Note:
This is a translation of the RSK statement entitled “RSK-Verständnis der Sicherheitsphilosophie”.
In case of discrepancies between the English translation and the German original, the original shall prevail.

RSK statement
(460th meeting of the Reactor Safety Commission (RSK) on 29.08.2013)

(published in the Federal Gazette, Official Section, on 05.12.2013, B4)

RSK’s understanding of safety philosophy

Contents

1 Introduction

According to § 1, No. 2 of the Atomic Energy Act (*Atomgesetz* – AtG), life, health and real assets are to be protected against the hazards of nuclear energy and the harmful effects of ionising radiation. This is the fundamental safety objective. To achieve this safety objective, it must be ensured in particular that precautions have been taken as are necessary according to the state of the art in science and technology to prevent damage caused by the construction and operation of a nuclear facility. The facility must be designed and operated such that it can be reliably shut down and kept in shutdown state, residual heat can be removed and radiation exposure to personnel and the environment can be kept as low as possible even if below the dose limits specified by the provisions of the Atomic Energy Act and the statutory ordinances promulgated on the basis of this Act at any time during specified normal operation and design basis accidents. Moreover, organisational and technical measures are to be provided to the extent appropriate to mitigate the consequences of beyond design basis plant states.

The safety philosophy described below is intended to support a consistent interpretation of the technical and organisational requirements specified in the "Safety Requirements for Nuclear Power Plants" (*Sicherheitsanforderungen an Kernkraftwerke*) and a coherent classification of future new requirements according to the defence-in-depth concept.

2 Basis of nuclear safety

Man, technology and organisation are to be coordinated within an integral approach such that the fundamental safety objective is met and hazards to the environment of the nuclear power plant due to early or large releases[1] are excluded[2].

3 Basic requirements for organisation and personnel

The licensee shall ensure that

(1) the safety requirements are met by the plant design and the required quality state of the plant is maintained throughout the operating life. Here, the further development of the state of the art in science and technology, the safety-relevant experiences in construction and operation from the own and other plants, and all relevant ageing phenomena are to be taken into account

[1] **Early release:** any releases of radioactive material into the environment of the plant, caused by the early failure or bypass of the containment and requiring measures of the external accident management for the implementation of which there is not sufficient time available.

Large release: any releases of radioactive material into the environment of the plant requiring wide-area and long-lasting measures of the external accident management.

[2] **"excluded":** The occurrence of an event or event sequence or a state can be considered as excluded if it is physically impossible to occur or if it can be considered with a high degree of confidence to be extremely unlikely to arise. This applies, for example, for the superposition of two independent events, each being unlikely considered separately.

(2) through an effective management system, the technical, organisational and administrative prerequisites to ensure plant safety are given at any time and will be further developed by continuous improvements,

(3) a strong safety culture is developed in the organisation and is exemplified and encouraged in particular by the senior management throughout the corporate and plant hierarchy,

(4) the reliability and technical knowledge of plant personnel is ensured,

(5) tasks and responsibilities are assigned within the organisation by clear definitions,

(6) the necessary procedures for maintenance of a safe plant condition, for safe operation, for the control of events and for mitigation of their consequences are in place and effective,

(7) identified safety improvement potentials will be implemented as appropriate,

(8) the human and financial resources to ensure plant safety are provided.

4 Safety principles for the technical plant design

4.1 Principles

(1) In order to comply with the fundamental safety objective, the radioactive material present in the nuclear power plant shall be multiple confined by technical barriers and retention functions and its radiation shall be sufficiently shielded. The effectiveness of the barriers and retention functions shall be ensured by fulfilling the main safety functions

- control of reactivity,
- fuel cooling, and
- confinement of the radioactive material.

A defence-in-depth concept is to be realised that ensures for all events to be considered and classified according to the levels of defence, taking into account their frequency of occurrence, the fulfilment of the main safety functions and the preservation of barriers and retention functions to the extent necessary.

The objective of using different levels is to be able to compensate for faults and failures by further measures and installations.

(2) Inadmissible radiological consequences from

- technical or human-induced internal failure events to be postulated, or
- an event of external natural or man-made origin

shall be prevented by the implementation of the defence-in-depth concept. That is, the frequency of occurrence for event sequences that may lead to radiological consequences above the dose levels of §§ 46 and 47 or § 49 of the Radiation Protection Ordinance (StrlSchV) is to be kept sufficiently low. Event sequences with early or large releases of radioactive material are to be excluded.

(3) As part of the defence-in-depth concept, multi-level, effective and reliable measures and installations are to be provided, on the one hand to avoid operational occurrences and prevent accidents within the design basis and, on the other hand, to control operational occurrences and design basis accidents postulated nonetheless, as well as measures and installations to mitigate the consequences of beyond design basis plant states and to exclude event sequences with early or large releases.

4.2 Barrier concept

(1) The barrier concept comprises multiple barriers and retention functions for the confinement of radioactive material.

(2) The required number and design of the multiple barriers and retention functions has to take into account

- the radiological significance of the activity inventory to be confined,
- the potential release mechanisms,
- the achievable effectiveness and reliability of the measures and installations for confinement, and
- the frequency of hazardous impacts on the barriers and retention functions.

(3) The required effectiveness and reliability of the barriers and retention functions is to be ensured by appropriate quality in design and manufacturing as well as monitoring and maintenance during operation.

4.3 Defence-in-depth concept

(1) For events that may affect the effectiveness of barriers and retention functions or the compliance with the main safety functions directly or indirectly, measures and installations are to be provided to prevent and control such events to the extent necessary. In this respect, the principle of "the more ... the lower" is to be applied, i.e. the more often an event is to be expected, the lower should the resulting potential radiological impact be or, the more severe the consequences of an event may be, the lower should be its frequency of occurrence. Here,

- plant operation with as little occurrences as possible is to be ensured by principles of design, manufacture and operation that enhance reliability, and deviations from normal operation are to be detected at an early state and largely limited so that operational occurrences are prevented,
- operational occurrences that occur nonetheless are to be controlled, if possible, thus preventing the occurrence of design basis accidents,
- the reliable control of design basis accidents postulated nonetheless is to be ensured, thus preventing the progression of a design basis accident to a beyond design basis plant state, and
- for the case of a beyond design basis plant state (severe accident) occurring nonetheless, the consequences are to be mitigated and event sequences with early or large releases of radioactive material to be excluded.

(2) A general safety objective of the concept of successive levels of defence is to enable the control of event sequences that might be uncontrollable at a certain level of defence at the next level of defence.

(3) The events and plant states that may lead to safety-relevant deviations from normal operation are to be classified according to event classes and levels of defence together with the respective initial and boundary conditions and postulates to be considered and acceptance targets to be complied with. A distinction is to be drawn between the following event classes and associated levels of defence. The frequencies specified here are to be understood as guidance values:

- Specified normal operation (level of defence 1)
- Anticipated operational occurrences (level of defence 2) > approx. 10^{-2}/a
- Design basis accidents (level of defence 3) < approx. 10^{-2}/a to > approx. 10^{-5}/a
- Beyond design basis accidents (level of defence 4) < approx. 10^{-5}/a

For internal and external hazards not assigned to a level of defence in the "Safety Requirements for Nuclear Power Plants", requirements apply in terms of a plant- and site-specific assignment of the hazard-related parameters to the levels of defence, using the guidance values.

For weather-related external hazards, assignment of the requirements to level of defence 3 is sufficient up to a frequency of 10^{-4}/a since for lower frequencies and thus a tendency to greater impacts, these can either be identified at an early stage and thus measures at level of defence 4 can be initiated at an early stage or the potential for damage is limited.

(4) Further, it is to be shown that for the total of the beyond design basis plant states, the expected value for the core damage frequency (events in the fuel storage pool are also to be included in the consideration) does not exceed 10^{-5}/a per plant in all phases of power, low power and shutdown operation.

(5) "Guidance value" in (3) means that events, including the combination of events with each other and the combination of events with plant operating states, should not only be assigned to the levels of defence based on the frequency ranges mentioned.

In any case, the uncertainties in the determination of the frequencies and in the event sequence analyses as well as the respective level of validity are also to be considered for the classification (uncertainties are due, among other things, to the complexity of the correlations relevant for the event sequence, completeness of knowledge on relevant phenomena, reliability of the database.).

Furthermore, it should be taken into account that it may be useful for dimensioning of safety or system functions to postulate scenarios in the form of enveloping events (such as the postulated 2A leak of a PWR reactor coolant line for the injection capacity of the emergency core cooling and residual heat removal system) that are assigned to levels of defence regardless of their frequency of occurrence.

(6) By classifying an event according to a specific level of defence, it is defined for the safety demonstration in the "Safety Requirements for Nuclear Power Plants" which postulates are to be considered in the event analysis and which acceptance criteria are to be complied with.

For combinations of initiating events with postulated failures that go beyond those stated in the "Safety Requirements for Nuclear Power Plants" (e.g. postulated failures beyond the single failure concept) or with short-term operating states, the assignment of this event sequence to a level of defence can be changed compared to the initiating event, taking into account (3) and (5),.

Other initial and boundary conditions can be considered in the context of uncertainty analyses according to the "Safety Requirements for Nuclear Power Plants", except where parameter values are explicitly "set" also for uncertainty analyses to ensure safety margins in the event analyses. Unlikely parameter values or combinations of parameter values are considered in the uncertainty analyses and do not change the classification of the event according to the levels of defence.

4.4 Main safety functions and safety functions

(1) Compliance with the main safety functions (control of reactivity, fuel cooling, confinement of radioactive material) is to be ensured by safety functions, where appropriate, in combination with precautionary measures[1]. The safety functions should be ensured by

[1] Here, the confinement of radioactive material includes those functions that may be needed to seal penetrations through the barriers or produce staggered pressures to minimise activity releases.

- measures and installations that avoid, prevent or exclude states and conditions that may jeopardise main safety functions, and
- measures and installations that – in case of non-excludable violation of the acceptance criteria for the main safety functions at a specific level of defence – control or mitigate the consequences at the next level of defence.

(2) The safety functions are to be ensured by sufficiently effective and reliable measures and installations (staggered to the extent required for effectiveness and reliability).

(3) The required reliability of the safety functions should be dependent on the requirements of the different levels of defence as well as on the potential consequences and controllability in case of postulated ineffectiveness of the measures and installations. In this respect, measures and installations for avoidance, prevention and exclusion are to be realised as far as technically reasonable even if measures and installations for control are provided at one of the next levels.

(4) The required performance and reliability of the safety functions for the control of events should be such that the acceptance targets assigned to the levels of defence are complied with for a range of events and plant states covering the effects and frequencies of the event classes, thereby avoiding or preventing escalation to the next level of defence.

(5) Safety functions to control an event with potentially safety-relevant impacts will not be required if the precautions (precautionary measures) against the occurrence of the event are so reliable in the individual case that these can be regarded as excluded.

(6) For a complete interaction of "exclusion", "prevention" or "avoidance" of events on the one hand and "control" on the other hand, it is also necessary that the measures and installations credited within the realised safety concept, including their prerequisites and their requirements for maintaining effectiveness during the operating period, are monitored and impermissible deviations will be remediated.

(7) The safety functions at levels of defence 1 and 2 are principally to be fulfilled by operational measures and installations, specifying any further requirements where necessary according to the relevance for the control of abnormal operation ("anticipated operational occurrences") and thus the avoidance of a design basis accident (e.g. additional margins, redundancy in active components, automation, emergency power supply).

The control of events assigned to level of defence 3 ("control of design basis accidents") is to be ensured effectively and reliably by measures and safety installations, taking into account specific design principles (e.g. protection against redundancy-wide failures due to internal or external events, redundancy, diversity as required, automation, fail safe).

For installations and measures credited for tasks at level of defence 4, it is to be demonstrated that they are effective under the boundary conditions of the respective beyond design basis plant states and can be performed with sufficient reliability.

(8) Where installations have to fulfil tasks for more than one level of defence, the enveloping requirements as regards effectiveness and reliability are to be considered for the design of these installations. Furthermore, it is to be ensured that with the staggered set of installations (system functions) provided the reliability of the safety function concerned is so high that not only the reliability requirements of levels of defence 1 to 3 are fulfilled but also the conditions for exclusion of large or significant releases.