Note:
This is a translation of the RSK statement entitled
"Randbedingungen der Nachweisführung zur Störfallbeherrschung"
In case of discrepancies between the English translation and the German original, the original shall prevail.

RSK statement

(492nd meeting of the Reactor Safety Commission (RSK) on 22.03.2017)

Boundary conditions for furnishing proof of the control of design basis accidents

Contents

1 Advisory request of the BMUB and consultations ... 3

2 Technical situation ... 3

2.1 Concept for the treatment of design basis accidents and furnishing proof during the construction of the plants ... 3

2.1.1 Essential principles (using the example of PWR) ... 3

2.1.2 Controlling a steam generator tube rupture and furnishing corresponding proof ... 4

2.2 Assessment criteria ... 7

3 Answers to the questions of the BMUB ... 7

3.1 On Question 1: Up until which plant condition should proof be furnished? ... 7

3.1.1 Answer to the question ... 7

3.1.2 Explanation using the example "Steam generator tube rupture". ... 8

3.1.3 Aspects concerning other design basis accidents on level of defence 3 ... 9

3.2 On Question 2: Consideration of non-safety systems ... 9

3.2.1 On Question 2a: Crediting of non-safety systems ... 9

3.2.2 On Question 2b: Favourable/adverse influences of non-safety systems ... 13

3.3 On Question 3: Consideration of human errors or failures to carry out actions provided for in the operating manual in the proof furnished ... 16

3.4 On Question 4: To what extent should the boundary conditions and scenarios considered within the framework of the verification process be included in the chapters of the operating manual dealing with design basis accidents? ... 19

4 References ... 20

5 Compilation of relevant requirements and definitions from RSK recommendations and the non-mandatory guidance instruments ... 21

5.1 On Question 1 (Up until which plant state should proof be furnished?) ... 21

5.1.1 Definition of the controlled plant state ... 21

5.1.2 Definition of the safe plant state ... 21

5.1.2.1 Requirements for furnishing proof regarding the achievement of the controlled plant state 22

5.1.2.2 Requirements for furnishing proof regarding the achievement of the safe plant state 23
5.1.3 Requirements for methods of furnishing proof 24
5.2 On Question 2 (Consideration of non-safety systems) 24
5.3 On Question 3 (Consideration of manual measures) 26
5.3.1 Furnishing deterministic proof 26
5.3.2 Probabilistic safety analyses 27
5.4 On Question 4 (Requirements for the operating manual) 28

1 Advisory request of the BMUB and consultations

At its 106th meeting on 16.04.2015, the RSK Committee on PLANT AND SYSTEMS ENGINEERING (AST) had been informed about the BMUB's advisory request regarding safety requirements for nuclear power plants to control the "Steam generator tube leak" design basis accident. In the advisory request [1], the BMUB asks the RSK for a written statement on the requirements for the analysis of an event on level of defence 3 (accident analysis) and the postulated initial and boundary conditions, in particular:

1 Up to which plant state should proof be furnished?

2 To what extent can non-safety systems (including actions required by the limitation system, as is the case, for example, with SGTR[1]) be taken into account in the various phases after the design basis accident has occurred (if necessary with the definition of associated conditions) as part of the process of furnishing proof?

In this context, how are non-safety systems to be treated that are in operation at the time of the occurrence of the event, are not switched off as per design, and influence the course of the event favourably or unfavourably?

3 In what way are possible human errors or the omission of actions provided for in the operating manual to be taken into account in furnishing proof?

4 To what extent should the boundary conditions and scenarios specified within the framework of the process of furnishing proof be included in the chapters of the operating manual dealing with design basis accidents?

In preparation for further discussion, the ad hoc working group on the topic of steam generator tube leak (Ad-hoc-AG DEHL II) was instructed at the 107th meeting of the Committee on 28 May 2015 to prepare a draft statement. The working group fulfilled this mandate in five meetings, and the AST Committee adopted the statement at its 119th meeting on 13 October 2016. The RSK discussed and adopted the statement at its 492nd meeting on 22 March 2017.

2 Technical situation

2.1 Concept for the treatment of design basis accidents and furnishing proof during the construction of the plants

2.1.1 Essential principles (using the example of PWR)

As concerns the design of the plants that are still licensed for power operation today, the concept for controlling design basis accidents was underpinned by the following principles, among others [3]:

[1] steam generator tube rupture

1 Proof of compliance with the acceptance criteria for design basis accidents:

- For the phase of stabilising the plant condition:
  - crediting only of safety systems (taking into account the postulates for the unavailability of systems); for special accident variants that may result from failure postulates, also crediting of functions of the limitation system,
  - automatic triggering of at least those functions that are required within < ½ h for the control of design basis accidents,
  - special alarm for manual measures with short grace periods beyond ½ h ("safety hazard alarm", e.g. in the case of PWRs if small leaks in the primary system and steam generator tube rupture occur).

- For the phases of stabilisation of the plant up to the state "cold, depressurised".:
  - crediting of safety systems, with long grace periods (i.e. sufficient time for recognition, analysis, implementation) and event-specific expected availability and effectiveness also crediting of non-safety systems,
  - as a rule, manual triggering of the functions.

2 Upstream verifications to minimise the release of activity in the event of special design basis accidents (in the case of PWRs in particular in the case of SGTR) or for optimised plant cooldown:

- crediting of all functions - upstream of the safety systems - whose availability is to be expected event-specifically (typically staggered deployment),
- typically automatic triggering of these functions for the period < ½ h.

The concrete application of these principles is explained in the following section, using the example of a more complex design basis accident, the steam generator tube rupture (SGTR) in a PWR.

2.1.2 Controlling a steam generator tube rupture and furnishing corresponding proof

In contrast to the other events on level of defence 3, the separation between the primary and the secondary side locally no longer exists in the case of an SGTR accident: There is a transfer of activity-containing coolant from the primary system (PS) to the secondary side of the defective steam generator (SG) and thus, in addition to the actual control of the event, there is the need for processes to minimise the release of activity to the environment.

This special feature was taken into account during the development of the concept for controlling SG tube ruptures by formulating event-specific design objectives [3], in particular by optimising the control of design basis accidents in such a way that upon the detection of a SG tube rupture, the reactor protection system will already trigger operational systems via the limitation system in order to head off the transient as far as possible before the reactor protection system will trigger safety systems whose operation is unfavourable for minimising the release of activity. This is achieved by a

- minimisation of the probability of occurrence for the excitation of the emergency cooling criteria (and thus an increase in the leak rate in the defective SG);

- relief of the shift personnel from the necessity of having to manually switch off any activated HP safety injection pumps under time pressure;

- minimisation of the response frequency of the main-steam relief valves of the defective SG;

- avoidance of a loss of offsite power (and thus the unavailability of turbine condenser and reactor coolant pumps) by load reduction before reactor scram.

In order to achieve radiologically optimised handling of a design basis accident by the shift personnel, the operating manuals distinguish between various cases in which a suitable frame is set up with regard to the possible boundary conditions for a SG tube rupture (cf. [4], Chapter 5.2):

- SG tube rupture without loss of offsite power, without excitation of the emergency cooling criteria,
- SG tube rupture without loss of offsite power, with excitation of the emergency cooling criteria,
- SG tube rupture with loss of offsite power, without excitation of the emergency cooling criteria, and
- SG tube rupture with loss of offsite power, with excitation of the emergency cooling criteria.

In the latter case, the handling of a design basis accident is divided into three phases with the following objectives:

- Phase 1: Stabilisation of the plant behaviour, termination of the activity release into the environment by isolation of the defective SG.

- Phase 2: Keeping the plant in the "subcritical, hot" state until grid supply is restored.

- Phase 3: Taking the plant to the "cold, depressurised" state.

Regarding Phase 1:

In Phase 1, equipment of the safety system is employed to ensure that the main safety functions are fulfilled:

- reactor scram (RESA),

- termination of the activity release into the environment by adjusting primary pressure to secondary pressure with isolation of the defective SG, and

- residual-heat removal via the intact SGs.

The extent of the activity release via the defective SG depends not only on the existing after-power but also on how quickly the pressure equalisation between primary and secondary side is reached and to what extent the steam release from the defective SG and a level rise there can be limited. With a view to a minimisation of the release of activity, measures have therefore been implemented (e.g. faster pressure reduction in the primary

system by using the operational spray functions) with the aid of which pressure equalisation and the termination of steam release from the defective SG can be achieved more quickly than with the exclusive use of safety equipment. In other words, operational equipment is used either upstream of or in addition to safety equipment. In this context, the operational equipment must not impair the function of the safety equipment.

At the end of Phase 1, a stationary plant state has established itself in which the acceptance criteria with regard to the main safety functions of reactivity control, fuel cooling and confinement of radioactive materials are fulfilled.

Regarding Phase 2:

If only the demineralised-water supplies in the emergency feeding pools are taken into account (i.e. via the safety system), the plant can remain in a "subcritical, hot" state for at least 10 hours. However, due to the emergency power supply of the start-up and shut-down pump(s), it is initially assumed in the concept of dealing with design basis accidents that the assured demineralised-water supplies in the feedwater tank and in the demineralised-water tanks are also available for steam generator feeding. Based on this assumption, the minimum demineralised-water supply of 800 Mg within the first 24 hours after the start of the accident will not be undercut.

Accordingly, restoration of the grid supply is expected before the plant has to be shut down to the "subcritical, depressurized, cold" state (phase 3) before the minimum supply of demineralised water is reached.

Regarding Phase 3:

The transition to the "subcritical, cold" state is initiated as soon as the restoration of the grid supply allows the reactor coolant pumps in the intact loops to be switched on. If grid supply does not return, Phase 3 is initiated once the minimum supply of demineralised water is undercut, i.e. after 10 hours at the earliest. The transition to primary-side residual-heat removal with the residual-heat removal system is carried out by way of:

- temperature reduction in the primary system by cooldown of the intact SGs,
- pressure reduction in the primary system by pressuriser spraying (upstream by the chemical and volume control system, otherwise by the extra borating system),
- make-up of the volume contraction by means of borated coolant (upstream by the chemical and volume control system, otherwise by the extra borating system),
- primary system cooling taken over by the residual-heat removal system.

When the reactor coolant pumps are available again in the intact loops, there is no risk during the cooldown that low-borated water plugs will form in the defective steam generator and reach into the reactor core.

When cooling the plant down under natural circulation conditions, the transfer of demineralised water into the primary system is prevented by lowering the pressure in the defective SG to below primary system pressure.

The pressure reduction in the defective SG can be achieved by a discharge of main-steam via the main-steam relief control valve, the main-steam safety valve or the warm-up line.[2] However, the pressure in the defective SG should be only slightly below primary system pressure in order to limit any overflow of primary coolant into the defective SG and thus prevent flooding of the fine scrubbers so that the rate of activity release will not increase (minimisation aspect).

The corresponding procedures were designed by engineering considerations and validated in tests on the reactor coolant line test bed or by analyses with suitable computer codes.

2.2 Assessment criteria

The assessment criteria to be applied to answer the BMUB's questions ensues in particular from the RSK recommendation "Regulations on plant conditions after occurrence of an accident" ([2]), the "Safety Requirements for Nuclear Power Plants (SiAnf)" [5]) as well as KTA 1201 "Requirements for the Operating Manual" ([6]). The annex to this statement lists the essential requirements and definitions that were considered when answering the BMUB's questions.

3 Answers to the questions of the BMUB

3.1 On Question 1: Up until which plant condition should proof be furnished?

3.1.1 Answer to the question

The function of furnishing proof for events on level of defence 3 (accident analysis) is to demonstrate compliance with the safety-related acceptance targets and the associated acceptance criteria in accordance with SiAnf [5], Annex 2, Tables 3.1a to 3.1c with regard to reactivity control, fuel cooling and the confinement of radioactive materials.

In accordance with [5], Annex 2 § 2(3), the furnishing of proof shall extend from the occurrence of an event to the achievement of a controlled plant state; in the case of the determination of a source term for radiological verification purposes, it shall extend until the end of the release (see also RSK Recommendation [2], Chapter 3.2.1).

The controlled plant state is characterised by the fact that the acceptance targets and acceptance criteria are met and the relevant safety variables have reached sufficiently stationary values (see [5], Annex 1).

Sufficiently stationary are states in which the safety variables are so stationary or in which the safety margin to the acceptance criteria continuously increases to such an extent that a sufficiently long period of time is available for the analysis and assessment of the plant state, making it possible to carry out further measures (e.g. for the control of design basis accidents) in the event of an adverse change of safety variables (see [5], Annex 1).

[2] See also Section 3.2.1.

As a rule, the control of design basis accidents is carried out step by step, i.e. in such a way that different, controlled plant states are targeted one after the other. If, after reaching the first controlled state, violations of the main safety function of "reactivity control" may still occur due to the event (e.g. violation of the main safety function "reactivity control" due to xenon decay or increased moderation effect of the coolant at low primary system temperatures, violation of the main safety function of "fuel cooling" due to limited demineralised-water supplies for steam generator feeding), proof should be furnished until the "last" controlled plant state is reached.

Annex 5, §3.2.1 (6) of [5] demands that that the verification on levels of defence 2 to 4a must extend from the occurrence of an event at least to the achievement of the controlled plant state in which the plant can permanently remain. In the opinion of the RSK, this requirement is fulfilled by reaching the last controlled plant state.

The required event-specific proof is usually limited to reaching the first controlled state. The further proof up to the achievement of the last controlled state (e.g. residual-heat removal via the residual-heat removal and emergency core cooling system) can then - in compliance with the rules and regulations - also be furnished by means of design calculations for the dimensioning of the safety systems, experiments and engineering assessments on the basis of representative events, which flow into the design of the strategies provided in the operating manual for cooldown to residual-heat removal mode.

In contrast to the controlled plant state, the safe plant state is characterised by the fact that at least the safety-related conditions of a comparable low-power and shutdown operation phase as described in the operating manual are met. The achievement of the safe plant state, possibly by restoring redundancy, is not the subject of the furnishing of proof.

3.1.2 Explanation using the example "Steam generator tube rupture".

Section 0 shows that after isolation of the defective SG (end of "Phase 1"), a system status has been achieved in which the acceptance targets and criteria are fulfilled. Furthermore, the plant state is sufficiently stationary so that sufficient time is available for initiating and implementing further measures, depending on the situation. Consequently, this condition is a controlled plant state.

The initial function of the accident analysis is therefore to show that this controlled "subcritical, hot, defective SG isolated" plant state has been achieved.

The "last controlled plant state" in terms of RSK recommendation [2], Chapter 3.2.1., is reached when the residual heat can be permanently removed via the residual-heat removal system. If there is sufficient redundancy in the residual-heat removal system, this state is "subcritical, cold" and also a safe plant state.

The achievement of the "last controlled plant state" is usually shown with consideration of the corresponding procedures provided in the operating manual for manual shutdown. In contrast to other design basis accidents, it has to be taken into account that in the case of SG tube ruptures, plant states may still occur during manual shutdown from the first controlled state in which, without any special precautions, low-borated water may reach from the secondary side into the primary side. It must therefore be clearly demonstrated as part of

furnishing proof that the main safety function of "subcriticality" will also not be violated even during manual operation in residual-heat removal mode.

3.1.3 Aspects concerning other design basis accidents on level of defence 3

As a rule, event-specific proof of the control of design basis accidents is only required up to the first controlled plant state, typically up to the "subcritical, hot" condition. For the further cooldown to the last controlled "subcritical, cold" state (residual-heat removal mode), it is usually sufficient to demonstrate that the main safety functions have been achieved by means of the procedure for representative events.

A review of the PWR event list performed by the WG (Annex 2 in [5]) has shown that in particular the following events or event groups may require in-depth consideration as regards the achievement of the last controlled state [7]:

- SGTR (events D3-08, D3-09, D3-19) with the acceptance target of sufficient subcriticality upon cooldown in natural circulation (cf. Section 0).

- Events in which the first controlled plant state is characterised by a very high pressuriser level: The acceptance target is a sufficient dimensioning of the equipment for primary and secondary pressure reduction as well as for borating the primary circuit so that a transition to residual-heat removal mode is ensured. Examples are, in particular, secondary-side leak accidents with non-isolatable leaks (D3-05, D3-06, D3-21) and event D3-11 (inadvertent injection by operational or safety systems in the event of ineffectiveness of planned limitation measures).

- Small leaks inside the containment (events D3-22, D3-26, D3-28, D3-42) with the acceptance target of long-term core cooling in residual-heat removal mode.

3.2 On Question 2: Consideration of non-safety systems

3.2.1 On Question 2a: Crediting of non-safety systems

Question by the BMUB according to [1]:

To what extent can non-safety systems (including actions requested by the limitation system, as is the case for example with the SGTR) be credited in the various phases after the accident has occurred (if necessary with the definition of associated conditions) as part of the process of furnishing proof?

Note on the term „non-safety system“:
In the following, the term "non-safety systems" means active devices which, according to [5], Annex 1, are not covered by the term "active safety equipment". Besides operational systems, various limitation devices have so far also been counted among the active safety equipment.

According to [5], 2.1(6), measures and equipment shall be provided on level of defence 3 which ensure the required safety-related condition of the plant independent of the measures and equipment of other levels of defence. Accordingly, proof up to the controlled plant state (if relevant also up to the "last" controlled plant state) shall in principle be furnished with sole consideration of equipment of the safety system.

According to the RSK, non-safety systems can be credited in accordance with the regulations in the following cases:

- In the case of furnishing proof of the effectiveness and reliability of precautionary measures intended to prevent the occurrence of certain events (events with the acceptance target "VM" in Annex 2 of the Safety Requirements for Nuclear Power Plants [5]).

  An example is the event *"Inadvertent injection from a system carrying demineralised or low-borated coolant with failure of the limitation systems or upstream measures (external deboration; homogeneous and heterogeneous)"* (event D3-19) from [5], for which, in addition to the main safety functions R (reactivity control) and K (fuel cooling), "VM" is also specified as an option. From the point of view of the RSK, it has to be considered that the event definition "*with failure of the limitation systems or upstream measures*" does not apply to furnishing proof that the event is prevented by fulfilment of the VM criteria since available limitation systems, such as the injection concentration monitoring system (EIKO), the control element motion limitation system (STAFAB) as well as the secured demineralised-water feed lock (GEDES), can be used in interaction with existing grace periods for furnishing corresponding proof.

- According to [9] (Section 2.1.4), the calculation of the radiological accident consequences (i.e. the verification concerning main safety function S according to Annex 2 of [5]) *"(...) may be performed taking into account the operational systems and equipment contributing to damage minimisation, provided that such equipment is manufactured and operated in accordance with the applicable rules and regulations, has suitable quality characteristics with regard to its design and service experience, and is not impaired in its functional capability by any accident consequences".*

- Furthermore, it should be noted that although limiting process variables are not credited with regard to the initiation of protection actions, they are taken into account with regard to the initial and boundary conditions to be applied in the accident analyses (cf. [5], Annex 1).

However, according to the information provided by WG SGTL II (see Chapter 2.1.1), at the time of construction of the plants it was assumed that non-safety systems could also be taken into account in the procedure of furnishing proof of the short-term control of design basis accidents in individual special cases as well as of the medium- and long-term control of design basis accidents if sufficiently long grace periods are available if

(1) their operability is not called into question as a result of the accident,
(2) their use is possible without repercussions on the safety-related function and reliability of safety equipment,
(3) the grace periods for their use are sufficiently long, and
(4) certain quality requirements are met.

The scope of the non-safety systems that could be credited in the proof was limited by the above-mentioned requirements. Against this background, the ad-hoc WG SGTR II carried out an exemplary evaluation for the PWR events in Annex 2 of the "Safety Requirements for Nuclear Power Plants" [5] with regard to the following criteria[3] [7]:

(1) Characterisation of the first controlled state and identification of the measures and equipment necessary to achieve this state.
(2) Characterisation of the last controlled state, if relevant for the furnishing of proof (cf. Chapter 0), and identification of the measures and equipment necessary to achieve this state.
(3) Assignment of the identified equipment to the safety system or the non-safety system.

Based on the evaluation of the WG SGTR II, the RSK arrives at the following results:

- An earthquake with assumed consequential damage (break of main-steam lines outside the reactor building with rapid secondary system isolation) can result in a pressure transient in the primary system. In practice when furnishing proof, the opening and later closing of the atmospheric steam dump station is credited. The atmospheric steam dump station is controlled via the coolant pressure limitation system (*Kühlmittelmassen-, -druck und -temperaturgradientenbegrenzung,* MADTEB) from the secured area and is designed for operation after induced vibrations from earthquakes. For the same reason, the pressuriser relief isolation valve is also designed to function after earthquakes and is also controlled from the secured area via the MADTEB. If the pressuriser blow-off valve is postulated not to close, the relief isolation valve ensures the leak tightness of the primary system.

  Note: Without crediting the opening of the pressuriser relief valve, the pressure in the primary system may increase to the set pressure of the pressuriser safety valve. A postulated single failure on a pressuriser safety valve (does not close) would result in a transient with a loss of coolant in the containment. With the use of the MADTEB as justified above, this scenario need not be postulated.

- In the context of the discussions on the formation and effect of a demineralised-water plug in connection with the steam generator tube rupture (see [4]), the question arose to what extent the opening of the valves of the warm-up line (for SG pressure reduction in case of a postulated non-availability of the blow-off control valve on the defective SG due to the single failure or due to necessary simulations in the reactor protection system for opening the main-steam safety valve, see also Section 2.1.2) may be credited.

  Since the motor-driven valves used for this purpose and their actuators are part of the safety system with regard to secondary system isolation, they are of sufficient quality with regard to the opening function and can therefore be credited in the event analysis. Creditability, however, presupposes that adequate availability requirements are defined in the operating rules.

- Furthermore, the RSK points out that in the proof of the control of design basis accidents, auxiliary systems are implicitly credited which serve to secure the operation of the safety systems in the longer term, e.g. heating and ventilation systems for maintaining the ambient conditions. These auxiliary systems are credited because their suitability for supporting the safety systems was established within

[3] Events with regard to the cooling of the fuel pool were not evaluated by the working group, cf. [8].

the framework of system assessments during construction. This also applies to so-called "self-sufficient" instrumentation and control systems.

- In addition, there have been no indications that the crediting of non-safety systems for the control of design basis accidents that should not be credited in accordance with the rules and regulations would be absolutely necessary.

  However, it is necessary to refer to the furnishing of proof in connection with design basis accidents concerning the cooling of the fuel pool, where the crediting of non-safety systems may become necessary (see separate RSK statement [8]).

In summary, against this background, the RSK comes to the following results with regard to Question 2a of the BMUB:

1 In accordance with [5], No. 2.1 (6) and [2], Chapter 3.2.1, proof of the control of design basis accidents shall in principle be furnished up to the controlled plant state (if relevant also up to the "last controlled plant state") with sole consideration of equipment of the safety system.

2 The following exceptions are permitted under the general rules and regulations:

- Non-safety systems may also be accredited in proof of the effectiveness and reliability of precautionary measures intended to prevent the occurrence of certain events (events with the acceptance target "VM" in Annex 2 of [5]).

- In accordance with [9], Section 2.1.4, the radiological consequences of design basis accidents may be calculated taking into account non-safety systems, provided these meet certain quality requirements.

- Limiting process variables are credited with regard to the initial and boundary conditions to be applied in the accident analyses (cf. [5], Annex 1).

3 If non-safety systems are credited in addition in the furnishing of proof, as in the cases mentioned above, this deviation should be justified.

  Here, it has to be demonstrated that the requirements of the defence-in-depth concept are met. This means that sequential measures must be in place to prevent anticipated operational occurrences, to prevent design basis accidents, and to control the latter. The non-safety systems considered on level of defence 3 must therefore not already have been credited with regard to the prevention of the event considered on levels of defence 1 and 2.

  In addition, it has to be demonstrated for the non-safety systems that are considered on level of defence 3 that the reliability and effectiveness of the credited non-safety systems are sufficient to replace a piece of safety equipment with respect to the requirements for the safety function required for the control of design basis accidents. In any case, the following has to be shown:

  3a The effectiveness of the measures with regard to the desired function has been demonstrated.

3b The equipment required to carry out the measure is not affected by the design basis accident for which it is to be used.

3c The required equipment is of a high quality (depending on the intended use, e.g. design against design basis earthquakes, emergency power supply, fault resistance or satisfactory performance in service under comparable pressure and temperature conditions which are similar to the requirements in the event of a design basis accident). The fulfilment of the required safety function is ensured even if the single-failure concept is applied to the entirety of all required equipment.

3d The I&C control system is sufficiently reliable, e.g.
- in the case of manually triggered actions:
  actuation from the control room, possibility of success control through feedback of the position of valves, suitable instrumentation for monitoring the relevant plant parameters, such as SG level, sufficient time for control and, if necessary, correction.

- in the case of automatic actions:
  I&C system designed at least in accordance with the requirements of instrumentation and control functions of Category B functions if there is no particular potential for the occurrence of a systematic error in the case of a challenge.

3e The measures are planned and appropriately anchored in the operating manual (cf. also answer to Question 4, chapter 0). The RSK recommendation [2], Section 3.2.4, regarding "Simulations in the reactor protection system", "Deactivation" and "Special Switching Operations" is observed.

3f The required equipment is tested at suitable time intervals for the desired functionality or is permanently in operation. Its availability in case of a challenge is guaranteed by corresponding specifications in the operating manual.

3g The influence of the non-availability of the credited equipment on the frequency of hazard states should be assessed probabilistically (e.g. sensitivity or importance analyses).

3.2.2 On Question 2b: Favourable/adverse influences of non-safety systems

Question of the BMUB according to [1]:

In this respect, how are non-safety systems to be treated which are in operation at the time of the occurrence of the event, are not switched off according to the design, and have a favourable/adverse influence on the course of the event?

<u>Consideration of favourable influences of non-safety systems:</u>

A failure of operational systems that are in operation at the time of the occurrence of an event or in the course of the event sequence is assumed in the furnishing of proof in any case if there is a causal connection with the initiating event, e.g. if the auxiliary, supply and energy systems required for operation fail (e.g. electrical power supply, control oil pressure for turbine and bypass valves). This is particularly the case if a loss of offsite power is assumed to occur simultaneously with the occurrence of the event (after reactor scram/turbine trip). Operational systems that have failed in this way will not be credited again even if the necessary auxiliary, supply and energy systems are available again after the emergency diesel generators have started up.

However, there are also operational functions that are not switched off or not switched off directly in the case of the assumed loss of offsite power.

In principle, proof of the control of design basis accidents has to be furnished with sole consideration of equipment of the safety system (cf. 3.2.1). Against this background, operational systems running independently of the assumed loss of offsite power would also have to be "artificially" shut down in the procedure of furnishing proof. If, however, they are subsequently shut down by operational I&C systems anyway, the analysis may also dispense with a prior "artificial" shutdown. However, it must be ensured that this does not lead to substantially more favourable event sequences. Hence, different variants of event sequences may have to be analysed.

Consideration of unfavourable influences of non-safety systems:

According to SiAnf, Annex 5, 3.2.4 (5), *the proper effectiveness of measures and equipment on levels of defence 1 and 2 shall be assumed if relevant adverse influences on the event sequence may result from this.*

The requirement that proper effectiveness shall be assumed does not in itself assume that these systems will become effective due to any inadvertent false signals during the accident sequence. This is justified as an inadvertent actuation of operational equipment due to faulty signals can lead to transients. Thus, the assumption of an inadvertent actuation of operational equipment during the accident sequence would correspond to an assumption of a simultaneous occurrence of an additional event independent of the accident. This cannot be assumed.

As described above, the failure of most operational functions ensues when offsite power is lost with reactor scram/turbine trip after an event has occurred. However, the assumption "loss of offsite power and thus failure of the operational functions without emergency power backup" is not necessarily always an unfavourable boundary condition: In individual cases, there may be relevant influences on the accident sequence if there is no loss of offsite power and if many operational facilities continue to operate unless they are switched off by priority I&C equipment. Therefore, proof of the control of design basis accidents also has to be furnished for the event that there is no loss of offsite power. For this analysis, the continued operation or proper connection of the operational devices is taken into account unless they are switched off (again) as per design by the reactor protection system, limitation systems, or equipment unit protection systems. In these cases, however, it should be checked and assessed to what extent the control of design basis accidents is ensured even in the case of an assumed ineffectiveness of the limitation or equipment unit protection systems. Otherwise, the requirements for the crediting of non-safety systems formulated by the RSK in Section 3.2.1 shall be fulfilled for the reliable shutdown of the non-safety systems in question.

Remark: In this context, however, in the opinion of the RSK, any boundary conditions brought on by the "selected" failure of all operational functions with possibly favourable effects and the continued operation of all operational functions with possibly unfavourable effects would be so hypothetical that this need not be assumed.

Unfavourable influences of non-safety systems due to false signals shall be considered as a causal consequence of earthquakes. However, an explicit consideration in the accident analyses is not necessary if these influences are controlled by measures of the priority I&C equipment and if the latter is designed to withstand the design basis earthquake or is "fail-safe".

The determination of the boundary conditions resulting from the failure or non-failure of equipment not designed against earthquakes may require an engineering assessment. For example, it would be implausible to assume that after an earthquake the electrical auxiliary station service supply would remain available and the reactor coolant pumps would continue to run, while at the same time the cooling of the pump seals and the monitoring equipment unit protection system would fail as a result of to the earthquake. A hypothetical destruction of the pump seals in this way with a possible consequential leak in the primary circuit need not be assumed since both the equipment unit protection system and the cooling of the pump seals would have to fail with both having to be classified as more seismically robust than the auxiliary station service supply.

In summary, the RSK arrives at the following results in answering Question 2b:

- Regarding favourable influences of non-safety systems, the following applies:

  In principle, proof of the control of design basis accidents has be furnished taking only equipment of the safety system into account (cf. 3.2.1). Against this background, operational systems running independently of the postulated loss-of-offsite-power case would also have to be shut down "artificially" in the verification procedure. If, however, they are subsequently shut down by operational I&C systems anyway, the analysis can also dispense with a prior "artificial" shutdown. However, it must be ensured that this will not lead to substantially more favourable event sequences. For this purpose, different variants of event sequences may have to be analysed.

- In the case of unfavourable influences of non-safety systems, the verification shall take into account the addition of signals intended in the event sequence or continued operation unless prevented or rendered ineffective by interventions of the reactor protection system, limitations, or equipment unit protection interventions in accordance with the design.

  Unfavourable influences of non-safety systems as a result of accidental false signals need not be assumed during the accident sequence since the assumption of a faulty actuation of operational systems would mean the simultaneous occurrence of an additional event independent of the accident. This need not be postulated. Causally-induced false signals need not be considered as a consequence of earthquakes either if these influences are prevented by measures carried out by priority instrumentation and control and the instrumentation and control system is designed to withstand the design basis earthquake or as "fail-safe".

However, it should be examined and assessed to what extent event control is given in case of a postulated ineffectiveness of the shutdown of operational facilities by I&C functions that are performed by the reactor protection system. Otherwise, the requirements formulated by the RSK in Section 3.2.1 for taking non-safety systems into account have to be fulfilled for the reliable shutdown of the non-safety systems in question.

Note: A manual shutdown of non-safety systems acting unfavourably may be taken into account in the accident analysis according to [5] 3.1.3h no earlier than 30 min after the occurrence of the event.

3.3 On Question 3: Consideration of human errors or failures to carry out actions provided for in the operating manual in the proof furnished

In what way do human errors or failures to carry out actions provided for in the operating manual have to be considered in the proof furnished?

For the concept of avoiding or controlling human errors or omissions by the plant personnel, the following types of errors have been distinguished:

(1) Operating error in one train (e.g. pump is started without auxiliary system)
(2) Non-implementation or late implementation of planned measures
(3) Aggravating actions, e.g. due to incorrect diagnosis, isolation of a wrong SG, selection of an incorrect path in the operating manual.

To (1):

A human error that results in a failure of a component or a redundant train in safety equipment is considered as being equal to a single failure (as defined in the Safety Requirements for Nuclear Power Plants).

Since the measures and equipment, including their auxiliary and supply systems, which ensure safety functions on level of defence 3 are designed with the single-failure concept in mind, such human errors will not unduly reduce the reliability and effectiveness of these functions.

In the verification process, the failure postulates according to the single-failure concept take such errors into account.

Note: It must be ensured that a corresponding operating error cannot occur in more than one train at the same time (e.g. detectability, grace period, group control).

To (2):

According to the concept of the control of design basis accidents, functions required at short notice have to be automated, i.e. the control is carried out via reliable and priority safety I&C systems. This applies as a rule to all functions that must be triggered within ½ h.

In addition, many functions are automated in the design of the systems for which there is a grace period for actuation that is longer than ½ h (e.g. 1-2 h). This ensures that even after the expiry of the period of ½ h after the occurrence of a design basis accident, during which no manual measures for controlling the incident may be considered, a larger number of manual actions by the plant personnel will not become necessary in the short run.

Based on this automation concept, the following sequence is provided for manual intervention by the plant personnel:

- In the case of the PWR, the personnel is guided via the accident decision tree in the operating manual to the relevant chapter of events on the basis of the reactor protection criteria present. It is checked whether the procedure documented by the instrumentation corresponds to the descriptions. In the case of the BWR, the decision as to which measures are to be taken is made on the basis of the accident sequence diagrams and the examination of the accident sequence on the basis of the main safety functions required in the operating manual.

  The manual measures described in the operating manual are then carried out one by one, using the four-eyes principle, and their expected effectiveness is permanently checked on the basis of feedback from the plant instrumentation.

  Deviations from the expected sequence are detected. If the expected sequence does not develop during further measures and checks, the subsequent measures are taken in accordance with the main safety functions according to the operating manual. Here, various options for fulfilling the main safety function parameters are described.

- In the case of the BWR, only the main safety functions as described in the operating manual are applied, so that any incipient deviations from the main safety function parameters are detected and can be counteracted by the measures described.

Altogether, the RSK assumes on the basis of the quality assurance measures in the development of the operating manual, the time available and various existing criteria for event recognition as well as on the basis of the examination of the decision-making by several persons who regularly have to validate their technical qualification by simulator training that the allocation of the event that has occurred and the resulting plant states to the applicable chapter of the operating manual (event- or main-safety-function-oriented operating manual) is timely and reliable.

In the case of some individual manual operations that are required relatively soon after ½ h has expired, the recognition of the event is confirmed by special acoustic and optical signals (safety hazard signals). For the majority of manual measures, the grace periods are in the range of > 1 hour. This provides the time needed for continuous monitoring by several persons who compare the event sequence with the expected sequence and also monitor compliance with the criteria of the main safety functions required in the operating manual, so that measures that have not been taken are identified in good time and then corrected. The omission of the correction or the transition to the main safety functions required in the operating manual would therefore be equivalent to another error, which need not be postulated.

If, however, the need for a measure is only recognised after a time delay by main safety function monitoring, this may have an unfavourable effect on the course of the event. This might be the case, in particular, for measures that are necessary to achieve the first controlled state (such as in the case of a SGTR or events during low-power and shutdown operation). The RSK assumes that it has been shown within the framework of plant design or probabilistic analyses that the results of the accident analyses are also valid in the case of a postulated delayed execution of planned manual measures. Here, assuming a significantly delayed execution, no single failure in the active safety equipment need be postulated.

The effectiveness of manual measures is also regularly checked within the framework of probabilistic safety analyses (PSA). The manual measures are modelled in the PSA and their remaining unavailability - after possible corrections ("recovery measures") - is evaluated. In the case of significant contributions to hazard states due to manual measures that are not executed or executed late, changes were made to further improve reliability. In the event of plant modifications or new findings, any new manual measures that may be required are reviewed.

All in all, for the reasons mentioned above, the RSK assumes that the non-execution or delayed execution of planned manual measures need not be postulated in the accident analysis.

To (3):

The concept of avoiding or controlling operator actions that could aggravate the sequence consists of the following building blocks:

- For the time range up to ½ h, but in most cases also beyond that, the control of design basis accidents is carried out and monitored by safety I&C, which acts with priority before any manual control. Relevant "aggravating" manual controls are therefore blocked or automatically corrected.

- In phases of accident control in which manual measures are planned, reactor protection signals may be reset under precisely defined conditions. If, however, reactor protection limits are reached as a result of human errors, the reactor protection system will again take over the control of the design basis accident. This way, the effects of "aggravating" manual interventions are limited by the safety I&C system (An example of this is the resetting of the emergency cooling criteria in order to be able to switch off the high-pressure safety injection pumps in the case of an SGTR. If the pressuriser level were inadvertently to drop too much, the pump would be switched on again by the reactor protection system as soon as the excitation criterion "pressuriser level low" is reached.).

- For longer-term processes in the control of design basis accidents, it has to be taken into account that not only the process and the fulfilment of the main safety functions are continuously monitored, which also includes the four-eyes principle as described above in (2), but that the process is also monitored and evaluated by several competent members of the shift and the persons on standby. Thus, "aggravating" manual control actions that are not prevented by the safety I&C and could have recognisable effects on the accident sequence as well as any omitted control actions are recognised and corrected with high reliability.

Hence, the safety concept also covers actions that aggravate the process, which is why these do not have to be explicitly considered in the accident analyses.

3.4 On Question 4: To what extent should the boundary conditions and scenarios considered within the framework of the verification process be included in the chapters of the operating manual dealing with design basis accidents?

The process variables that are important for the operation of the plant are kept within certain tolerance ranges by means of controls and limiting process variables. These have been included as boundary or initial conditions in the accident analyses and must also be included in the operating manual in the form of control values, signal values, and limit values. Further limit values, e.g. from higher-value limitations or from the reactor protection system, have to be adopted in the operating manual in the way they were used in the accident analyses to demonstrate compliance with the acceptance targets.

The boundary conditions resulting from the accident analyses - parameters for event recognition, conditions for the initiation of measures, systems that are available and parameters that have to be reached - shall be fully considered in the operating manual dealing with design basis accidents and, in the case of BWR plants, analogously also in the operating manual dealing with the main safety functions. In particular, these parameters are included in the control of the main safety functions, the control of the system functions, and the effectiveness controls. This makes it possible to initiate, if necessary, any further measures and to check whether the controlled state has been reached.

In principle, the control of a design basis accident can only be demonstrated with the safety system. The required instructions for action are to be contained in the operating manual in a suitable position. However, in accordance with the task, design basis accidents are dealt with in more detail in the operating manual than in the accident analyses, since as a rule all existing equipment is available. Insofar, the descriptions in the operating manual should realistically describe the processes to be expected. Any measures that result from changes in processes which in turn result from the occurrence of faults or failures as they are to be assumed in the verifications have to be dealt with either in an event-sequence-oriented manner or else a manner aiming at the fulfilment of the main safety functions. For the latter, the operating manual dealing with the main safety functions lists measures and equipment with which the main safety functions can be fulfilled. These must also include the measures and equipment credited in the verifications.

If no instructions for action result from the analysis of the event sequence, e.g. in the case of a reactivity accident due to a spurious operation of control elements, no detailed handling of procedures is required in the operating manual. The control of the fulfilment of the main safety functions is an overriding process.

4 References

[1] Beratungsauftrag des BMUB
Sicherheitsanforderungen an Kernkraftwerke zur Beherrschung des Auslegungsstörfalles „Dampferzeuger-Heizrohrleck"
17.03.2015

[2] RSK-Empfehlung (439. Sitzung am 07.07.2011)
Regelungen zu Anlagenzuständen nach Eintritt eines Störfalls

[3] Beherrschung des Störfalles DE-Heizrohrleck – Übersichtsbericht
KWU-Arbeitsbericht R10/2012/81b vom 14.10.1987

[4] Stellungnahme des RSK-Ausschusses ANLAGEN- UND SYSTEMTECHNIK
11.12.2014
Ausbildung und Auswirkungen eines Deionatpfropfens beim Dampferzeugerheizrohrleck

[5] Sicherheitsanforderungen an Kernkraftwerke, 03. März 2015, BAnz AT 30.03.2015 B2

[6] KTA 1201
Anforderungen an das Betriebshandbuch
Fassung 2009-11

[7] Ad-hoc-AG DEHL II
Tabellarische Zusammenfassung von Auswertungen zur Störfallbeherrschung anhand der DWR Ereignisliste aus den „Sicherheitsanforderungen an Kernkraftwerke“, April 2016

[8] RSK-Empfehlung (479. Sitzung der Reaktor-Sicherheitskommission (RSK) am 09.12.2015)
Anforderungen an die Brennelement-Lagerbeckenkühlung

[9] Störfallberechnungsgrundlagen für die Leitlinien zur Beurteilung der Auslegung von Kernkraftwerken mit DWR gemäß § 28 Abs. 3 StrlSchV und Neufassung der „Berechnung der Strahlenexposition“ vom 29. Juni 1994 (BAnz. 1994, Nr. 222a)

5 Compilation of relevant requirements and definitions from RSK recommendations and the non-mandatory guidance instruments

5.1 On Question 1 (Up until which plant state should proof be furnished?)

5.1.1 Definition of the controlled plant state

In the RSK recommendation [2], Chapter 3.1, the **controlled plant state** after the occurrence of an event on level of defence 3 is defined as follows:

*After the occurrence of a design basis accident, a controlled plant state is characterised by the fact **that** the acceptance targets and acceptance criteria are met and the relevant safety variables have reached **sufficiently stationary** values.*

This is explained further below:

Sufficiently stationary** are states in which the safety variables are so stationary or in which the safety margin to the acceptance criteria continuously increases to such an extent **that a sufficiently long period of time is available for the analysis and assessment of the plant state** in order to be able to carry out further measures (e.g. for dealing with design basis accidents) in the event of an unfavourable change in safety variables. **In addition, the period of time must be sufficiently long to allow the preparation and execution of these measures following the analysis.

These definitions and explanations have been incorporated in the "Safety Requirements for Nuclear Power Plants" [5], Annex 1.

In addition, the RSK recommendation [2], Chapter 3.1, explains the following:

*The **initially strongly transient plant state** - in particular in the case of design basis accidents with initial power operation state - **is taken to a controlled plant state, usually by means of the automatic measures of the safety equipment, if necessary also by means of manual measures defined in the accident instructions, taking into account the 30-minute criterion** - in particular in the case of design basis accidents with an initial state of "low-power and shutdown operation". In the case of event-oriented accident procedures, the controlled plant state to be aimed at in each case is specified in the procedures; **when dealing with the design basis accident, there may also be several controlled plant states to be aimed at in succession [...].***

5.1.2 Definition of the safe plant state

In RSK Recommendation [2], Chapter 3.1, the **safe plant condition** after an event on level of defence 3 has occurred is defined as follows:

*After the occurrence of a design basis accident, a safe plant state is characterised by the fact that a **controlled plant state** prevails and that at least the safety-related conditions of a comparable low-power and shutdown operating phase as described in the operating manual are met.*

This definition has been incorporated in the "Safety Requirements for Nuclear Power Plants", Annex 1.
In addition, [2], Chapter 3.1, explains the following:

The long-term goal of the further treatment of a design basis accident after a controlled plant state has been reached is to take the plant to a safe state that meets these requirements. This ensures that, in the sense of the defense-in-depth concept, the plant also controls any failures or events that may occur during a possibly longer phase of the management of the consequences of a design basis accident (see below) [...].

It should be noted that after design basis accidents, plant conditions may prevail that were not considered in the above-mentioned specifications because they do not exist in the specified low-power and shutdown operating state, e.g. the missing "primary system" activity barrier after LOCA events. Insofar as this results in additional requirements for the availability of safety-related equipment to ensure a safe state, these have to be specified specifically for events or main safety functions [...].

The period between reaching a controlled and a safe plant state depends on the type of event and in particular on the extent of available safety equipment. As a rule, it has to be expected that in the case of design basis accidents, the "safe plant state" will establish itself at the same time as the "controlled plant state" with regard to the availability requirements as the failures of safety equipment considered by the design did not occur.

In case that the safety equipment necessary for the safe state is not available to the required extent or other safety-related conditions are not fulfilled due to failures or event-related actions, the operational regulations shall, in accordance with KTA 1201, Chapter 7 [6], contain instructions (e.g., repair measures, transfer to other phases of low-power and shutdown operation, change of conditions, etc.) for the establishment of a safe operating state. If it becomes already apparent at an early stage that repairs or other measures are required to establish a "safe state", such measures may be initiated at any time during the management of an accident, provided that this will note impair the achievement of the controlled state, i.e. the additional resources required for this purpose are available.

5.1.2.1 Requirements for furnishing proof regarding the achievement of the controlled plant state

The RSK Recommendation [2], Chapter 3.2.1, specifies the following requirements for the verification procedure:
*In accordance with the deterministic design concept for achieving the **controlled state**, only safety equipment may be credited for the verification in the licensing procedure (accident analyses). The redundancy requirements of the nuclear non-mandatory guidance instruments have to be taken into account.*

The accident analyses must be carried out under the above-mentioned boundary conditions at least until a controlled state - in the case of several controlled states to be aimed for chronologically until the last "controlled state" - has been reached. *This applies in particular to neutron-physical and thermal hydraulics analyses.*

Irrespective of the furnishing of proof as part of the accident analyses, in case of an event, operational equipment may also be used for dealing with a design basis accident in an optimal manner provided that this equipment is available and its utilisation is possible without repercussions on the safety-related function and the reliability of the safety equipment - in particular the reactor protection functions. However, the operational equipment must not be required from a safety-related point of view. The explanations in Chapter 3.2.4 have to be observed here.

Explanation:

For example, irrespective of the proof that the controlled state can be achieved by safety equipment alone, it is permissible to take operational equipment into account for analyses to demonstrate minimisation of the effects of the postulated design basis accident if this does not impair the reliability of the safety equipment.

Annex 6 of the "Safety Requirements for Nuclear Power Plants", Section 3.2.1 (6), demands the following:
Safety demonstration on levels of defence 2 to 4a must extend from the occurrence of an event at least to reaching ***a controlled plant state, in which the plant may remain permanently****.*

With regard to radiologically representative events, the following is added in Annex 2 of the "Safety Requirements for Nuclear Power Plants", Section 2(3):

The safety demonstration shall cover the period from event occurrence until reaching a controlled plant state, for determination of a source term for radiological safety analyses, the period lasts until the end of the release.

5.1.2.2 Requirements for furnishing proof regarding the achievement of the safe plant state

The RSK Recommendation [2], Chapter 3.2.2, specifies the following requirements for the achievement of the safe state:

After a controlled state has been reached, the plant must be transferred to a safe state, usually with the help of manual measures, unless this state has already been achieved when the controlled state was reached.

Accident instructions must include all steps until a safe plant state is reached.

If necessary for the establishment of a safe state, the restoration of failed safety equipment should be carried out by repair measures. The assumption of functions of the safety equipment by operational equipment in this phase is permissible if the latter is available and its utilisation is possible without repercussions on the safety-

related function and the reliability of the safety equipment. This should be carried out with priority if the start-up of the operational equipment is possible at shorter notice than the repair of failed safety equipment.

5.1.3 Requirements for methods of furnishing proof

The "Safety Requirements for Nuclear Power Plants" [5] place the following requirements on methods of furnishing proof:

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

The deterministic methods comprise

a) computational analysis of events or states,
b) measurement or experiment,
c) engineering assessment.

5 (6) *A measurement or an experiment may be used for the safety demonstration if*

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

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

5 (7) *Engineering assessments may be used for the safety demonstration if assessment criteria exist that are based on scientifically/technically com-prehensible fundamentals.*

5.2 On Question 2 (Consideration of non-safety systems)

The *safety system* and the associated *safety equipment* are defined in Annex 1 of the "Safety Requirements for Nuclear Power Plants" [5]:

Protective action:
The actuation or operation of active safety equipment that is needed for the control of events.

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

Active safety equipment
Equipment of the safety system performing protective actions.

Safety system

The entirety of all equipment that has the task to protect the plant against undue impacts and, in case of design-basis accidents, to keep their effects on the operating personnel, the plant and the environment within specified limits.

According to Annex 1 of the "Safety Requirements for Nuclear Power Plants" [5], the role of the limitation systems is as follows:

Limitation system

Instrumentation and control equipment with one of the following functions:

- *Operational limitation: Limiting process variables to set values in order to increase the availability of the plant.*

- *Protective limitation: Actuation of those protective actions that return monitored safety variables to values at which a continuation of specified normal operation is permissible*

- *Limitation of process variables: Limiting of process variable values to maintain initial conditions for accidents to be considered.*

The following provisions of the "Safety Requirements for Nuclear Power Plants" [5] are particularly relevant for the systems to be considered in the procedure of furnishing proof:

Section 2.1(6):
On levels of defence 2 and 3, measures as well as equipment shall be provided that are arranged in such a way that upon the failure of measures and equipment on levels of defence 1 and 2, the measures and equipment on the subsequent level establish the required safety-related condition independent of measures and equipment of other levels of defence.
Measures and equipment that have to be effective on all or on several of these levels of de-fence shall be designed according to the requirements applicable to the level of defence with the respective most stringent requirements.

Annex 5, 3.2.4 (3):
A loss of station service power supply occurring simultaneously or - depending on the event - with a time lag shall be postulated for all measures and equipment necessary for accident control if this will have an adverse effect on the event sequence. Emergency power supply shall be considered in the analysis according to the switch-on programme of the devices supplied with emergency power.

Annex 5, 3.2.4 (5):

In addition to the assumed loss of functions of the single-failure concept, safety demonstration shall also take into account accident-induced consequential loss of functions of measures and equipment with an adverse effect on the accident with regard to the acceptance target.
If relevant adverse influences on the event sequence may result in case that measures and equipment on levels of defence 1 and 2 will become operative during the event as specified, these influences shall be taken into account.

In Annex 5, 3.2.4 (3), the "Design basis accident calculation bases for the guidelines for the assessment of the design of nuclear power plants with PWR" [9] state that under certain conditions, operational systems can be used to determine the radiological consequences of design basis accidents:

Consideration of operational systems: The consequences of design basis accidents may be calculated taking into account the operational systems and equipment contributing to damage minimisation, provided that this equipment is manufactured and operated in accordance with the applicable rules and guidelines, possesses suitable quality characteristics with regard its design and proven operation, and is not impaired in its functionality by the consequences of design basis accidents.

5.3 On Question 3 (Consideration of manual measures)

5.3.1 Furnishing deterministic proof

In accordance with the "Safety Requirements for Nuclear Power Plants" [5], 3.1 (3), manually actuated protective actions shall generally not be credited in the accident analysis before 30 minutes have elapsed ("30-minute criterion"):

To ensure sufficient reliability of the equipment of level of defence 3 (safety equipment), the following design principles shall be applied in addition to Subsection 3.1 (2):
[…]
h) automation (in the accident analysis, equipment that has to be actuated manually shall in principle not be credited until 30 minutes have passed).

According to 3.1 (6), the reliability and effectiveness of safety functions on level of defence 3 shall be ensured by measures and equipment, including their auxiliary and supply systems, in accordance with the single failure concept in accordance with 3.1 (7) even in the event of failures or unavailabilities. This is specified in Annex 1 as follows:

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

5.3.2 Probabilistic safety analyses

The basic methods and boundary conditions for the preparation of probabilistic safety analyses (PSA) as well as the requirements for their documentation are described in the "Guide Probabilistic Safety Analysis". With regard to the non-availability of manual measures, the following passages in particular are relevant:

Guide PSA, Ch 3.1 – PSA Level 1 for full power operation and low-power and shutdown operation
Dependencies between system functions, common cause failures as well as human actions have to be considered.

Guide PSA, Ch 3.3.6 – Human actions
The analysis of human actions comprises the identification, modelling and probabilistic assessment of actions having an impact on event sequences by the operating personnel. The functions required in the course of an event sequence can depend on human actions in different respects.

Guide PSA, CH 4 – Assessment of the results
The results of the PSA are to be used ***in addition to the deterministic review of the safety status of the plant to assess the balance of the safety concept*** *and to determine the necessity and urgency of necessary safety improvements.*
[Analyses shall be] performed to identify relevant influences of uncertainties on the results when determining reliability parameters of components or when determining probabilities for common-cause failures and ***erroneous human actions****.*

Proposals for the assessment of manual measures within the framework of the PSA are made in the "Methods for probabilistic safety analysis for nuclear power plants", Ch. 3.4, "Human actions":

"Methods for probabilistic safety analysis for nuclear power plants", Ch. 3.4.:
In addition to the technical system analysis, the probabilistic analysis of human actions is an essential part of the PSA. The ***objective is to identify and probabilistically evaluate human actions that influence the result-relevant sequences of the PSA.***

A further distinction is made between the following categories of action:

(A) human actions prior to the occurrence of an initiating event during specified normal operation of the plant,
(B) human actions that result in an initiating event, in particular those that additionally cause the failure of safety-relevant systems,
(C) human actions after the occurrence of an initiating event.

Within category C, a further distinction is made:
(C1) Safety measures based on instructions (procedural safety action),
(C2) measures/errors aggravating [the situation] (aggravating actions/errors),
(C3) unplanned corrective/repair measures (improvising recovery / repair actions).

With regard to the assessment of the failure probabilities, the following is then concluded:

In view of the lack of robust methods for the analysis of types C2 and C3, this document deals only with the analysis of type C1 actions.

When analysing a type C1 action, omission errors (action or partial action not initiated) and execution errors (initiated action and partial action incorrectly executed, e.g. confusion errors, sequence errors, time errors) ***leading to the failure of the action itself*** *have to be taken into account.*

5.4 On Question 4 (Requirements for the operating manual)

With regard to the design of the operating manual for events on level of defence 3, the requirements from KTA 1201 ([6]), Chapter 8, " Requirements Pertaining to the Operating Manual, Part 3 – Design Basis Accidents (Incidents)" are particularly relevant:

(1) This part of the operating manual shall be used to describe the protective goals.

(2) The measures automatically initiated in case of design basis accidents (incidents) shall be specified, as well as those that must be manually initiated by the shift group.

(3) The design basis accidents (incidents) that must be considered for power operation and for no-power operation shall be covered in this part.

(4) The following procedures for the control and mitigation of design basis accidents (incidents) are permissible:
the condition-oriented (protective-goal oriented) handling of design basis accidents (incidents),
the event-oriented handling of design basis accidents (incidents).

(5) The condition-oriented (protective-goal oriented) procedure may be used alone but also in combination with the event-oriented procedure.

(6) A procedure shall be prescribed (e.g. Incident Decision Guide) that can be used in deciding
a. which of the two procedures shall be applied, and in which way, whenever a design basis accident (incident) occurs,
b. how the transition from the event-oriented to the condition-oriented chapter of the operating manual shall be made in the course of a design basis accident (incident), and
c. how the transition to emergency measures (i.e., from the operating manual to the emergency manual) shall be made whenever the protective goal cannot be maintained anymore.

(7) The condition-oriented (protective-goal oriented) chapters of the operating manual shall contain:
a. a description of the individual protective goals to be maintained and of the all-protective-goals-encompassing auxiliary functions,
b. a procedural strategy for maintaining the protective goals,

c. a specification of concrete measures, including the systematic procedural steps to be followed and the specification of the minimum effectiveness of these measures,
d. details with respect to monitoring the effectiveness of measures, including a list of plant parameters which must be particularly monitored,
e. a description of the transition process from the operating manual to the respective emergency measures […].

(8) The event-oriented chapters of the operating manual shall contain documents prepared for the individual plant conditions or events that, in a clear and as concise a form as possible (so-called "concise version"), shall contain the following information:
a. criteria for identifying the plant condition or the event,
b. specification of the automatically proceeding safety-related measures,
c. specification of the essential measures required for the control and mitigation of the design basis accident (incident) that must be manually initiated by the shift group, and
d. details with respect to monitoring the effectiveness of measures, including a list of plant parameters which must be particularly monitored.

(9) Both the condition-oriented chapters and the event-oriented chapters of the operating manual shall contain descriptions of the power plant condition that must be achieved and in which the plant must be kept.

N o t e :
The plant conditions to be achieved shall be specified in such a way that the shift group can check the effectiveness of their measures and can detect any deviations.