RSK Recommendation

DEFENCE-IN-DEPTH CONCEPT

08.09.2005 (386th meeting)

1 Initiation

Within the framework of the BMU project on the update of the nuclear rules and regulations, existing deviations of these rules and regulations from the state of the art in science and technology or gaps shall be identified and proposals shall be submitted to the BMU in form of modules for the necessary amendments. These modules were published with the request for comments until 1. August 2005. In Module 3 “Events to be considered at pressurised and boiling water reactors, as of 15.11.2004”, the safety requirements and demonstration criteria of the levels of defence are defined.

At the 379th meeting on 27.01.2005, the RSK defined the course of discussions for comments on the modules. At the 380th meeting on 24.02.2005, the RSK decided to establish an ad hoc working group LEVELS OF DEFENCE for defining the requirements at the different safety levels in a “defence-in-depth” concept.

2 Course of discussions

The discussions of the ad hoc working group LEVELS OF DEFENCE on the “defence-in-depth concept” took place within the framework of four meetings on 15.03., 21.04., 31.05. and 19.07.2005. At the 381st to 384th meeting, the ad hoc working group presented preliminary results to the RSK which were discussed.

This recommendation was discussed by the RSK at the 385th and 386th meeting and adopted as recommendation at the 386th meeting.

3 Principles of the “defence-in-depth concept”

Within the framework of its discussions on the update of the nuclear rules and regulations, the RSK dealt with concept, strategy and measures of the defence-in-depth concept. The aim of this recommendation is to promote the discussion and practical implementation of the defence-in-depth concept to further improve the safety of the nuclear power plants in operation.

The primary safety objective, the protection of life, health and material goods against the risks of nuclear energy and the harmful effects of ionising radiation, determines design and the safety concept of the nuclear power plants.

The purpose of the defence-in-depth concept is to compensate potential technical failures and human errors at the plant, to maintain the effectiveness of the barriers for confinement of radioactive substances at the nuclear power plant and thus to protect the public and the environment against damages. These goals shall be achieved by the following:

- Prevention of operational occurrences, incidents and accidents by fulfilment of high-standard quality requirements on design, construction, operation, monitoring and maintenance of the plant.

- Availability of several systems and prepared measures that are independent of each other according to a multi-level concept to protect barrier integrity and, if integrity is violated, to mitigate the consequences; in case of failures of systems and measures at a level of defence of this multi-level concept, the consequences of this failure are controlled or mitigated by systems and measures at the next higher level.

- Events that might lead to a failure of systems and equipment relative to defence in depth affecting several levels can be practically excluded by reliable systems and prepared measures.

- Radioactive releases due to incidents or accidents that may occur nevertheless are mitigated by systems and prepared measures.

The defence-in-depth concept should be implemented at five levels according to the following tables. This concept comprises a combination of different technical systems and administrative measures for the prevention or control of abnormal operation and incidents (Levels of defence 1, 2 and 3), for mitigation of the consequences of accidents (Level of defence 4) and measures to support off-site emergency response of the responsible authorities (Level of defence 5).

Note:

The principles related to requirements on components stated in Level 1 are applicable accordingly for Levels 2 to 4.

4 Defence-in-depth concept

Level 1 **Normal operation** **(specified normal operation)** Consistent operation of systems and plant components over the design lifetime. Prevention of abnormal operation, incidents and accidents	Defined as trouble-free operation of the plant. Deviations in operational systems or modes from normal conditions not affecting the operating modes provided in the operating manual for normal operation or affecting power operation shall also be classified as normal operation.
Objective **Confinement of radioactive materials**	During normal operation, the barriers fuel cladding, reactor coolant pressure boundary, enclosure of radioactive materials and containment including operational retention functions ensure confinement. The extent of operation-induced fuel cladding damage (without radiological significance) or operation-induced leakages via glands, flanges etc. shall be kept as small as technically feasible. (Verification objective of the mechanical fuel rod design is that statistically no more than 1 fuel rod per cycle is to be expected as defective.)
Objective **Control of reactivity**	To be ensured by control systems and their control elements, such as control rods, boron injection (PWR), reactor recirculation pumps (BWR). The design of the core and core loading shall be such that there is an inherently stabilising behaviour by reactivity feedback.
Objective **Fuel cooling**	To be ensured by the operational feedwater systems and removal of the steam produced via the main heat sink or the residual-heat removal systems provided.

Impact on the environment and the public	Radiation Protection Ordinance (StrlSchV) § 47, limitation of radioactive releases, adherence to licensed limits, adherence to operational limits, principle of minimisation.
Requirements on systems	The systems shall be designed such that these show margins regarding the requirements on functional condition and integrity applicable for normal operation which cover the uncertainties in design, manufacturing and regarding the ageing effects to be expected. Quality and maintenance shall be such that the frequency of anomalies remains limited to the frequency to be expected according to “good practice”.
Requirements on components	**Principles:** - Consideration of sufficient safety margins in the design of components; - Use of suitable materials; - Maintenance friendliness of components under special consideration of radiation exposure to personnel; - Ensuring and maintaining the quality features during manufacturing, construction and operation; - Performance of in-service inspection to the extent required for safety purposes; - Reliable monitoring of the operating conditions (including ageing); - Recording, evaluation and safety-related use of operational experience; - No crack initiation due to operational loads; - Monitoring concept/monitoring instruments for detection of operation-induced damages. **Design level 0** Limitation of the primary stresses for the design data. Containment: Design level 0 **Load level A (operational loads)** Stress limitation from the sum of primary and secondary stresses, fatigue analysis, verification that the functional requirements of active components are fulfilled Verification for component supports according to load case H (= Hauptlasten, *main loads*) Containment: Load level 1 **Load level P (= Prüflasten, *test loads*)**

	Limitation for primary stresses
Requirements on I&C and electrical engineering	Design and dimensions of the systems and equipment shall be such that a trouble-free operation can be ensured. Operational I&C equipment shall be proven in use. Electrotechnical equipment with operational function incorporated in the safety system has to fulfil the requirements of the safety system.
Requirements on monitoring systems	All processes of specified normal operation shall be monitored and documented according to their significance. This monitoring shall be organised such that spontaneous or slowly developing changes of process parameters, design features of components, reliability features, functions or functional availabilities are identified in a reliable manner. The monitoring system shall display the information in such a form that the operating personnel can reliably perform necessary actions.
Requirements on buildings/structures	For the design, combinations of impacts representing permanent and preliminary loads shall be considered (requirement category A1). The requirements on limitation shall comply with the principles of design requirements on components.
Organisational requirements	A safety management (safety management system, safety-oriented organisation and plant management, promotion of a highly developed safety culture, quality management, qualification of the personnel, maintenance management, ageing management, occupational safety management and environmental protection management) shall be established which ensures safe operation of the plant.

Level 2 **Abnormal operation** **a) Anticipated operational transients without scram (ATWS) or events requiring plant shutdown for operational reasons** **(specified normal operation)** Events occurring in case of malfunction of plant components or systems and whose occurrence is to be expected frequently over the lifetime of the plant concerned according to operational experience and as far as there are no safety-related reasons against (immediate) continuation of operation. Prevention of events requiring use of safety systems and equipment	These include, e. g., turbine trip, load rejection to auxiliary power/zero, loss of a main coolant pump, loss of a main feedwater pump, leakages not leading to actuation of safety systems.
Objective **Confinement of radioactive materials**	The barriers fuel cladding, reactor coolant pressure boundary, enclosure of radioactive materials and containment shall ensure confinement. Loads from these transients must not lead to systematic additional cladding damages or operation-induced leakages via glands, flanges etc.
Objective **Reactivity control**	Power reduction or power limitation required in the short and long term shall be ensured by limitation systems in combination with the control elements. The core design and core loading shall be such that the inherent behaviour (reactivity feedback) ensures the effectiveness of the control elements. The initial values for safe control of incidents shall be adhered to.
Objective **Fuel cooling**	The fulfilment of the criteria of continued usability of the fuel elements/rods shall be ensured by limitation systems in combination with the systems for heat removal. The initial values for safe control of incidents shall be adhered to.

Impact on the environment and the public	Radiation Protection Ordinance (StrlSchV) § 47, limitation of radioactive releases, adherence to licensed limits.
Requirements on systems	Systems (limitation systems) shall be provided that have to be designed and operated such that safe plant operation is also ensured without use of safety systems.
Requirements on components	**Load level B (transient operational loads)** Stress limitation from the sum of primary and secondary stresses, fatigue analysis, verification that the functional requirements of active components are fulfilled No crack initiation due to transient operational loads Verification of component supports according to load case HZ (Haupt- /Zusatzlasten, *main/additional loads*) Containment: see 1
Requirements on I&C and electrical engineering	Design and dimensions of the systems and equipment shall be such that a trouble-free operation can be ensured. Limitation systems shall be proven in use. Electrotechnical equipment incorporated in the safety system has to fulfil the requirements of the safety system. The effectiveness of the limitation of process variables and protective limitation shall also be maintained under consideration of a random error in combination with a maintenance case.
Requirements on monitoring systems	Leakages must be detected that early that they do not lead to the actuation of safety systems. Regarding their impacts, transients shall be monitored insofar that impermissible loads are identified. The monitoring system shall display the information in such a form that the operating personnel can reliably perform necessary actions.
Requirements on buildings/structures	For the design, combinations of impacts representing permanent and preliminary loads shall be considered (requirement category A1). The requirements on limitation shall comply with the principles of design requirements on components.
Organisational requirements	The safety management shall ensure that transient events are analysed for their cause and that effective measures to prevent recurrence are taken.

Level 2 **Abnormal operation** **b) Events with reactor scram** **(normal specified operation)** Events occurring in case of malfunction of plant components or systems and whose occurrence is to be expected over the lifetime of the plant concerned according to operational experience and as far as there are no safety-related reasons against continuation of operation. Prevention of incidents	These include, e. g. loss of main heat sink, loss of all main feedwater pumps, loss of all main coolant pumps, loss of offsite power.
Objective **Confinement of radioactive materials**	see 2a
Objective **Control of reactivity**	Ensuring subcriticality: short term, see 3a, long term, see 2a
Objective **Fuel cooling**	The fulfilment of the criteria of continued usability of the fuel elements/rods shall be ensured by heat removal via operational systems or, in case of their unavailability, via safety systems.
Impact on the environment and the public	see 2a
Requirements on systems	see 2a for operational systems, see 3a for safety systems
Requirements on components	see 2a
Requirements on I&C and electrical engineering	see 3a
Requirements on monitoring systems	see 3a
Requirements on buildings/structures	see 2a
Organisational requirements	see 2a

Level 3 **Incidents** a) Event in case of which plant operation or the respective action cannot be continued for safety reasons. The plant shall be designed against such event sequences. Prevention of accidents	These include, e. g., steam generator tube leak, leaks of the reactor coolant pressure boundary up to a leak size of 0.1A, ruptures outside the containment, transients with failure of the first reactor scram actuation, fuel handling incident, earthquake, fire with impact on safety-relevant equipment. These also include events determining the design under radiological or systems engineering aspects.
Objective **Confinement of radioactive materials**	As far as the initiating event is not a violation of a barrier itself, confinement shall be ensured by the barriers fuel cladding, reactor coolant pressure boundary and containment. In case of LOCAs, • the confinement of radioactive materials shall be ensured by the containment, • the extent of cladding damages shall not exceed 1 % .
Objective **Control of reactivity**	Achievement and maintenance of subcriticality required in the short and long term shall be ensured by the devices of the safety system in combination with the control elements. The core design and core loading shall be such that the inherent behaviour (reactivity feedback) ensures the effectiveness of the control elements. In case of subcooling transients, a short-term recriticality is permissible if the fuel rod integrity remains intact. In case of events such as misloading or falling of fuel elements into the fuel pool, subcriticality must be maintained.
Objective **Fuel cooling**	Fulfilment of the criteria of fuel rod integrity shall be ensured by the safety systems for heat removal.
Impact on the environment and the public	Radiation Protection Ordinance (StrlSchV) § 49, safety-related design for the operation of nuclear power plants.

Requirements on systems	The systems shall be designed and operated such that the requirements of control of incidents are reliably fulfilled. The design features are, among others, the necessary redundancies according to the single-failure concept, diversity for the prevention of common-mode failures, demeshing of subsystems to a large extent, spatial separation of redundant subsystems, safety-oriented system behaviour in case of malfunction of subsystems; preference of passive over active safety functions.
Requirements on components	Verification of capacity for load transfer of primary stresses according to Load level C for the limitation of impermissible plastic deformation and exclusion of instable behaviour. For components whose functions are not required after earthquake and 0.1A leak: stress limitation according to Load level D. For systems required for the control of incidents, verification according to Load level B, for component support according to HS1. Verification for component supports according to load case HS1 (main and special loads). For earthquakes, verification according to HS2/HS3. Verification for containment according to Load level 1, ST1. For earthquakes, verification according to Load level 2, ST3. For ruptures outside the containment, Load level 3. Incident-induced loads must not lead to consequential damages at activity-retaining components due to instable crack propagation. Reaction and jet forces on pipes, components, component internals and parts of buildings shall be considered for load transfer and must not lead to impermissible consequential damage or ruptures.
Requirements on I&C and electrical engineering	I&C systems and equipment shall be designed and set up such that a reliable actuation of the safety-relevant systems and equipment can be ensured at any time. The equipment used shall be qualified for the consequences of incidents and accidents and the operating conditions to be expected. Software used shall be generated according to the principles of safety-relevant programming. Regarding set-up, redundancy and interconnections it shall be ensured that the occurrence of a single failure does not lead to the actuation of safety functions also during maintenance work. For the prevention of consequences transgressing redundancies or systematic failures, adequate measures shall be taken. The design must ensure that the reactor plant is not brought into a beyond-design condition by incident-induced damages, e. g. generation of faulty signals in the safety I&C. The procedural concept of I&C shall be such that there is no

	need for manual intervention within the first 30 minutes.
Requirements on monitoring systems	All processes and parameters required within the frame of incidents for the identification of the event, the assessment of the effectiveness of the safety system, the assessment of the consequences and the assessment of the necessary supplementary measures shall be monitored. The monitoring system must display the information in such a form that the operating personnel can reliably perform necessary actions. The necessary instrumentation shall be designed such that it reliably withstands the consequences of incidents and accidents (e. g. pressure, temperature, acceleration). The information shall be processed such that traceability is ensured also in case of long-lasting events.
Requirements on buildings/structures	With this combination of loads, further usability of the building shall be given after occurrence of the load cases. Design earthquake: see 3b.
Organisational requirements	It shall be ensured that the responsible operating personnel has all the knowledge, means, capabilities and authorisations required for the control of incidents. It shall be ensured that in case of design-basis accidents skilled personnel will be available for support at any time.

Level 3 **Incidents** b) Postulated event in case of which plant operation or the respective action cannot be continued for safety reasons. Independent of their occurrence probability, these load cases serve for the design of defined systems and components. Prevention of accidents	These include leak cross sections of a main coolant line (PWR), or for BWR main steam and feedwater lines up to the first shut-off valve, from > 0.1A up to 2A and the RPV bottom leak. A prerequisite regarding the requirements is that for the reactor coolant pressure boundary the requirements for limited break postulations are fulfilled.
Objective **Confinement of radioactive materials**	The confinement of radioactive materials shall be ensured by the containment. The extent of cladding damages shall not exceed 10 %.
Objective **Control of reactivity**	Achievement and maintenance of subcriticality required in the short and long term shall be ensured by the devices of the safety system in combination with the control elements and the inherent properties of the reactor core.
Objective **Fuel cooling**	By safety systems for heat removal, the damage shall be limited to such an extent that the coolability of the core remains ensured.
Impact on the environment and the public	see 3a
Requirements on systems	see 3a
Requirements on components	Verification of capacity for load transfer of primary stresses according to Load level D. For systems required for the control of incidents: verification according to Load level B. Verification of component supports according to load case HS2 and HS3 (main and special loads). Verification for containment according to Load level 1, ST1. Incident-induced loads must not lead to consequential damages at activity-retaining components due to instable crack propagation. The stability of the components reactor pressure vessel, steam generator, main coolant pumps and pressuriser

	must be ensured for the static force P_{ax} (2 x P x F).
Requirements on I&C and electrical engineering	see 3a
Requirements on monitoring systems	see 3a
Requirements on buildings/structures	For global structures, crack formation and deformations that remain limited are admissible as far as there are no safety-related reasons against it. For reasons of stability or reliability of plant components, additional conditions shall be fulfilled, where required, at defined locations (e. g. deformation and crack width limitations) that go beyond the minimum requirements of load-carrying capacity.
Organisational requirements	see 3a

Level 4 **a) Very rare events** Very rare events against which the plant shall be designed. Prevention of significant releases into the environment.	Military aircraft crash, explosion blast waves, toxic or explosive gases, anticipated operational transients without scram (ATWS).
Objective **Confinement of radioactive materials**	The confinement of radioactive materials shall be ensured by maintenance of the integrity of reactor coolant pressure boundary and containment.
Objective **Control of reactivity**	Achievement and maintenance of subcriticality required in the short and long term - in case of ATWS only long term - shall be ensured by the operational and safety systems in combination with the control elements. The core design and core loading shall be such that the inherent behaviour (reactivity feedback) ensures the effectiveness of the control elements.
Objective **Fuel cooling**	The coolability of the core shall be ensured by operational or safety systems.
Impact on the environment and the public	Prevention of significant releases.
Requirements on systems	For the short-term control of event sequences, systems with high reliability shall be available that are protected and designed against the causal impacts. For the control of these events in the medium and long term, all systems may be considered in case of demand. For military aircraft crash, explosion blast waves and toxic or explosive gases, the necessary systems shall be designed such that an intervention by the personnel is not required for ten hours.

Requirements on components	Stress limitation for the components during ATWS according to Load level C. Vibration-induced system loads for military aircraft crash, explosion blast waves, toxic or explosive gases: verification according to Load level D. For components for active control of the events: stress limitation according to Load level B. Requirements for containment: Load level 3, ST6. Component support: verification according to HS2/HS3.
Requirements on I&C and electrical engineering	ATWS (short-term measures) see 3a A control point designed against military aircraft crash, explosion blast waves and toxic or explosive shall be established where all information required for the control of the event are available and at which the necessary interventions and controls can be performed in case of demand. An intervention by the personnel must not be required within the first ten hours. All necessary systems and equipment shall be protected against loads from external impacts.
Requirements on monitoring systems	see Requirements on I&C and electrical engineering
Requirements on buildings/structures	see 3b Special requirements from military aircraft crash: Prevention of consequential damages due to concrete fragments, prevention of fuel entry through large crack openings.
Organisational requirements	Regarding personnel and local conditions, the organisation shall be such that the loss of the main control room is also covered. For military aircraft crash, explosion blast waves and toxic or explosive gases, adequately qualified personnel shall be available at the plant within ten hours. For these events, adequate communication facilities shall be provided.

Level 4 **b) Accidents** Events with multiple failures of necessary safety systems and equipment. Prevention of severe core damages.	These are events during which multiple failures of necessary safety systems and equipment occur and design-basis limits are exceeded. Severe core damages shall be prevented by preventive accident management measures.
Objective **Confinement of radioactive materials**	Measures and equipment shall be provided which, regarding the activity inventory of the reactor core and the irradiated fuel elements stored in the fuel pool, are aimed at the maintenance of at least one of the barriers still existing.
Objective **Control of reactivity**	Subcriticality shall be maintained or restored by the respective control elements.
Objective **Fuel cooling**	Measures and equipment shall be provided to maintain or restore fuel element cooling for the prevention of severe core damages, to bring the plant into a condition which enables the fulfilment of the objectives of defence in depth.
Impact on the environment and the public	see 4a
Requirements on systems	The concept for measures and equipment of accident management shall be such that they can be used effectively for a broad spectrum of events, event sequences and phenomena. They shall be diverse to the safety systems postulated to be failed. The compatibility with the safety concept of the plant shall be verified. The accident management measures must neither impair specified operation in an inadmissible manner nor the use of safety systems for the control of design-basis events. There are no requirements on redundancy, diversity, demeshing and spatial separation of the technical systems and equipment specially provided for accident management measures.
Requirements on components	For components provided for accident management, it shall be demonstrated that they can effectively be operated under the loads and environmental conditions to

	be expected for the event sequence. The corresponding verifications for these required properties shall be oriented towards the limitations for integrity and function, as they are formulated in Levels of defence 2 and 3.
Requirements on I&C and electrical engineering	Accident management measures requiring intervention in I&C and electrical systems are to be considered anticipatory and shall be implemented by qualified devices. Special systems and equipment for accident management measures must not have any retroactive effects on the safety system.

Requirements on monitoring systems	The instrumentation shall provide sufficient information about the condition of the plant in order to • be able to take necessary accident management measures and to determine their effectiveness, • give indications on the event sequence, and • allow an assessment of the impacts on the environment.
Requirements on buildings/structures	see 3b
Organisational requirements	For these events, an emergency response organisation shall be available which performs the co-ordination of the measures internally and with the external organisations. For the description of the organisation and the technical measures, an accident management manual shall be prepared.

Level 4 **c) Accidents with severe core damages** Prevention of significant releases into the environment.	These are events that led to severe core damages. By special measures and equipment (mitigative emergency measures and strategies) the consequences of accidents shall be mitigated.
Objective **Confinement of radioactive materials**	Measures and equipment shall be provided which, regarding the activity inventory of the reactor core and the irradiated fuel elements stored in the fuel pool, are aimed at the maintenance of at least one of the barriers to achieve limitation of activity release. Here, the integrity of the containment should be maintained and a condition that is controllable in the long term reached. Accordingly, adequate strategies and systems • for the prevention of high-pressure core melting, • for the prevention of extensive H_2 combustions that might endanger the integrity of the containment, and • for the prevention of overpressurisation failure of the containment and unfiltered release shall be provided.
Objective **Control of reactivity**	-
Objective **Fuel cooling**	Strategies for the use of systems still available for heat removal.
Impact on the environment and the public	see 4a

Requirements on systems	The concept for measures and equipment shall be such that they can be used effectively for a broad spectrum of accident sequences and phenomena. The compatibility with the safety concept of the plant shall be verified. The accident management measures must neither impair specified operation in an inadmissible manner nor the use of safety systems for the control of design-basis events. There are no requirements on redundancy, diversity, demeshing and spatial separation of the technical systems and equipment specially provided for accident management measures.
Requirements on components	It shall be demonstrated that for the containment an adequate margin to the failure load is maintained.
Requirements on I&C and electrical engineering	see 4b
Requirements on monitoring systems	The information necessary for the assessment of the plant condition shall be provided by an adequate instrumentation. A sampling system shall be provided for the analysis of radioactive aerosols and gases in the containment atmosphere.
Requirements on buildings/structures	Building parts and structures required to mitigate the consequences of accidents shall be designed such that the stability of the respective buildings or building parts can be ensured. Measures shall be provided that enable the personnel to stay at the control room for a longer time.
Organisational requirements	Severe accident management guidance strategies shall be provided for the support of the emergency task force.

Level 5 **Accidents with significant releases into the environment**	These are defined as events that lead to significant releases into the environment and require protective measures within and outside the plant. Measures shall be provided to support off-site emergency response of the responsible authorities, as for example • provision of information on the release and plant condition, • classification of events and recommendation on triggering of alarms, • support for environmental monitoring and measurement programmes, and • provision of qualified personnel.
Objective **Confinement of radioactive materials**	-
Objective **Control of reactivity**	-
Objective **Fuel cooling**	-
Impact on the environment and the public	Mitigation of consequences of accidents
Requirements on systems	-
Requirements on components	-
Requirements on I&C and electrical engineering	-
Requirements on monitoring systems	-

Requirements on buildings/structures	-
Organisational requirements	For these events, an emergency response organisation shall be available which performs the co-ordination of the measures internally and with the external organisations. This organisation shall ensure that proper communication with the disaster management authorities takes place. Further, all information shall be submitted immediately that may be of importance for the assessment of the accident occurrence and initiation of protective measures. The effectiveness of emergency organisation and the co-operation with the competent authorities shall be checked by means of regular emergency exercises. The emergency response organisation shall have technical systems, communication facilities, tools and protective equipment at its disposal to the required extent for the fulfilment of its tasks.