inner diameter measured in mm. The outer diameter and the wall thickness are defined in standards

and depend on the material and intended application. The diameter nominal could differ from the actual inner diameter measured in mm.

Dismantling

Removal of structures, systems and components after the decontamination with the aim of reusing, recycling or disposal of materials.

Diversity

Availability of two or more operable *installations* to fulfil the intended function, having different physical or technical designs.

E

Emergency control centre

Room from which emergency response can be directed by the emergency management group of the operating organization.

Emergency power consumer

An electrical consumer which is supplied from an *emergency power supply facility*.

Emergency power generator including batteries

Plant component that supplies the electrical energy in case *of loss* of function of the *house load supply.*

Emergency power supply facility

The combination of a specific *emergency power generator* including batteries with all *plant components* required for the supply of the associated consumers.

Emergency power supply

Supply of the *emergency power consumers* from *emergency power generators including batteries*.

Emergency power supply, uninterrupted

Emergency power supply, which in case of failure of the *house load supply* or the *grid connections*, supplies electrical energy via an *emergency power generator including batteries* without interruption.

Emergency power system

Entirety of the various *emergency power supply facilities* - partly different according to power generation and function.

Emergency preparedness

All precautions taken outside a plant for the protection of the population and the environment in connection with *a release of radioactive materials* that is impending, happening or has already occurred. Emergency preparedness measures are subdivided into disaster control measures and precautionary radiation protection measures.

Event

An incident that potentially or actually impairs the safety of a plant because it can lead to *anticipated operational occurrences* or accident conditions.

Event analysis

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

Event, representative

Event whose analysis allows an sufficiently covering safety demonstration.

External hazards

Impacts caused by the ambient conditions, natural events or external human induced influences from outside the plant site.

External systems

Pressure- and activity retaining systems and components of light water reactors that do not belong to the reactor coolant pressure boundary which have safety significance. This applies if one of the following criteria is fulfilled:

a) The *plant component* is necessary in connection with the control of *events on levels of defence* 3a and 3b with regard to shutdown, maintenance of long-term subcriticality, and immediate *residual-heat removal.*

b) If the *plant component* fails, high energies are released, and the functions of *safety-relevant installations* are not protected against impacts in connection with an assumed *failure* of these plant components.

c) The failure of the *plant component* my lead immediately or via a chain of postulated consequential events to an event of *level of defence* 3 or beyond.

F

Fail safe principle

A system, structure or component is designed in such a way that in case of a failure the failed system, structure or component behaves safety oriented.

Failure

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

Failure, loss

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

N o t e: The event failure marks the moment in time of the transition from correctness to a failure. A loss may involve a failure at the same time, but not necessarily. For example, a piece of equipment that is not demanded may be lost; it will only have failed if it is demanded and can no longer fulfil its function.

Feedwater

Water for secondary-side supply to the steam generators in PWR plants.

Fire protection measure

Structural, system design, operational or defensive *measure* or *installation* preventing the initiation or spreading of fires and allowing a detection of fires and effective fire extinguishing actions as well as the escape and rescuing of humans.

Forced reactions under normal operational loads

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

Fuel assembly damage, severe

Degradation of the fuel assembly by e.g. melting or exothermal oxidation (zirconium-water-reaction) leading to a loss of the fuel rod cladding as a barrier and formation of flammable and explosive gases.

.

Fuel rod damage

Synonym for *cladding damage*.

G

Grid connection

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

H

Hazard

A situation that poses a level of threat to the installation and / or the environment. An external hazard could cause internal hazards or internal events.

Hazard, human-induced

An accidental event outside the plant area that is caused by human activities.

High-energy

Operating pressure greater than or equal to 20 bar or operating temperature greater than or equal to 100°C.

House load supply

The entirety of those *plant components* that serve to supply power to the connected electrical loads and to feed power into the *emergency power system*.

House load operation

The electrical power supply required for supplying the electrical loads necessary for operation of a power plant unit and for supplying the *emergency power system*. It may be supplied by the main generator, the *main* or *standby grid*, or from other external grids.

Human error

Non-compliance with a requirement during a personnel action.

Human factors

A body of scientific facts about human characteristics. The term covers all biomedical, psychological, and psycho-social considerations; it includes, but is not limited to, principles and applications in the areas of human factors engineering, personnel selection, training, job performance aids, and human performance evaluation (*see Human factors engineering*).

Human factors engineering

The application of knowledge about human capabilities and limitations to plant, system, and equipment design. Human factors engineering provides reasonable assurance that the design of the plant, systems, equipment, human tasks, and the work environment

are compatible with the sensory, perceptual, cognitive, and physical attributes of the personnel who operate, maintain, and support the plant (*see Human factors*).

I

Impact

Forces or media with physical, chemical or biological effects or a combination thereof acting on *installations.*

Incorporation

Intake of radioactive materials into the human body.

Independency of equipment

Equipment that possesses both of the following characteristics:

a) The ability to perform its required function is unaffected by the operation or failure of other equipment;

b) The ability to perform its function is unaffected by the occurrence of the effects resulting from the postulated initiating event for which it is required to function.

In-service inspection

Inspection performed at specified intervals.

Inspection

Measure for the identification and assessment of the actual condition of *structures, systems and components*.

Installation, instrumentation and control

Installation for the execution of *instrumentation and control functions*.

Installation, safety-relevant

Installation

- whose *failure* leads to uncontrollable *event sequences*, or
- that is required for effective and reliable control of postulated single initiating events, including *the auxiliary and supply systems* required for it, or
- that is required for effective and reliable prevention of events, including the *auxiliary and supply systems* required for it, or
- that serves the compliance with and *monitoring* of specified radiological values, in particular by maintenance of the required effectiveness of barriers and *retention functions*, or
- that serves the performance of tasks with safety-related significance which is not assigned to the above-mentioned conditions.

Instrumentation and control

The entirety of the instrumentation and control *installations* for the performance of *instrumentation and control functions*. *Instrumentation and control installations* comprise automatic *installations* as well as the installations for process control by an operator.

Instrumentation and control function

Function for measuring, managing, controlling, monitoring, recording and protecting a process or an *installation*

Integrity

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

Item important to safety

An item that is part of a system and/or whose malfunction or failure could lead to radiation exposure of the site personnel or members of the public. Items important to safety include:

- Those *structures, systems and components* whose malfunction or failure could lead to undue radiation exposure of site personnel or members of the public;
- Those *structures, systems and components* that *avoid* anticipated operational occurrences from leading to accident conditions;
- Those *structures, sytems and components* that *prevent* postulated single initiating events from escalating to more severe accident conditions;
- Those *structures, systems and components* that *avoid* postulated multiple failure event from escalating to core melt scenario;
- Those features that are provided to mitigate the consequences of malfunction or failure of *structures, systems and components.*

Interlock

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

Internal hazard

Impacts resulting from occurrences within the plant site (e.g. fire, plant-internal flooding).

Internal event

An event primary caused by credible equipment failures or operator errors.

Internal flooding

Floodings in buildings or at the plant site not being due to an *external event*.

L

Leak

Continuous or discontinuous outflow of media from the respective enclosures (e.g. vessels, piping systems, fuel pool) with an outflow rate to such a high level that *safety systems* are demanded.

Leak, large

Leak with an outflow surface > 0.1 A (A: cross-sectional area of the piping considered).

Leak, medium

Leak with an outflow surface ≤ 0.1 A (A: cross-sectional area of the piping considered) 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 postulated single initiating events.

Leak, small

Leak with an outflow surface ≤ 0.1 A (A: cross-sectional area of the piping considered) and where, for PWRs, secondary-side heat removal is necessary for the control of postulated single initiating events.

Leakage

Continuous or discontinuous outflow of media from the respective enclosures (e.g. vessels, piping systems, fuel pool) with an outflow rate that remains at such a low level that *safety systems* are not demanded.

Licensee [19]

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 corporation as licensee of the nuclear power plant, the attending to this responsibility by the corporate management, i.e. the board members, general managers or another body of this corporation which is authorised to represent by law, statutes or contract, as well as the tasks, responsibilities and authorisations of other persons and organisational units of the company that are derived from the licensee's responsibility.

Life cycle of the I&C system

A process, that includes following aspects:

- Design,
- Development,
- Integration and testing,
- Acceptance and installation,
- Deployment,
- Maintenance,
- Obsolescence and replacement

Limitation system

Instrumentation and control *installation* with one of the following functions:

- Limiting *process variables* to pre-set values in order to increase the availability of the plant.
- 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 variable* values to maintain initial conditions for postulated single initiating events to be considered.

[19] To be checked with dutch legal framework.

Loss-of-coolant accident

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

Low-power and shutdown operation

The *operating phases* that do not serve a targeted nuclear heat production (*operating phases B to F)*.

M

Main grid

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

Main grid connection

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

Main heat sink

The main heat sink is the condenser in the secondary cooling loop. See also *ultimate heat sink.*

Maintenance

The entirety of the *measures* for maintenance and restoration of the specified condition as well as for the identification and assessment of the actual condition (including *in-service inspection*). Maintenance is subdivided into *inspection*, servicing and repair.

Measure

Action, instruction or organisational activity or organisational process.

Monitoring

Collective term for all kinds of controlled recording of operating parameters, including a comparison with specified values.

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

Multiple failure of safety systems

Event sequence with *failures of safety systems* such that sufficient effectiveness of safety functions for the control of postulated single initiating events is no longer given. These are postulated multiple failure events on level of defence 3b such as

- anticipated transient without scram (ATWS), and
- combinations of failures selected on the basis of a risk assessment.

N

Normal operation

The operating conditions and processes during functional condition of the installations (undisturbed condition), including *in-service inspections* and *maintenance* processes (*level of defence 1*).

Normal operation, specified

The mode of operation for which a plant has been intended and designed and for which it is suitable according to its technical purpose, comprising the operating conditions and processes

- under functional conditions of the installations (undisturbed operating condition, normal operation, level of defence 1),
- of abnormal operation (disturbed operating condition, anticipated operational occurrence, level of defence 2), as well as
- during maintenance processes (inspection, servicing, repair).

O

Operability

Ability of an *installation* to fulfil the tasks specified by the corresponding mechanical, electrical or another function.

Operating procedures

All written documents that are needed for the operation of the plant. They include, in particular, the operating manual, emergency operating procedures, testing manual, and procedural and working instructions.

Operational limits and conditions

A set of rules setting forth parameter limits, the functional capability and the performance levels of equipment and personnel approved by the regulatory body for safe operation of an authorized facility.

Operation conditions monitoring

Controlled recording of operating parameters, including a comparison with specified values.

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

Operation, safe

The safe operation of a plant comprises the nuclear safety of the plant, the safety of the environment from ionising radiation, and the protection of all individuals inside the plant.

P

Passive system

A passive *system* is system which relies on a passive process to fulfil the intended safety function.

A passive system could rely on active components for the initiation of the passive process. However, those active components

- shall not rely on actuation by processed signals,
- shall not need external power sources or forces and
- shall not rely on manual initiation.

In cases were energy is needed to initiate the process, the energy shall be supplied from stored sources.

Physical separation

Arrangement of redundant subsystems with spatial distance or separated by appropriate *structures*.

Plant component

Any structural, mechanical, process-based, electrical or other technical part of a plant. Synonym is: *system.*

Plant condition

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

Plant condition, controlled

Plant condition after occurrence of an *event,* characterised in that the *acceptance targets* and *acceptance criteria* are complied with and the relevant *safety variables* have reached sufficiently stationary values.

Sufficiently stationary conditions are conditions in which the *safety variables* are so stationary or in which the *safety margin* to the *acceptance criteria* is constantly increasing in such a way that a sufficiently long period of time is available for the analysis and as-

sessment of the *plant condition* to be able to carry out further actions (e.g. *for accident treatment*) in the case of an unfavourable change in *safety variables*.

Plant condition, safe

Plant condition after occurrence of a design-basis accident characterised in that a *controlled plant condition* is given and at least the safety-related requirements of a comparable low-power and shutdown operation phase as described in the operating manual are fulfilled.

Plant state

Plant states consist of the operational states (normal operation and anticipated operational occurrences) and the accident conditions (accidents with and without core melt).

Plant structure

Part of the plant assembled from building products (building materials and component parts) and connected with the ground.

Power density oscillation (global, regional)

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

- 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 operating phase of a nuclear power plant in which nuclear heat is produced in a targeted manner (*operating phase A*).

Practical elimination

The possibility of certain conditions occurring is considered to have been practically eliminated if it is physically impossible for the conditions to occur or if the conditions can be considered with a high level of confidence to be extremely unlikely to arise.

to prevent

Events and event sequences shall be prevented, if items important to safety and procedures with a higher level of reliability are not available on a higher level of defence in depth. Consequently, the development of events or event sequences on level of defence 3a to such events or event sequences on levels of defence 3b or 4 have to be prevented.

Primary circuit

System area which comprises the *reactor coolant pressure boundary* in PWR plants.

Primary coolant

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

Procedure

A series of specified actions conducted in a certain order or manner. The set of actions to be taken to conduct an activity or to perform a process is typically specified in a set of instructions.

Process variable

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

Programmable logic device (PLD)

An electronic module used to build reconfigurable digital circuits.

Protection goal

Fundamental *safety function* that comprises different subordinate safety functions to be ensured for fulfilment of the respective *acceptance targets and acceptance criteria*.
The protection goals are:

d) reactivity control

e) fuel cooling

f) confinement of the radioactive materials.

Protective action

The actuation or operation of active *safety systems* that are needed for the control of events.

Q

Qualification of persons

The existence of knowledge, abilities (physical and psychical) and skills (learnt or trained behaviour patterns) as well as attitudes to be able to behave according to the demands.

R

Reactor coolant

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

Reactor coolant pressure boundary

Entirety of all pressure-retaining boundaries of the *components* of the pressure zone of the reactor pressure vessel up to and including the first isolating valve; for piping of the pressure zone of the reactor pressure vessel penetrating the containment, up to the first isolating valve outside the containment.

Reactor coolant system

System which comprises the *reactor coolant pressure boundary* in PWR and BWR.

Reactor protection system

The part of the *safety system* which monitors and processes the *process variables* relevant for safety and initiates *protective actions* for the prevention of undue impacts and registration of *design-basis accidents* (*level of defence 3a*) in order to keep the condition of the reactor plant within safe limits.

As part of the *safety system*, the reactor protection system comprises all *installations* for the recording of measured values, of signal conditioning, of the logic level and parts

of the control assigned to the individual drives for initiating *protective actions* as well as the functional group control.

Redundancy

Existence of more operable *installations* than required for the fulfilment of the intended function.

Redundancy wide event

Internal event or external event with the potential to cause the failure of several and redundant system trains.

Redundant

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

Refuelling

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

Release of radioactive materials

Inadvertent escape of radioactive materials from the enclosures provided into the plant or into the environment due to *events* on level of defence 3 or 4.

Research Reactor

A research reactor is a nuclear reactor used mainly for the

- generation and utilization of the neutron flux and ionizing radiation for research, develop-ment, isotope production, generation of positron beams, or any other purpose and
- Critical assemblies

with its associated experimental devices.

Residual heat

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

Residual-heat removal operation

Removal of residual heat with the *residual-heat removal system*.

Residual-heat removal system

System for the removal of *residual heat*.

Retention function

Measure and / or *installation* for the retention of radioactive materials, e.g. by filtering, water coverage, guided flow by maintenance of subatmospheric pressure, delay lines, vessels and other enclosures.

S

Safety analysis, deterministic

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

Safety analysis, probabilistic (PSA)

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

Safety demonstration

Verifiable information and data which demonstrate the fulfilment of requirements. A demonstration can be performed, among others, by analyses, experiments and measurements, test re-ports, certificates or by combining these forms of demonstrations.

Safety distance

Difference between the value of a parameter that is permissible according to an acceptance criterion and the value in case of which the loss of the required characteristic can no longer be excluded.

Safety function

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

Safety margin

Margin to protect against uncertainties.

Safety related item

An *item important to safety* that is not part of a safety system.

Safety system

A system important to safety, provided to ensure the safe shutdown of the reactor or the residual heat removal from the core, or to limit the consequences of anticipated operational occurrences and postulated single initiating events. Safety systems consist of the reactor protection system, the safety actuation systems and the safety system support features. Components of safety systems may be provided solely to perform safety functions, or may perform safety functions in some accident conditions and non-safety functions in other operational states.

Safety variable

Safety-relevant operating parameter and / or safety-relevant *process variable*.

Segregation

Avoiding interconnections (electric power, signals, piping, etc.) between redundant items important to safety to prevent mutual disturbances.

Self sufficiency criterion, 72 hours

Sufficient resources (e.g. fuel, cooling water, lubrication, etc.) are available on-site to ensure AC emergency power for at least 72 hours without off-site support. The plant is autonomous.

Separation, physical

Separation by geometry (distance, orientation, etc.), by appropriate barriers, or by a combination thereof.**Shutdown (of the plant)**

Controlled transfer of the plant from *operating phase* A or B to *operating phase* C.

Shutdown reactivity

The reactivity when all control devices are introducing their maximum negative reactivity to bring and maintain the reactor in a subcritical state.

Shutdown system

An *installation* that is able to transfer the reactor to a subcritical condition and maintain it in this condition.

Single failure concept

Concept of combining failure assumptions due to an active or passive *single failure* and maintenance processes.

Single failure

A *failure* that is additionally assumed to occur in *installations* in case of demand considered independent of the initiating event, but which does not occur as a consequence of the case of demand and is not known before the case of demand itself has occurred. The single failure also includes the consequential failures resulting from a postulated single failure.

A single failure has occurred if a *system part* of the *installation* does not fulfil its function upon demand. An incorrect operation that is possible under operating conditions and which results in a malfunction of the *installation* is equated with a single failure.

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

Software failure

Non-fulfilment of functions of the software.

Spiking effect

Release of gaseous fission products into the reactor coolant during shutdown of the reactor from full power operation in case of cladding defects.

Standby grid connection

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

Standby grid

The grid from which the nuclear power plant unit can be supplied with electrical energy via the *standby grid connection independently from the main grid*.

Startup

The controlled transfer of the plant to *operating phase A (power operation).*

Structural and procedural organisation

The structural organisation forms the hierarchical framework of an organisation in which the boundary conditions for dealing with the tasks to be performed are defined.

The procedural organisation regulated the work and information processes developing within these boundary conditions. The procedural organisation comprises all safety-relevant activities and processes in accordance with the requirements of the management system.

Structures, systems and components (SSC)

A general term encompassing all of the elements (items) of a facility or activity which contribute to protection and safety, except human factors. Structures are the passive elements: buildings, vessels, shielding, etc. A system comprises several components, assembled in such a way as to perform a specific (active) function. A component is a discrete element of a system. Examples of components are wires, transistors, integrated circuits, motors, relays, solenoids, pipes, fittings, pumps, tanks and valves.

Subassembly

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

Subsystem

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

Suitability for use

Ability of a *plant structure* to allow use as planned under the impacts considered in the planning.

Supplementary control room

Installation outside the *control room* from which in case of *failure* or unavailability of the *control room*, the reactor can be made subcritical, subcriticality can be maintained and heat removal from the core after its shutdown can be monitored and controlled.

Supply system

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

Support stability

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

Surface contamination

Radioactive substances on surfaces, or within solids, liquids or gases (including the human body), where their presence is unintended or undesirable, or the process giving rise to their presence in such places. The following types of contaminations can be distinguished:

- fixed contamination: Contamination other than non-fixed contamination
- non-fixed contamination: Contamination that can be removed from a surface during routine conditions of transport.

System assessment

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

System

See *structures, systems and components*.

Synonym for *plant component*.

Systematic failure

Failure due to the same cause.

T

Transient

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

U

Ultimate Heat sink

Medium (usually a water reservoir or the atmosphere) to which the residual-heat can be ultimately removed.

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 6
Requirements for research reactors
19.3.2015

Contents

1 General requirements

1 (1) Most research reactors have a small potential for hazards to the public compared with power reactors, but they may pose a greater potential for hazards to operators. This shall be taken into account in the design of the reactor in order to provide technical solutions prior to administrative rules. Hazards to the public, operators, users[20], and visitors shall be minimized. It shall be ensured by procedures, restrictions, and controls, that users have safe working conditions and that their activities will not affect the safety of the reactor.

1 (2) In this annex the term research reactor comprises the following facilities:

- Nuclear reactor used mainly for the generation and utilization of the neutron flux and ionizing radiation for research, development, isotope production, generation of positron beams, or any other purpose and
- Critical assemblies

with its associated experimental devices.

2 Appropriate application of the "Dutch Safety Requirements for Nuclear Reactors"

2 (1) The appropriate application is a structured method by means of which the stringency of application of requirements is balanced with the hazard potential of a specific research reactor. Such a structured method is necessary to consider the differences of a research reactor regarding its uniqueness in design and utilization in contrast to a nuclear power plant.

[20] A user of a research reactor is a person which is not a member of the operating organization of the research reactor (e.g. students, trainees, scientists, technicians of experimental devices etc.). Users are not involved in the operation of the reactor, except in case of reactors for training.

This method of appropriate application is a systematic approach of three steps:

- Step 1: Categorization of the research reactor according to the specific hazard potential
- Step 2: Analysis of specific factors which are not properly covered by the categorization in step 1
- Step 3: Decision and Justification of an appropriate application or waiving of requirements for nuclear power plants for the specific research reactor

2 (2) For an appropriate application of safety requirements defined in the “Dutch Safety Requirements for Nuclear Reactors” the research reactor shall be in the first step assigned to a risk category (see 2 (2c)) and to a cooling category (see 2 (2b)). The risk category takes the radiological impact into account and represents the fundamental safety function “confinement of the radioactive materials”. The cooling category considers the necessary measures for residual heat removal and represents the fundamental safety function “fuel cooling”.

2 (2a) The control of reactivity in a research reactor core has to be ensured at any time.

2 (2b) The research reactor shall be assigned to a cooling category:

- Cooling category 1: After shut-down from full power operation no cooling systems are necessary for residual heat removal from the reactor core to an ultimate heat sink. In the worst case scenario no cladding failure or melting of fuel element occurs.
- Cooling category 2: After shut-down from full power operation the reliability of passive cooling systems must be ensured to remove the residual heat from the reactor core to an ultimate heat sink. In the worst case scenario cladding failure and melting of fuel element shall be considered.
- Cooling category 3: After shut-down from full power operation the reliability of active cooling systems must be ensured to remove the residual

heat from the reactor core to an ultimate heat sink. In the worst case scenario cladding failure and melting of fuel element shall be considered.

2 (2c) The research reactor shall be assigned to a risk category:

- Risk category 1: The radiological impact is restricted to supervised or controlled areas[21]. In the worst case scenario appears no off-site radiological impact or only minor radiological impact;
- Risk category 2: Facilities with on-site radiological impact only. In the worst case scenario appears no off-site radiological impact or only minor radiological impact;
- Risk category 3: Facilities with off-site radiological impact and research reactors with the potential of severe core damage. In the worst case scenario limited protective measures in area and time are required.

The worst case scenario with the highest possible releases from an assumed damaged core leading to the highest doses shall be considered for categorization. A worst credible accident shall be considered for an unprotected plant as the worst case scenario. No credit shall be taken either from accident procedures or from confinement or retention functions.

2 (3) In the second step (mentioned in 2.1) the factors listed below shall be analysed to identify specific risk potentials, which could contradict an appropriate application or waiving of requirements proposed for a certain risk category or cooling category.

- The reactor power;
- The source term;
- The amount and enrichment of fissile and fissionable material;
- Spent fuel elements, high pressure systems, heating systems and the storage of flammables, which may affect the safety of the reactor;

[21] This could be the area of the reactor hall or external neutron guide hall.

- The type of fuel elements;
- The type and the mass of moderator, reflector and coolant;
- The amount of reactivity that can be introduced and its rate of introduction, reactivity control, and inherent and additional safety features;
- The quality of the containment structure or other means of confinement;
- The utilization of the reactor (experimental devices, tests and reactor physics experiments);
- Siting;
- Proximity to population groups.

These factors shall be checked for completeness for the particular research reactor.

2 (4) Based on the results of the first and second step the applicant / licensee shall justify its decision in case of an appropriate application or waiving of requirements described in the "Safety requirements for nuclear power plants". The applicant / licensee shall document the way of grading or waiving of a certain requirement and provide the justification in a traceable manner to the regulatory body[22].

2 (5) In principal for research reactors of risk category 3 or cooling category 3 the requirements for nuclear power plants defined in the "Dutch Safety Requirements for Nuclear Reactors" apply. Section 3 of this annex provides a guidance[23] for the appropriate application of the "Dutch Safety Requirements for Nuclear Reactors" to research reactors. However, this guidance shall not relief the applicant / licensee from its responsibility defined in 2 (4).

[22] This could be documented in the Preliminary Safety Analysis Report/ Final Safety Analysis Report (PSAR/FSAR).

[23] In Tables 3.1.1 to 3.6 generic research reactors were considered. Such tables shall be prepared by the licensee for a specific research reactor project.

3 Guidance for an appropriate application of the “Dutch Safety Requirements for Nuclear Reactors” on research reactors

3 (1) This section is intended to provide guidance how the approach of appropriate application could by applied on the safety requirements for nuclear power plants. As the design of research reactors could be manifold, each proposed grading or waiving of requirements shall be carefully checked and verified for a specific design of a research reactor.

For this purpose, the following tables give an overview of the appropriate application of the “Dutch Safety Requirements for Nuclear Reactors” to research reactors. In these tables, the first column gives the number of the corresponding requirement as defined in the main document. The three following columns represent the risk category as identified in this document in 2 (2c). Column five to seven give the respective cooling category as described in 2 (2b). The colouring of the cells indicates whether the specific requirement is generally applicable (green), grading is possible (yellow), or the requirement can be waived (red). The term “generally applicable” means that both risk and cooling categories shall be considered. In the case of a leading category, the specific description is given in the table.

3.1 Technical safety concept

3.1.1 Defence-in-depth concept

Requirement	Risk category 1	Risk category 2	Risk category 3	Cooling category 1	Cooling category 2	Cooling category 3
2 (1)	Defence in depth is an important design principle that must be applied to the design of a research reactor of any type or power level.					
2.1 (1)	Level 4 of defence in depth can be waived		Generally applicable			
2.1 (2)	Level 5 of defence in depth can be waived		Generally applicable			
2.1 (3a)	Generally applicable					
2.1 (3b)	Requirement can be waived		Generally applicable			
2.1 (4)	Generally applicable					
2.1 (5a)	Generally applicable					
2.1 (5b)	Generally applicable					
2.1 (6)	Generally applicable					
2.1 (7)	Generally applicable					
2.1 (8)	Generally applicable					
2.1 (9)	Generally applicable					
2.1 (10)	Generally applicable					
2.1 (11)	Generally applicable					

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

Requirement	Risk category 1	Risk category 2	Risk category 3	Cooling category 1	Cooling category 2	Cooling category 3
2.2 (1)	Generally applicable					

2.2 (2)	Generally applicable					
2.2 (3)	At least two barriers shall be included in the design. No containment is required.	At least two barriers shall be included in the design. A containment system could be necessary depending on the design of the reactor.	Generally applicable			
2.2 (4)	One barrier for the confinement of radioactive material shall be maintained.		Generally applicable			
2.2 (5)	Requirement can be waived		Generally applicable			

3.1.3 Concept of the fundamental safety objectives functions

Requirement	Risk category 1	Risk category 2	Risk category 3	Cooling category 1	Cooling category 2	Cooling category 3
2.3 (1)	In general, the fundamental safety functions cannot be graded.					
2.3 (2)						
For reactivity control	Generally applicable					
For fuel cooling				The heat sink could be the atmosphere in the reactor hall.	Generally applicable	Generally applicable
For the confinement of the radioactive materials	Instead of the containment the last barrier shall be considered.	Instead of containment confinement of radioactive material is sufficient.	Generally applicable			
2.3 (3)	Requirement can be waived		Generally applicable			
2.3 (4)	Generally applicable					

3.1.4 Evaluation of the site characteristics and potential effects of the nuclear reactor in the region

Requirement	Risk category 1	Risk category 2	Risk category 3	Cooling category 1	Cooling category 2	Cooling category 3
2.4 (1)	Requirement can be waived	In case of releases to verify minor radiological impacts.	Generally applicable			
2.4 (2)	Requirement can be waived	In case of releases to verify minor radiological impacts.	Generally applicable			
2.4 (3)	Requirement can be waived	In case of releases to verify minor radiological impacts.	Generally applicable			
2.4 (4)	Requirement can be waived	In case of releases to verify minor radiological impacts.	Generally applicable			
2.4 (5)	Requirement can be waived	In case of releases to verify minor radiological impacts.	Generally applicable			
2.4 (6)	Requirement can be waived	In case of releases to verify minor radiological impacts.	Generally applicable			
2.4 (7)	Requirement can be waived	In case of releases to verify minor radiological impacts.	Generally applicable			
2.4 (8)	Requirement can be waived	In case of releases to verify minor radiological impacts.	Generally applicable			
2.4 (9)	Requirement can be waived	In case of releases to verify minor radiological impacts.	Generally applicable			
2.4 (10)	Requirement can be waived	Generally applicable				

2.4 (11)	Requirement can be waived	Generally applicable				
2.4 (12)	Generally applicable					
2.4 (13)	Requirement can be waived.	In case of a multiple research reactor site, radiological consequences of all research reactors simultaneously in accident conditions need to be estimated.	Generally applicable, if more than one research reactor is located at the same site			

3.1.5 Concept of protection against internal and external hazards

Requirement	Risk category 1	Risk category 2	Risk category 3	Cooling category 1	Cooling category 2	Cooling category 3
2.5 (1)	Only fundamental safety function "control of reactivity" shall be considered	Generally applicable				
2.5 (2)	Requirement can be waived	Generally applicable				
2.5 (3)				Requirement can be waived		Generally applicable

3.1.6 Radiological safety objectives

Requirement	Risk category 1	Risk category 2	Risk category 3	Cooling category 1	Cooling category 2	Cooling category 3
2.6 (1)	Requirements for level 4 of defence in depth		Generally applicable			

	can be waived					
2.6 (2)	Generally applicable					

3.2 Technical requirements

3.2.1 Overall requirements

Requirement	Risk category 1	Risk category 2	Risk category 3	Cooling category 1	Cooling category 2	Cooling category 3
3.1 (1)	Generally applicable					
3.1 (2)	Generally applicable					
3.1 (3)	Generally applicable					
3.1 (4)	Requirement can be waived	Applies only for level 3b of defence in depth.	Generally applicable			
3.1 (5)	Generally applicable					
3.1 (6)	Generally applicable					
3.1 (7)	Generally applicable					
3.1 (8)	Generally applicable					
3.1 (9)	Applying only the single failure criterion (n+1) could be possible if core damage is practically eliminated.	Applying only the single failure criterion (n+1) could be possible. It shall be demonstrated, that the core damage frequency is not significantly increased. In such cases maintenance shall only be permitted during shutdown states as specified in	Generally applicable			

Requirement	Risk category 1	Risk category 2	Risk category 3	Cooling category 1	Cooling category 2	Cooling category 3
		the operational limits and conditions.				
3.1 (10)	Generally applicable					
3.1 (11)	Generally applicable					
3.1 (12)	Generally applicable					
3.1 (12a)	Requirement can be waived	Generally applicable				
3.1 (12b)	Generally applicable					
3.1 (12c)	Requirement can be waived	Generally applicable				
3.1 (13)	Requirement can be waived	Shall be applied to the design of control room displays and audible signals for parameters important to safety of the reactor.	Generally applicable			
3.1 (14)	Generally applicable					

3.2.2 Requirements for the design of the reactor core and the shutdown systems

Requirement	Risk category 1	Risk category 2	Risk category 3	Cooling category 1	Cooling category 2	Cooling category 3
3.2 (1)	Generally applicable					
3.2 (2)	Generally applicable					

Requirement	Risk category 1	Risk category 2	Risk category 3	Cooling category 1	Cooling category 2	Cooling category 3
3.2 (3)	Generally applicable					
3.2 (4)	Generally applicable					
3.2 (5)	Generally applicable					
3.2 (6)	The diverse shutdown system could be different to the injection of soluble neutron absorbers					
3.2 (7)	Generally applicable					
3.2 (8)	Generally applicable					
3.2 (9)	Reactivity variations due to samples shall be taken into account.					
3.2 (10)	The requirements for pressurized water reactors (PWR) and boiling water reactors (BWR) can be waived. Requirements for criticality control of research reactors are provided in section 4. 2 of Annex 6.					

3.2.3 Requirements for the systems for fuel cooling in the reactor core

Requirement	Risk category 1	Risk category 2	Risk category 3	Cooling category 1	Cooling category 2	Cooling category 3
3.3 (1)				Requirement can be waived	Generally applicable	
3.3 (2)				Requirement can be waived	Requirement for maintenance can be waived	Generally applicable
3.3 (3)				Requirement can be waived	In case of loss of coolant systems for refilling the reactor pool shall be provid-ed.	Generally applicable

Requirement	Risk category 1	Risk category 2	Risk category 3	Cooling category 1	Cooling category 2	Cooling category 3
3.3 (4)				Requirement can be waived	If the heat transfer to an ultimate heat sink cannot be re-established in due time, a redundant residual-heat removal system shall be provided.	Generally applicable
3.3 (5)				Requirement can be waived	Sufficient cooling water shall be provided to ensure water coverage of the fuel.	Generally applicable
3.3 (6)				Requirement can be waived	Generally applicable	

3.2.4 Requirements for the reactor coolant pressure boundary and the pressure-retaining walls of components of external systems an activity retaining components of systems outside the reactor coolant pressure boundary (“external systems”)

Requirement	Risk category 1	Risk category 2	Risk category 3	Cooling category 1	Cooling category 2	Cooling category 3
3.4 (1)				Requirement can be waived	Requirement shall be adapted to the relevant barrier depending on the design of the reactor.	Generally applicable
3.4 (2)				Requirement can be waived	Requirement shall be applied on piping systems to ensure heat transfer to an ultimate heat sink.	Generally applicable
3.4 (3)				Requirement can be waived	Requirement shall be adapted to the relevant barrier depending on the design of the reactor.	Generally applicable
3.4 (4)				Requirement can be waived	Requirement shall be applied on piping systems to ensure heat transfer to an ultimate heat sink.	Generally applicable
3.4 (5a) 3.4 (5b)				Requirement can be waived		Generally applicable
3.4 (6)				Requirement can be waived		Generally applicable
3.4 (7)				Requirement can be waived	In case of swimming pool reactors restricted to piping.	Generally applicable

3.2.5 Requirements for structures

Requirement	Risk category 1	Risk category 2	Risk category 3	Cooling category 1	Cooling category 2	Cooling category 3
3.5 (1)	Generally applicable					

3.2.6 Requirements for the containment system

Requirement	Risk category 1	Risk category 2	Risk category 3	Cooling category 1	Cooling category 2	Cooling category 3
3.6 (1)	No containment is required, but confinement of radioactive material shall be ensured.	In case the confinement of radioactive material cannot be reliably ensured to fulfil radiological objectives, containment shall be implemented.	Generally applicable			
3.6 (2)	Requirement can be waived.	No containment is required, but confinement of radioactive material shall be ensured. The required degree of leaktightness of the reactor building shall and the requirements for the ventilation system shall be determined in accordance with the safety analysis of the reactor and its utilization.	Generally applicable			
3.6 (3)	Requirement can be waived.	Applies only, if the containment is part of the design. The	Generally applicable			

Requirement	Risk category 1	Risk category 2	Risk category 3	Cooling category 1	Cooling category 2	Cooling category 3
		confinement or retention function shall be able to reliably fulfil the radiological objectives.				
3.6 (4)	Requirement can be waived.		Generally applicable			
3.6 (5)	For shielding of direct radiation no credit shall be taken from the surrounding building.	If the surrounding building is essential for the confinement of the radioactive material, it shall be designed to protect the reactor against external hazards.	Generally applicable			
3.6 (6)	Requirement can be waived	Generally applicable				
3.6 (6b)	Requirement can be waived	Gemerally applicable				
3.6 (7)	Requirement can be waived	In case of accidents on levels 3a and 3b of defence in depth the confinement function shall not be endangered.	Generally applicable			
3.6 (8)	Requirement can be waived		Generally applicable			
3.6 (9)	Requirement can be waived	If radioactive materials could be emitted into the reactor hall, air locks shall be provided to ensure the confinement and	Generally applicable			

Requirement	Risk category 1	Risk category 2	Risk category 3	Cooling category 1	Cooling category 2	Cooling category 3
		retention function.				
3.6 (10)	Requirement can be waived.	Generally applicable				
3.6 (11)	Requirement can be waived	Applies only when containment is part of the design.	Generally applicable			
3.6 (12)	Requirement can be waived	No pipes in contact with the reactor coolant or transporting radioactive fluids shall penetrate the containment.				
3.6 (13)	Requirement can be waived	Applies only when containment is part of the design. Isolation of the containment shall be realised by a double wall structure of the penetrating beam tubes (see also Annex 6, para. 4.3 (6)).	In addition, isolation of the containment shall be realised by a double wall structure of the penetrating beam tubes (see also Annex 6, para. 4.3 (6)).			

3.2.7 Requirements for instrumentation and control system (I&C)

Requirement	Risk category 1	Risk category 2	Risk category 3	Cooling category 1	Cooling category 2	Cooling category 3
3.7 (1)	Generally applicable					
3.7 (2)	Generally applicable					
3.7 (3)	Generally applicable					
3.7 (4)	Generally applicable					
3.7 (5)	Generally applicable					

3.7 (6)	Generally applicable
3.7 (7)	Generally applicable
3.7 (8)	Generally applicable
3.7 (9)	Generally applicable
3.7 (10)	Generally applicable
3.7 (11)	Generally applicable
3.7 (12)	Generally applicable
3.7 (13)	Generally applicable
3.7 (14)	Generally applicable

3.2.8 Requirements for control rooms and emergency response facilities

Requirement	Risk category 1	Risk category 2	Risk category 3	Cooling category 1	Cooling category 2	Cooling category 3
3.8 (1)	Generally applicable					
3.8 (2)	A remote emergency shutdown of the reactor shall be possible from outside the reactor hall.	A supplementary control room shall be provided, if the control room has to be deemed unavailable due to the condition at levels 3a and 3b of defence in depth.	Generally applicable			
3.8 (3a)	Requirement can be waived	Generally applicable				
3.8 (3b)	Requirement can be waived	The emergency control centre can be limited to on-site emergency response.	Generally applicable			
3.8 (3c)	Requirement can be waived	Generally applicable				
3.8 (4)	Requirement can be waived	Generally applicable				

Requirement	Risk category 1	Risk category 2	Risk category 3	Cooling category 1	Cooling category 2	Cooling category 3
3.8 (5)	Requirement can be waived	The supplementary control room is only needed for shutdown and ensuring subcriticality. The radiological conditions in the reactor hall and on-site shall be monitored.	Generally applicable			
3.8 (6)	Generally applicable					
3.8 (7)	Requirement can be waived		Generally applicable			
3.8 (8)	Requirement can be waived		Generally applicable			
3.8 (9)	Requirement applies only for the reactor hall / control room.	Requirement applies only for the control room / supplementary control room	Generally applicable			

3.2.9 Requirements for the electrical energy supply

Requirement	Risk category 1	Risk category 2	Risk category 3	Cooling category 1	Cooling category 2	Cooling category 3
3.9 (1)	Generally applicable					

Requirement	Risk category 1	Risk category 2	Risk category 3	Cooling category 1	Cooling category 2	Cooling category 3
3.9 (2)	No emergency diesel generators are required. Shutdown systems of the reactor shall be designed in such a way that in case of loss of offsite power the reactor will be automatically shut down (fail safe principle).	One grid connection is sufficient. Emergency power shall be provided for systems to shut down the reactor and to monitor relevant parameter and radiological conditions inside the reactor hall an on-site.	Generally applicable			
	Requirement on house load operation utilizing the main generator can be waived.					
3.9 (3)	No alternate emergency power supply facilities are required. Shutdown systems of the reactor shall be designed in such a way that in case of loss of offsite power the reactor will be automatically shut down (fail safe principle).		Generally applicable			
3.9 (4)	Generally applicable					
3.9 (5)	Generally applicable					
3.9 (6)				Requirement can be waived.		Generally applicable
3.9 (7)				Requirement can be waived.		Generally applicable
3.9 (8)				Requirement can be waived.	Only for items important to safety to ensure confinement of radioactive material.	Generally applicable

3.2.10 Requirements for the handling and storage of the fuel assemblies

Requirement	Risk category 1	Risk category 2	Risk category 3	Cooling category 1	Cooling category 2	Cooling category 3
3.10 (1)	Generally applicable					
3.10 (2)	Generally applicable					
3.10 (3)				Requirement can be waived	The self-sufficient criterion can be waived	Generally applicable
3.10 (4)				Requirement can be waived	A diverse heat sink shall be provided in case of the time needed to re-establish an ultimate heat sink is too short and put the integrity of the fuel rods on risk.	Generally applica-ble
3.10 (5)	Generally applicable					

3.2.11 Requirements for radiation protection

Requirement	Risk category 1	Risk category 2	Risk category 3	Cooling category 1	Cooling category 2	Cooling category 3
3.11 (1)	Generally applicable					
3.11 (2)	Generally applicable					
3.11 (3)	Only for levels 1 to 3b of defence in depth		Generally applicable			
3.11 (4)	Generally applicable					
3.11 (5)	Generally applicable					
3.11 (6)	Only for planned releases during normal operation	Generally applicable				
3.11 (7)	Generally applicable					
3.11 (8)	Generally applicable					

3.2.12 Requirements for waste management

Requirement	Risk category 1	Risk category 2	Risk category 3	Cooling category 1	Cooling category 2	Cooling category 3
3.12 (1)	Additional requirement: In case of on-site storage of radioactive waste the volume and characteristics of the waste from irradiated equipment of dismantled experimental devices and samples shall be estimated. The measured or estimated activities shall be evaluated and the safe storage of the radioactive waste shall be demonstrated.					

3.3 Postulated operating conditions and events

3.3.1 Operating conditions, anticipated operational occurrences and accidents (Level of defence 1 – 3a)

Requirement	Risk category 1	Risk category 2	Risk category 3	Cooling category 1	Cooling category 2	Cooling category 3
4.1 (1)	Generally applicable					
4.1 (2)	Generally applicable					
4.1 (3)	Generally applicable					

3.3.2 Events involving multiple failure of safety systems (Level of defence 3b)

Requirement	Risk category 1	Risk category 2	Risk category 3	Cooling category 1	Cooling category 2	Cooling category 3
4.2 (1)	Generally applicable					
4.2 (2)	Requirement can be waived		Generally applicable			
4.2 (3)				Requirement can be waived		Applies only if active cooling of the spent fuel storage pool is necessary
4.2 (4)	Generally applicable					

3.3.3 Accidents with core melt (Level of defence 4)

Requirement	Risk category 1	Risk category 2	Risk category 3	Cooling category 1	Cooling category 2	Cooling category 3
4.3 (1)	Requirement can be waived		Generally applicable			

3.3.4 Internal and external hazards

Requirement	Risk category 1	Risk category 2	Risk category 3	Cooling category 1	Cooling category 2	Cooling category 3
4.4 (1)	Generally applicable					
4.4 (2)	Generally applicable					
4.4 (3	Generally applicable					
4.4 (4)	Generally applicable					

3.4 Requirements for the safety demonstration

Requirement	Risk category 1	Risk category 2	Risk category 3	Cooling category 1	Cooling category 2	Cooling category 3
5 (1)	Generally applicable					
5 (2)	Generally applicable					
5 (3)	Generally applicable					
5 (4)	Generally applicable					
5 (5)	Generally applicable					
5 (6)	Generally applicable					
5 (7)	Events are provided in section 6 of this annex					
5 (8a)	Requirement can be waived.		Generally applicable			
5 (8b)	Requirement can be waived.		Generally applicable			
5 (8c)	Requirement can be waived.		Generally applicable			
5 (8)	Generally applicable					
5 (9)	Generally applicable					
5 (10)	Generally applicable					
5 (11)	Generally applicable					
5 (12)	Generally applicable					
5 (13)	Generally applicable					
5 (14)	Generally applicable					

3.5 Requirements for operating rules

Requirement	Risk category 1	Risk category 2	Risk category 3	Cooling category 1	Cooling category 2	Cooling category 3
6 (1)	Description of provision to control events at levels 1 to 3b of defence in depth. No severe accident management guidelines (SAMG) are required	Description of provision to control events on levels 1 to 3b of defence in depth. No severe accident management guidelines (SAMG) are required.	Generally applicable			
6 (2)	Documents shall only be available in the control room.	Applies only if a supplementary control room is part of the design	Generally applicable			
	Requirement for documents needed for the work of the emergency response team can be waived.					
6 (3)	Generally applicable					
6 (4)	Generally applicable					
6 (5)	Generally applicable					

3.6 Requirements for documentation

Requirement	Risk category 1	Risk category 2	Risk category 3	Cooling category 1	Cooling category 2	Cooling category 3
7 (1)	Generally applicable					

4 Specific requirements for research reactors

4.1 General requirements

4.1 (1) The reactor designer shall consider not only the reactor itself but also any associated facilities that may affect safety. In addition, the reactor designer shall also consider the effects of the reactor as designed on the associated facilities and the implications of the design in all the stages of the reactor's lifetime (e.g. in terms of service conditions, electromagnetic fields and other interferences).

4.1 (2) In order to come to a safe design, a close liaison between the reactor designer and the operating organization is required. The designer shall arrange for the orderly preparation, presentation and submission of design documents to the operating organization for use in the preparation of the safety analysis report (SAR).

4.1 (3) The mode of operation (e.g. operation on demand rather than continuous operation, operation at different power levels, operation with different core configurations and operation with different nuclear fuels) and the stability of the reactor at different levels of operating power shall be given due consideration in the design of the safety systems.

4.1 (4) All system, structures, and components shall be designed in such a way, that the intended function is ensured over the whole lifetime. The effects of intense radiation fields on changing the material properties shall be taken into account.

Note: Details are provided in IAEA Safety Standards Specific Safety Guide No. SSG-24 "Safety in the Utilization and Modification of Research Reactors"

4.1 (5) Where no data are available on materials, a suitable programme of inspection and periodic testing of materials shall be put in place. The results of this programme shall be used in reviewing the adequacy of the design at

appropriate intervals. The design shall consider provisions for monitoring materials whose mechanical properties may change in service owing to such factors as stress corrosion or radiation induced changes. Improved safety factors may be achieved by the selection of materials of high strength or high melting point.

4.2 Reactor core and fuel design

4.2 (1) Analyses shall be performed to show that the intended irradiation conditions and limits (such as fission density, total fissions at the end of lifetime and neutron fluence) are acceptable and will not lead to undue deformation or swelling of the fuel elements. The anticipated upper limit of possible deformation shall be evaluated. These analyses shall be supported by data from experiments and from experience with irradiation. Consideration shall be given in the design of the fuel elements to the requirements relating to the long term management of irradiated elements.

4.2 (2) All foreseeable reactor core configurations from the initial core through to the equilibrium core for various appropriate operating schedules shall be considered in the core design.

4.2 (3) Perturbations in the neutron flux shall be evaluated, especially in the vicinity of items important to safety. Where experiments can be inserted, withdrawn or otherwise relocated while the reactor is at power, the effects on the power distribution in fuel assemblies and on the controllability of reactivity changes shall be carefully assessed.

4.2 (4) The maximum rate of addition of positive reactivity allowed by the reactivity control system or by an experiment shall be specified and shall be limited to values justified in the safety analysis report.

4.2 (5) Core configurations are frequently changed in research reactors and could affect the nuclear and thermal characteristic of the core. These effects shall be correctly determined and checked against the relevant conditions for nuclear and thermal safety before the reactor is put into operation.

4.2 (6) The shutdown reactivity shall be sufficient to safely shut down the reactor and maintain a subcritical state at levels 1 to 3b of defence in depth, if the control element with the highest reactivity value is completely drawn out and simultaneously the highest possible positive reactivity due to experiments is inserted. The possible amount of reactivity increase due to insertion, removal and / or potential failure modes of samples and experimental devices shall be taken into account The admissible maximum rate of addition of positive reactivity shall be justified in the safety analysis report and specified in the operational limits and conditions.

4.2 (7) The design of reactivity control devices shall take into account the wear-out and effects of irradiation, such as burn-up , changes in physical properties and the production of gas. Sufficient shutdown reactivity shall be ensured over the expected life time of the reactivity shutdown devices.

4.2 (8) In case of pulsed research reactors criticality safety shall be ensured by inherent safety. The reactor shall be designed in such a way that uncontrollable supercritical states are practically eliminated.

4.3 Reactor coolant system and related systems

4.3 (1) Research reactors belonging to cooling category 3 require that reactor coolant systems carrying activity shall be designed as closed systems.

4.3 (2) The residual heat shall be transported from the primary circuit with an intermediate cooling circuit to an ultimate heat sink. The heat exchanger will serve as a barrier for radioactive particles transported in the primary circuit. This requirement applies for cooling category 2 and cooling category 3 research reactors.

4.3 (3) If two fluid systems that are operating at different pressures are interconnected, either the systems shall both be designed to withstand the higher pressure, or provision shall be made to preclude the design pressure of the system operating at the lower pressure from being exceeded, on the assumption that a single failure occurs.

4.3 (4) In the design of water cooled reactors of cooling category 2 and 3 particular attention shall be paid to preventing the uncovering of the core. Special features, such as locating penetrations above the core, whenever feasible, siphon breaks and suitable isolation devices shall be used. High quality design and fabrication together with the characteristics of ease of inspection and testing and redundancy, where appropriate, shall be ensured.

4.3 (5) Flappers or equivalent systems for natural circulation cooling as part of the safety system, an additional safety feature, or a complementary safety feature shall fulfil the single failure criterion. Devices verifying the functioning and to providing signals to the reactor protection system shall be included.

4.3 (6) Beam tubes penetrating the barriers or which are located inside the pool shall be designed as double wall structure and sealed in such a way, that leakage through such penetrations is reliably prevented in order to avoid uncovering of the core.

4.4 Confinement of radioactive materials

4.4 (1) Where confinement of radioactive materials depends on the efficiency of filters, appropriate provision shall be made for in situ periodic testing of the efficiency of the filters.

4.4 (2) Materials used for the confinement, covering and coating shall be properly selected. The specification of methods of application shall ensure their required safety functions. If an interference with other safety functions cannot be avoided, the resulting deterioration of these safety systems shall be minimized.

4.5 Commissioning and operation

Experimental devices shall be given adequate consideration during the commissioning of the research reactor.

4.6 Human factors and ergonomic considerations

4.6 (1) Human factors are an important aspect in the safety of research reactors as the state of the reactor changes frequently and the operator has easy access to the reactor core and to experiments.

4.6 (2) Special consideration shall be given in design to ensure reliance on necessary administrative controls and procedures. Administrative procedures may include operating rules in the form of operational limits and conditions, which are derived from the design of the reactor and the safety analysis. Human factors and human-machine interfaces shall be given systematic consideration at an early stage of the design and throughout the entire design process.

4.6 (3) Persons manipulating experimental devices and materials in the vicinity of the reactor core shall adhere strictly to the procedures and restrictions established to prevent any nuclear or mechanical interference with the reactor.

4.7 Radiation protection

4.7 (1) Structural materials (such as core supports, grids and guide tubes), in particular those used near the core, shall be carefully chosen to limit the dose to personnel during operation, inspection, testing and maintenance, and decommissioning, as well as to fulfil their other functions. The effects of radionuclides (e.g. ^{16}N, ^{3}H, ^{41}Ar, ^{24}Na and ^{60}Co) produced by neutron activation in reactor process systems shall be given due consideration in the provision of radiation protection for people on and off the site. The expected activation of samples shall be estimated before irradiation and adequate radiation protection measures shall be defined.

4.7 (2) In the design shielding against neutron and gamma radiation shall be considered for the reactor as well as for the experimental devices and associated facilities (beam tubes, particle guides, facilities for neutron radiography, boron neutron capture therapy). Provisions shall be made for installing the necessary shielding associated with the future utilization of the reactor. Hazard analyses and shielding arrangements shall be given due consideration in relation to the use of beam tubes and other experimental devices.

4.7 (3) Records shall be kept of materials, samples, equipment and devices inserted into the reactor, and such items shall be retrieved and accounted for at the end of their irradiation. These records shall also include the measured or estimated activity of each item.

4.8 Extended shutdown

4.8 (1) Provision shall be made in the design to meet the needs arising in long shutdown periods, such as the needs for maintaining the conditions of the nuclear fuel, the coolant or the moderator, for the inspection, periodic testing and maintenance of the relevant systems, structures and components of the facility, and for providing physical protection. Special consideration shall be given to long living neutron poisons, which may affect the restarting of the reactor.

4.8 (2) The operating organization shall take appropriate measures during an extended shutdown to ensure that materials and components do not seriously degrade. The following measures shall be considered:

- Unloading the fuel elements from the reactor core to the storage racks;
- Changing the operational limits and conditions in accordance with the requirements for the shut-down reactor;
- Removing components for protective storage;
- Taking measures to prevent accelerated corrosion and ageing;
- Retaining adequate staff in the facility for the purposes of performing the necessary inspection, periodic testing and maintenance.

4.9 Advisory groups / safety committees

4.9 (1) One or more reactor advisory groups or safety committees that are independent of the reactor manager shall be established to advise the operating organization on:

- relevant aspects of the safety of the reactor and the safety of its utilization;
- on the safety assessment of design, commissioning and operational issues.

At least one of the groups or committees shall advice the reactor manager.

4.9 (2) The functions, authority, composition and terms of reference of such committees shall be documented.

4.9 (3) Members of such a group or groups shall be experts in different fields associated with the operation and design of the research reactor. External experts (i.e. from outside the organization) can be members of the advisory group / safety committee.

4.9 (4) The advisory groups / safety committees shall advise the reactor manager and the operating organisation in the following fields:

- proposed changes in the OLCs;
- proposed new equipment, systems or procedures having an impact on nuclear safety;
- proposed modification of items important to safety
- proposals of new tests, experiments, especially significant to nuclear safety;
- design of nuclear fuel elements and reactivity control elements;
- events that have to be reported to the regulatory body;
- periodic review of the operational performance and safety performance of the facility;

5 Utilization and modification

5 (1) Research reactors and their associated experimental devices are often modified in order to adapt their operational and experimental capabilities to changing requirements for their utilization.

Every modification of the research reactor or experimental devices shall be properly assessed, documented and reported in terms of its potential effects on safety. The reactor shall not be restarted without formal approval after the completion of modifications with major effects on safety.

5 (2) Special precautions shall be taken in the design in relation to the utilization and modification of the research reactor to ensure that the configuration of the reactor is known at all times. In particular, special consideration shall be given to experimental devices since:

a) It can cause hazards directly if it fails;

b) It can cause hazards indirectly by affecting the safe operation of the reactor;

c) It can increase the hazard due to an initiating event by its consequent failure and the effects of this on the event sequence.

5 (3) Any modification of the research reactor or experimental devices shall be assigned to one of the following categories according to its influence on the nuclear safety of the research reactor:

1. Experiments and modifications with major effects on safety
2. Experiments and modifications with significant effects on safety
3. Experiments and modifications with minor effects on safety
4. Experiments and modifications without impact on safety

Note: Details can be found in the IAEA Safety Standards Specific Safety Guide No. SSG-24 "Safety in the Utilization and Modification of Research Reactors"

5 (4) The design of an experiment or a modification project shall minimize the demands on the reactor protection system. Experimental devices shall be designed in such a way, that a safe condition can be achieved without actuating the reactor protection system.

5 (5) The activity and contamination of irradiated equipment and samples shall be evaluated in advance, under each of two assumptions:

- The most probable course of the experiment;
- The worst possible combination of equipment failures and human errors.

All operations connected with the handling, dismantling, post-irradiation examination, transport, and storage or disposal shall be taken into account in the design phase.

5.1 Experimental devices

5.1 (1) Experimental devices shall not adversely affect the safety of the reactor in any operational states. The experimental devices shall be designed in such a way that neither its operation nor its failure will result in

- an unacceptable change in reactivity for the reactor,
- a reduction of cooling capacity, or
- an unacceptable radiation exposure.

5.1 (2) Experimental devices with major effects on safety shall be designed to standards equivalent to those applied for the reactor itself and shall be fully compatible in terms of the used materials, the structural integrity and the provision for radiation protection.

5.1 (3) A design basis shall be established for each experimental device associated directly or indirectly with the reactor. The radioactive inventory of the experimental device as well as the potential for the generation or release of energy shall be taken into consideration. A safety analysis shall also be

performed, including an analysis of the damage caused by experimental devices during the postulated initiating events of the reactor.

5.1 (4) Items important to safety of experimental devices, which are interconnected with the reactor protection system, shall meet the requirements for quality and reliability of the reactor protection system. The possibility of deleterious interactions with the reactor protection system shall be assessed.

5.1 (5) If necessary for the safety of the reactor and the safety of the experiment, the design of the experiment shall provide appropriate monitoring of the parameters for experiments in the reactor control room.

5.1 (6) Experimental devices containing stored energy shall be equipped with adequate protection features to avoid damage of items important to safety in case of an unintended and uncontrolled release of the stored energy.

5.1 (7) Items important to safety used only to protect the experiment itself and which can be permitted to fail without causing a hazard on the reactor or to personal shall not be connected with the reactor control and reactor protection system. Appropriate requirements for quality and reliability can be applied with respect to safety-significance of the item important to safety.

5.1 (8) Requirements for the safe utilization of experimental devices and requirements for deciding which devices and experiments shall be referred to the regulatory body shall be included in the operational limits and conditions. Operational limits and conditions shall be prepared for the device and incorporated as appropriate into the operational limits and conditions of the research reactor. A preliminary decommissioning plan shall be prepared for the device.

5.1 (9) Where experimental devices penetrate the reactor boundaries, they shall be designed to preserve the means of confinement and shielding of the reactor. Protection systems for experimental devices shall be designed to protect both the device and the reactor.

5.1 (10) Potential activation of systems, structures, and components of experimental devices shall be estimated before experiments will be performed. This in-

cludes items for handling or manipulating of samples and experimental devices, especially in areas of the research reactor with high neutron flux densities. Materials with low neutron absorption cross sections shall be preferred.

5.1 (11) Adequate radiation protection measures and disposal of activated samples shall be arranged in advance. After performing an irradiation of a sample the activity of the sample shall be measured. The further handling of the probe shall be in accordance with the radiation protection decree.

5.1 (12) The use and handling of experimental devices shall be controlled by means of written procedures. Responsibilities of involved persons shall be defined. The possible effects on the reactor, particularly changes in reactivity, shall be taken into account in these procedures.

5.2 Modification Projects

5.2 (1) A modification project with major, significant or minor effects on safety shall be performed in three phases:

1. Pre-implementation phase
2. Implementation phase
3. Post-implementation phase

Note: Details can be found in the IAEA Safety Standards Specific Safety Guide No. SSG-24 "Safety in the Utilization and Modification of Research Reactors"

5.2 (2) Every proposed modification to an experiment or to the reactor that may have a major significance for safety shall be designed in accordance with the same principles as apply for the reactor itself.

5.2 (3) Utilization and modification projects having a major safety significance shall be subject to safety analyses and to procedures for design, construction and commissioning that are equivalent to those for the reactor itself.

5.2 (4) Any modifications made to experimental devices shall be subject to the same procedures for design, operation and approval as were followed for the original experimental device.

5.2 (5) For modification projects with major or significant effects on safety an assessment of the radiation exposure of the staff expected during or as a result of the modification project shall be prepared. Measures to reduce radiation exposures based on the principle of optimization of protection shall be described for all reactor states. Any potentially necessary mitigation measures shall be identified.

5.2 (6) The safety documentation shall be updated after the implementation phase and after the post-implementation. The documentation covering the design, operational limits and conditions, operating procedures, and other safety documentation shall be reviewed in advance to be used as a basis for approval for normal operation of the experiment or modified research reactor. The as-built description of the utilization or modification and the results of the commissioning process shall be included. Obsolete safety documentation shall be removed from service and archived.

6 List of postulated initiating events

6.1 Acceptance targets and acceptance criteria

6.1 (1) The acceptance targets and acceptance criteria of Annex 1 shall be applied. Where acceptance targets and acceptance criteria prescribed in Annex 1 cannot appropriately be applied, adequate surrogate acceptance targets and criteria for a specific research reactor design shall be provided by the applicant. The applicant shall provide complete and comprehensible information on the chosen surrogate acceptance targets and acceptance criteria.

6.1 (2) The acceptance criteria for the fuel in Annex 1 are provided for LWR fuel with UO_2 pellets and zirconium cladding. For research reactors these acceptance criteria shall be revised according to the specific research reactor fuel. The applicant shall provide complete and comprehensible information on fuel qualification.

6.1 (3) The specific characteristics of the research reactor type resulting in new kind of events have to be considered in the determination of the research reactor specific event list.

6.1 (4) For the research reactor specific application of the event list, the completeness and representative character of the events mentioned in the list shall be checked for levels 2 to 3b of defence in depth for all relevant operating conditions. The working steps described in section 2 (5) of Annex 1 shall be applied.

6.1 (5) Operating phases[24] shall be defined by the licence covering at least the following operational states: power and start-up operation, subcritical, refuelling and spent fuel storage. A further differentiation between hot and cold subcritical states depends

[24] See e.g. Tab. 1-1 and Tab. 1-2 of Annex 1.

on the specific reactor design. Operating phases with a reduced number of barriers, e.g. with opened primary loop normally closed during power operation, shall be defined depending on the specific research reactor design. Adequate operating phases shall be assigned to the events listed in Table 6-2.

6.2 Event list

No.	Event	Fundamental safety function	Operating phase[25]	Comment
Level of defence 2				
Change of flow rate in primary circuit				
R2-01	Loss of one primary pump	R,K	A-B	
R2-02	Loss of all primary pumps	R,K,B	A-B	
R2-03	Reduction of flow in primary loop	R,K	A-B	
Change of secondary-side heat removal				
R2-04	Loss of ultimate heat sink	R,K,B	A-B	
R2-05	Inadvertent closure of valves leading to significant changes in secondary cooling water flow rate.	K,B	A-B	
R2-06	Failure of a secondary cooling pump	R,K	A	

[25] Need to be adapted reactor specific according to Annex 6 para.6.1 (5)

No.	Event	Fundamental safety function	Operating phase[25]	Comment
R2-07	Failure of all secondary cooling pumps	R,K	A-B	
Loss of residual heat removal				
R2-08	Loss of a residual heat removal train including cooling chain	K,B	C-E	Note: Only if more than one cooling train is available
R2-09	Loss of all residual heat removal trains	K,B	C-E	
Loss of cooling systems of experimental devices				
R2-10	Failure of the cooling system of experimental devices	R,K,B	A-F	Note: Cold / hot neutron source Neutron converter Irradiation facilities
R2-11	Failure of the moderator tank cooling system	R,K,B	A-F	
R2-12	Failure of reactor pool cooling system	R,K,B	A-F	
Change of reactivity and power distribution				

No.	Event	Fundamental safety function	Operating phase[25]	Comment
R2-13	Malfunction in the reactor power control system	R,K	A	Note: Start-up accidents shall be taken into account Control rod follower failure / control drive failure shall be taken into account.
R2-14	Most unfavourable loading of a most reactive fuel assembly at wrong position	R,K	A,E	Additional boundary condition: Reactor start-up with not correctly positioned fuel assembly is analysed regarding protection goal K in operating phase A. Comment: - Protection goal R (subcriticality) in operating phase E - Protection goal K in operating phase A
R2-15	Insertion of a fuel element with higher reactivity than specified	R	E	Note: Loading of fuel element with higher reactivity than specified.
R2-16	Reactivity changes due to operation of cold neutron sources	R, K	A-B	Note: Operation of cold sources (e.g. H_2, D_2, CH_4) could influence the neutron spectrum in the vicinity of the cold source
R2-17	Reactivity changes due to operation of hot neutron sources	R,K	A-B	Note: Operation of hot sources (usually hot graphite) could influence the neutron spectrum in the vicinity of the hot source
R2-18	Reactivity changes due to opera-	R,K	A-B	Note:

No.	Event	Fundamental safety function	Operating phase[25]	Comment
	tion of neutron converters			The reactivity increase due to insertion of the converter plate shall be analysed.
R2-19	Reactivity changes due to operation of irradiation facilities	R,K	A-B	
R2-20	Reduction of reactivity worth of control and shut-down elements	R, K	A-E	
R2-21	Inadvertent drop or insertion of one or more control or absorber elements	R,K	A	
R2-22	Fast temperature transient of cooling medium	R,K	A-E	Note: Fast increase or decrease of moderator temperature shall be considered and the effects on k_{eff} shall be analysed.
Loss of energy supply				
R2-23	Loss of offsite power for 10 hours or less	R,K,B	A-E	Additional boundary condition: The restoration of the external electrical power supply has to be analysed as well.

Level of defence 3				
Level of defence 3a				
Change of flow rate in primary circuit				
R3a-01	Primary coolant pump seizure (locked rotor)	R,K,B	A-B	
R3a-02	Primary coolant pump shaft break	R,K,B	A-B	
R3a-03	Rupture of the primary coolant boundary leading to a loss of flow	R,K,B	A-F	Note: Rupture in baffles controlling the coolant flow through the reactor core without a loss of cooling medium
R3a-04	Reduction in coolant flow due to bypassing of the core			
R3a-05	Reduction in flow rate while storing spent fuel elements in storage rack		F	
R3a-06	Blockage of coolant flow while storing spent fuel elements in storage rack		F	
R3a-07	Fuel channel blockage	K	A-E	
Change of reactivity and power distribution				
R3a-08	Reactivity change due to leaks			

	leading to an exchange of D_2O and H_2O.			
R3a-09	Reactivity change due to flooding of beam tubes	R, K, B	A-F	Note: Flooding of beam tubes with coolant medium leading to the highest k_{eff} shall be considered.
R3a-10	Inadvertent withdrawal of the most effective control element or control element group with loss of limitation systems	R,K	A-B	
R3a-11	Inadvertent withdrawal of shut-down elements	R,K	B	Note: Subcriticality shall be maintained with control elements.
R3a-12	Ejection of the most effective con-trol or shutdown element	R,K	A-B	
R3a-13	Drop of a fuel element onto the moderator tank or reactor core	R,K	D-E	Note: Effects of H2O and D2O on criticality shall be analysed.
Loss of coolant				
R3a-14	Leak in the primary coolant boundary			
R3a-15	Leaks of beam tubes or other penetrations			
R3a-16	Inadvertent pump-down of reactor pool			
R3a-17	Leakage at the reservoir lining			
R3a-18	Leakage at reactor pool hatch			Note: Water level lower in one part of the pool.
R3a-19	Leckage in the reactor pool cool-ing system			

R3a-20	Leckage in the moderator cooling system			
Loss of energy supply				
R3a-21	Long term loss of offsite power (>10h)	R,K,B,S	A-F	
Failure of experimental devices with release of radioactive materials				
R3a-22	Damage of capsules of irradiation samples			
R3a-23	Meltdown of neutron converter			
R3a-24	Disruption of barriers of the cold source			
Handling of fuel assemblies				
R3a-25	Failure of the cladding of the fuel	B	A-E	
R3a-26	Drop of a fuel assembly while changing fuel assemblies			
R3a-27	Damage of a fuel assembly during handling			
R3a-28	Drop of fuel assembly transport cask			
R3a-29	Drop of heavy loads over reactor			

	pool or storage pool			
R3a-30	Inadvertent criticality in fuel storage	R	E	Note: Dry and wet storage of fresh and spent fuel
Level of defence 3b				
Anticipated transient without scram (ATWS)				
R3b-01	Maximum reactivity insertion by withdrawal of control elements on the basis of the operating conditions “full load”	R,K,B	A,B	
R3b-02	Loss of main heat sink with unavailable station service power supply		A,B	
Loss of energy supply				
R3b-03	Loss of off-site power cumulated with the failure of all emergency diesel generators	R,K,B	A-F	
Loss of component cooling				
R3b-04	Loss of the component cooling water system	R, K, B	A-F	
Loss of secondary-side heat removal				
R3b-05	Total loss of secondary site cooling water	R,K,B	A	