Appendix 1 to the minutes of the 450th meeting of the Reactor Safety Commission (RSK) on 26./27.09.2012

Note:
This is a translation of the document entitled: "Empfehlungen der RSK zur Robustheit der deutschen Kernkraftwerke". In case of discrepancies between the English translation and the German original, the original shall prevail.

RECOMMENDATION
Recommendations of the RSK on the robustness of the German nuclear power plants

Introduction

One focus of the review of the RSK in its safety review (RSK SÜ) of May 2011 [1] with regard to the robustness of all installations and measures was on the identification of an abruptly occurring aggravation in the event sequence (cliff edges) and, where necessary, on the derivation of measures for its avoidance.

The RSK particularly examined the question of whether for beyond design basis hazards and postulates such failures in safety installations may occur that protection goals (*translator's note: in the IAEA standards referred to as fundamental safety functions*) are violated and may result in sequences with abruptly increasing, significant impacts in the environment.

The considerations related to potential failures in safety installations due to

A. beyond design basis impacts on safety installations in case of

   a. natural hazards (Chapter 6.2 of the RSK safety review (RSK-SÜ))
   b. postulated failure of precautionary measures against internal hazards (Chapter 6.4)
   c. man-made hazards (Chapter 6.6)

B. beyond design basis assumptions on failures in safety installations, postulated to affect more than one redundant system not due to the hazards above, but due to unspecified causes – "CCF[1] postulate" (Chapter 6.3).

Regarding the beyond design basis impacts and on the basis of available information, it was primarily observed that robustness of the safety installations to varying degrees is plausible, but for a proven confirmation particularly of higher robustness levels/degrees, additional information is required. For the further development of the accident management concept regarding robustness, it is be considered for which beyond design basis extent of the impacts sufficient effectiveness of safety installations is no longer to be expected, but the vital safety functions required for compliance with the protection goals can be ensured by modified or additional accident management measures. Owing to the dependency on other related

[1] CCF = **C**ommon **C**ause **F**ailure

considerations or investigations, recommendations on specific measures have not been formulated yet in the RSK-SÜ of May 2011.

Regarding the beyond design basis assumptions on CCF postulates, no analysis of the secondary damage caused by impacts was needed, so that recommendations on specific measures could be formulated (Chapter 6.5).

Furthermore, it should be checked whether accident management measures can be performed under unfavourable boundary conditions.

From the point of view of the RSK, the further development of the accident management concept should therefore take into account aspects both with regard to beyond design basis impacts and beyond design basis assumptions on system failures and co-ordinate the requirements derived from it.

In the following, the aspects are explained and specified in more detail.

As mentioned above, two approaches were pursued in the RSK-SÜ for the assignment of robustness levels and degrees of protection regarding postulated beyond design basis scenarios:

A. For beyond design basis external and internal hazards, the vital safety functions are to be fulfilled primarily by existing safety installations or emergency systems where credit can also be taken of the design margins of these installations and systems.

Moreover, it is possible - if functionality of necessary installations can no longer be assumed when exceeding a certain impact load - to compensate for the corresponding losses by appropriate accident management measures (AMM) to ensure the vital safety functions.

B. Regardless of the question of hazard-induced failures (Approach A), beyond design basis failures postulated in safety installations or emergency systems affecting more than one redundancy are also to be considered, e.g. station blackout (SBO) > 2h[2].

As a follow-up to its statement of May 2011, the RSK continued the consultations on the assessment of robustness. Based on these consultations, the RSK updates and supplements their recommendations on the robustness of the German nuclear power plants.

For Approach A, the RSK recommends performing a systematic analysis. The procedure to be pursued is described in Part 1 of this statement.

The procedures and measures for Approach B recommended by the RSK in addition to the analyses according to Approach A are presented in Part 2. In this respect, the first recommendations on the further

2 This is to cover, in particular, CCF mechanisms that cannot be represented adequately in the impact analysis and cannot be classified as practically excluded through precautions either. For more complex systems, this typically applies to system-internal CCF mechanisms.

development of the accident management concept in [1], Chapter 6.5 "Generic key aspects" are dealt with in particular and specified.

The RSK has completed its consultations on the robustness of the German nuclear power plants except for the topics “crashes of commercial aircrafts” and “extreme weather conditions”. The forthcoming consultations may result in further recommendations.

With regard to the external hazard “blast wave”, for which according to [1] Degree of Protection 1 can be confirmed for all plants but, upon presentation of appropriate documents, also degrees of protection up to 3 may be possible, the RSK does not see the need for further analyses and additional accident management measures beyond the review of the statements on the safety margins recommended in the statement [1].

The results of further investigations according to Part 1 and the measures already defined in Part 2 are to be taken into account in the further development of the accident management measures.

Part 1: Robustness analysis to check the effectiveness of the vital safety functions for beyond design basis external or internal hazards

1. To ensure the vital safety functions in case of beyond design basis external or internal hazards, a systematic analysis should be conducted to identify potential for increasing robustness appropriately, for which supplementary measures should be designed where required (see Annex 1).

   In this respect, it is appropriate to also analyse and assess the consequences of unlikely, but not yet practically excluded impacts on safety installations or emergency systems - possibly taking into account site-and system-specific features. However, the RSK holds the view that scenarios with superposition

   - of an impact > design basis impact
   - with an independent (i. e. not induced), failure of safety installations or emergency systems affecting more than one redundancy

   are not to be postulated, since these combinations can be classified as “practically eliminated”[3].

2. Thus, the design margins in the existing safety installations or emergency systems are to be assessed with regard to whether and when the required safety function of safety installations or emergency systems may be endangered in case of increased (beyond design basis) assumptions on external and internal hazards. These analyses can be performed by means of engineered judgements.

   In this respect, it is also to be assessed to which extent existing precautionary measures to prevent beyond design conditions also remain effective under the increased impacts. The assessments have to

[3] IAEA SSR 2/1 Specific Safety Requirements “Safety of Nuclear Power Plants: Design”, January 2012, 2.11: “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 degree of confidence to be extremely unlikely to arise.”

consider all components that are necessary to ensure the vital safety functions. If, for example, failures in safety-relevant electrical equipment are considered in the context of beyond design basis external or internal hazards, the resistance of the whole chain from the diesel generator set via switchgears, cabling, etc. to the respective beyond design basis impact has to be considered to assess whether these will still be available under the specified conditions with a sufficient degree of probability.

3. On the basis of 2., it is then to be assessed whether increase of robustness is possible

   - either by appropriate measures to upgrade existing safety installations or emergency systems,

   - or by existing or additional accident management measures to ensure vital safety functions in case of expected failure of safety installations or emergency systems. These accident management measures must not lose their operability by those impacts that in the analyses have led to a functional failure of safety installations or emergency systems.

4. With the accident management measures to ensure the vital process-based safety functions designed in this way it is then possible to derive the tasks for auxiliary functions and thus for appropriate accident management measures to compensate for possibly occurring failures in the safety-related auxiliary functions (in particular electrical energy supply and service water supply).

   The RSK considers it appropriate that at least Robustness Level 1 or at least Degree of Protection 2 (man-made hazards) is targeted as a result.

In the following, there are further explanations for the performance of an analysis with a view to a pragmatic approach:

External hazards

Earthquake

As shown in [1], the RSK holds the view that the German nuclear power plants have significant design margins for beyond design basis earthquakes. To verify this assessment, the following is recommended:

a) For plants for which results of probabilistic seismic safety analyses are available, the robustness to beyond design basis earthquake impacts is to be assessed. The assessment should be based on the HCLPF (High Confidence for Low Probability of Failure[4]) values of the buildings and installations required to ensure the vital safety functions.
b) For plants for which no results of probabilistic seismic safety analyses are available, there is the option to assess robustness to beyond design basis earthquake impacts by means of applicability

[4] IAEA, "Seismic Evaluation of Existing Nuclear Power Plants"; Safety Reports Series, No 28, April 2003
IAEA, "Evaluation of Seismic Safety for Existing Nuclear Installations; Safety", Guide No. NS-G-2.13; 2009

considerations (possibly supported by a plant walkdown by an expert commission) based on results according to a)).

To improve robustness, superposition of operating conditions during low-power and shutdown operation of short duration with an earthquake should be considered, which goes beyond the requirements specified in the existing rules and regulations. This case has not been dealt with within the RSK-SÜ either. For the analysis of robustness, it is to be demonstrated that the design basis earthquake does not lead to significant impacts in the environment during temporary operating conditions of short duration.

Here, particular attention is to be paid to situations where vital safety functions may be impaired in case

- that changes in mass distributions (e.g. filled reactor well during reloading) in the reactor building lead to higher seismic loads on safety-relevant installations and building structures than during power operation,

- that certain installations are only operated (e.g. reactor cavity seal liner in a BWR) or in a specific mode of operation (e.g. refuelling machine outside the parking position) during low-power and shutdown operation for which there are no specific or higher-level proofs regarding seismic loads,

- that parts (e.g. fuel element transport casks, heavy components) and operating media (lubricating oils and solvents) that are introduced into the plant or handled during low-power or shutdown operation cause damage to safety-relevant installations and building structures due to an earthquake,

- that in the event of an earthquake, safety-relevant measures and installations are only available to a limited extent during low-power and shutdown operation (e. g. isolation of residual heat removal trains, short-term manual actions), which are required to manage the consequences of an earthquake.

For plants that are permanently in low-power and shutdown operation, the proof of robustness is to be provided for longer lasting states also for beyond design basis earthquakes according to a) and b) (see above)).

Flooding

If a water level that may endanger vital safety functions cannot be excluded due to site-specific conditions, the criteria specified in the safety review [1] for at least Level 1 shall be referred to. Alternatively, it may be demonstrated on the basis of site-specific conditions that a postulated discharge quantity, which is determined by extrapolation of existing probabilistic curves to an occurrence frequency of 10^{-5}/a, will not result in the loss of vital safety function. For sites located near tidal waters, an analogous approach is to be applied. The methodology used for it is to be explained in a comprehensible manner.

In this respect, the uplift resistance of canals and buildings is to be considered.

Internal hazards

Flooding of the annulus

Within the RSK-SÜ [1], the RSK has seen a potential for "cliff edge" effects caused by beyond design basis annulus flooding.

The following issues should be explained or clarified:

- Identification of a safety-relevant installation failing in case of a flooding level of 2 m at the lower annulus level. Here, it is to be examined, in particular, which impacts the flooding of transducers and other electrical and I&C equipment located in the annulus may have on residual heat removal and the boration of the primary coolant. It is to be shown whether measures may be hindered, prevented or triggered incorrectly.

- Taking into consideration this issue, it is to be specified what measures will be reliably available in the different operating phases under the boundary conditions of a design basis flooding of the annulus up to a flooding level of 2 m for the prevention of an impermissibly long loss of vital safety functions. In particular, it is to be shown by which measures

    - secondary-side heat removal and, moreover, shutdown into a cold unpressurised, subcritical state are ensured in the short term in case of beyond design basis flooding during power operation, and which installations have to be taken into account for it and are available,

    - cooling of the fuel pool can be ensured within the required time in case of beyond design basis flooding both during power operation and low-power and shutdown operation,

    - replacement of the evaporated inventory can be achieved in the short and medium term in case of beyond design basis flooding during low-power and shutdown operation with a lowered level in the reactor coolant lines (also demonstrating, e. g. that the accumulator injection system is reliably available and can be activated).

Furthermore, it is to be shown how in operating phases with flooded reactor pool scenarios with water losses into the annulus from the connected system (RPB - reactor well - fuel pool) are prevented under all operating conditions of the spent fuel pool cooling and purification system (including leakage caused by human errors or false triggering of reactor protection signals) and, in case of failure of the precautionary measures provided, be managed.

Load drop

In addition to the RSK-SÜ [1], the RSK sees a potential for "cliff edge" conditions regarding the failure of precautionary measures against load drop. Therefore, the following is recommended:

- The impacts of the drop of a fuel element transport cask into the fuel pool should be analysed regarding the loss of pool water. The possibility of overfeeding a loss of fuel pool water should be checked and specific accident management measures should be introduced, if required.

- Likewise, the impacts of the drop of loads into the RPV or onto the connection between RPV and fuel pool established during low-power and shutdown operation should be analysed. If necessary, specific accident management measures should be introduced in dependence of the consequential impacts.

- Regarding the handling of loads in the environment of necessary safety-related installations, it should be analysed whether a postulated drop load leads to inadmissible retroactive effects on the reactor coolant pressure boundary or damage affecting more than one redundancy that may lead to "cliff-edge" conditions in the plant.

Part 2: Measures with regard to postulated failures

As a result of the RSK-SÜ, in May 2011, the RSK formulated first recommendations in Chapter 6.5 of [1] to increase the robustness of the German nuclear power plants regarding postulated failures. As a follow-up, the RSK continued their consultations on the assessment of robustness. On the basis of these consultations, the RSK specifies and supplements its recommendations in Chapter 6.5 in [1] of May 2011 as follows:

1. The safety objectives of the accident management measures mentioned in Part 2 should also be achieved during or after natural external design basis hazards. In particular, the following aspects should be considered during/after these hazards:

   - Limitations of the accessibility of the power plant area and power plant buildings that may have to be postulated,

   - operability of the accident management measures, and

   - availability of the remote shutdown and control station.

2. The availability of three-phase alternating current is a necessary prerequisite for the majority of the measures by which vital functions can be ensured or re-established.

   a. It is to be demonstrated that the supply of three-phase alternating current required for the vital safety functions is ensured even if there is no grid connection available for up to a week.

      The long-lasting loss of offsite power with unavailability of the grid connections for up to a week is assumed due to the external hazard with corresponding damage to the infrastructure outside the plant. As far as the plant-internal emergency power generators are taken into account for three-phase alternating current supply after loss of offsite power, the fuel stocks for these generators are to be stored so that they remain available also when taking into account such impacts. When taking credit of external resources (fuel, lubricating oils, mobile power generators), it is to be demonstrated that they also remain available when considering such impacts and can be brought to the place of use.

   b. In the case of a postulated station blackout, the vital safety functions have to be maintained or re-established in time before reaching “cliff-edge” effects. This involves the following:

      - The direct current supply required for the vital safety functions is also to be ensured if three-phase alternating current supply is not available for up to 10 hours. An independent battery charger for recharging of relevant batteries, which is protected against external hazards and kept available, can be credited if it is ensured that there is sufficient grace time for connection and use of such a battery charger.

- Furthermore, it is to be demonstrated that three-phase alternating current supply can be re-established within a plant-specifically determined grace time by means of back-up units. From the point of view of the RSK, this includes:

  · layout of standardised hook-up points protected against external hazards outside of the buildings for supplying the systems required to maintain the vital safety functions. The aim of an adequate layout of the hook-up points is to ensure supplying the emergency power bus bars and, if necessary, emergency power bus bars required for it without impairing the degree of protection of the respective buildings (e. g. ventilation isolation and flood protection) against the respective external hazard. The hook-up points are to be installed so that they have no retroactive effects,

  · at least one mobile emergency power generator protected against external hazards with sufficient capacity for supplying one redundant residual heat removal train.

3. Review of the accident management concept with regard to injection possibilities for the cooling of fuel assemblies and for ensuring subcriticality. Here, the following aspects have to be taken into account:

   - Availability of mobile pumps and other injection equipment (hoses, fittings, couplings, etc.) protected against external hazards as well as of boron under consideration of the specified grace time for preparation and delivery.

   - Water intake points whose availability is also ensured after an external impact.

   - Possibilities of injecting water into the steam generator, the reactor coolant system and, if required, the containment (in the latter case also taking into consideration the higher back pressures) without the need to enter areas with high risk potential (dose rate, debris load) and to be able to compensate local destruction (e.g. by installed and physically separated injection paths)

Regarding the postulated failure of the primary ultimate heat sink, details can be found in [2].

4. The filtered containment venting system is to be designed so that pressure relief can also be repeatedly performed during or after natural external design basis hazards and in the event of a station blackout Furthermore, the effectiveness of installations to reduce hydrogen in the containment is to be ensured accordingly.

5. Increased consideration of wet storage of fuel assemblies in the accident management concept, taking the following aspects into account:

- Possibilities of injecting water into the wet storage facility for fuel assemblies without the need to enter areas with high risk potential (dose rate, debris load) and to be able to compensate local destruction (e. g. by installed and physically separated injection paths).

- To ensure evaporation cooling: updating of the safety demonstrations for the fuel pool, reactor cavity, setdown pool, reactor cavity seal liner at boiling temperature.

Furthermore, the RSK considers it necessary that the Severe Accident Management Guidelines (SAMG) will be implemented in the short term.

References

[1] RSK-Stellungnahme
Anlagenspezifische Sicherheitsüberprüfung (RSK-SÜ) deutscher Kernkraftwerke unter Berücksichtigung der Ereignisse in Fukushima-I (Japan)
Anlage zum Ergebnisprotokoll der 437. Sitzung der RSK am 11. - 14.05.2011
RSK statement
Plant-specific safety review (RSK-SÜ) of German nuclear power plants in the light of the events in Fukushima-I (Japan)
Appendix to the minutes of the 437th meeting of the RSK on 11. - 14.05.2011

[2] RSK-Stellungnahme
Ausfall der primären Wärmesenke
Anlage 1 zum Ergebnisprotokoll der 446. Sitzung der Reaktor-Sicherheitskommission (RSK) am 05.04.2012
RSK statement
Loss of the primary ultimate heat sink
Appendix 1 to the minutes of the 446th meeting of the Reactor Safety Commission (RSK) on 05.04.2012

Annex 1: Robustness analysis on ensuring vital safety functions in case of beyond design basis hazards (Case A)

Scheme for the analysis with beyond design basis assumptions

What vital safety functions are needed to prevent fuel element damage with significant impact on the environment? (in dependence on the initial condition of the plant)
Which safety installations and emergency systems are still available after increased (beyond design basis) assumptions on external or internal hazards to provide these vital safety functions, or what failures would have to be expected?*
How far can such failures either be prevented by retrofitting or compensated by appropriate accident management measures to maintain the vital safety functions?
Which auxiliary functions will be required when and with what capacity to support installations for the vital safety function in time?
Which of the installations provided for the auxiliary functions per design are still available and sufficient after the respective impacts?*
What requirements do accident management measures have to fulfil to compensate for failures in the auxiliary functions when required?
How can appropriate accident management measures for vital safety functions and auxiliary functions be realised?
*No considerations for scenarios that are practically to be excluded