This is an unofficial translation of the text.

The translation is prepared based on Govt. Decree No. 118/2011 (VII. 11.) being effective as of 10.04.2018

Annex 3 of Govt. Decree No. 118/2011 (VII. 11)

Nuclear Safety Code

Volume 3

Design requirements for operating nuclear power plants

3.1. INTRODUCTION

3.1.1. The scope of regulation

3.1.1.0100. The purpose of this code is to define the design requirements and design principles for the nuclear power plant as a nuclear facility, as well as for its systems, structure and components that are important to nuclear safety.

3.1.1.0200. The provisions of this Code Volume shall apply to setting design requirements for all nuclear power plants having water-cooled, thermal neutron reactors currently operated in the territory of Hungary, with the proviso that

the provisions applicable to the design process described under Sections 3.2.1.0100 to 3.2.1.0500, 3.2.1.2200, 3.2.1.2500 to 3.2.1.2800, 3.3.1.0100 to 3.3.1.0200, 3.3.1.0500, 3.3.2.0700 to 3.3.2.0900, 3.3.2.1200 to 3.3.2.1300, 3.3.2.2800, 3.3.2.3600, 3.3.3.0100, 3.3.3.0700, 3.3.3.0900, 3.3.5.0400, 3.3.5.0700, 3.3.5.1000, 3.4.3.0300 and 3.5.1.1700 shall apply during the modification of an operating unit and preparatory design activities for the successive lifecycle phase.

3.2. GENERAL DESIGN REQUIREMENTS

3.2.1. Basic design requirements

3.2.1.0100. The licensee shall operate such a management system that controls the complex design system and ensures the quality and consistency of the designs as well as the fulfilment of nuclear safety requirements.

3.2.1.0200. The adequacy of the designs including design tools, data and results shall be reviewed by an organization independent of the designer.

3.2.1.0300. The design process shall be defined by identification of all design requirements in the preliminary design phase. Based on the identified requirements the necessary design specifications and tasks shall be defined for the fulfilment of such requirements.

3.2.1.0400. A nuclear power plant shall only be designed by such a design organisation, which holds such a qualification that is valid for the specific design field as determined by law or in the absence of that determined by the licensee and which is authorized to perform the task.

3.2.1.0500. The licensee may contract a design organisation for the coordination of the design review and design management tasks for the nuclear power plant.

3.2.1.0600. The licensee shall ensure that the plans are at least as detailed as it is required for conducting the regulatory licensing procedures relevant for the specific lifecycle phase.

3.2.1.0700. The design basis for nuclear safety related systems, structures and components shall be systematically defined and documented. The technical requirements must be recorded in the design specifications.

3.2.1.0800. It shall be ensured that the licensee of the nuclear power plant has all such design information which is necessary to uphold the responsibility for the safe operation of the nuclear power plant. The licensee shall be able to make safety related decisions, and to perform or have such activities performed that ensure the safety of the nuclear power plant throughout its service lifetime.

Ensuring fundamental safety functions

3.2.1.0900. Fundamental safety functions shall be achieved in the case of DBC1-4. Following DEC1-2 plant states, the fundamental safety functions shall be performed to such a degree that the nuclear reactor can be brought to a controlled, safe shutdown condition, while following a severe accident to a safe condition.

3.2.1.1000. Systems shall be designed to perform the fundamental safety functions.

3.2.1.1100. To perform the fundamental safety functions all safety functions and systems providing these safety functions shall be defined.

3.2.1.1200. Monitoring of the status of the systems, structures and components of the nuclear power plant shall be provided in order to verify if the basic design requirements are fulfilled.

3.2.1.1300.

Application of the defence in-depth principle

3.2.1.1400. During the application of the five levels of defence in-depth, beside the requirements specified in Article 7 the additional requirements listed in sections 3.2.1.1500.-3.2.1.1800 shall also be complied with.

3.2.1.1500. Multiple physical barriers shall be applied during the design to prevent uncontrolled release of radioactive materials to the environment. The mutually

independent physical levels shall ensure that possible failures, deviations from normal operations can be detected, compensated and managed.

3.2.1.1600. The barriers shall be protected. Design solutions shall ensure the safety functions and the fulfilment of safety criteria should either level of defence in depth be impaired.

3.2.1.1700. During design of a nuclear power plant, in accordance with the defence in-depth principle:

a) it shall be ensured by design solutions that the fundamental safety functions are performed by means of the safety barriers or mitigating the consequences of any abnormal operation or deviation.

b) systems providing safety functions shall be applied to prevent or manage DBC2-4 and DEC1-2 and;

c) the design of the barriers shall be conservative, their implementation shall be of the highest standards to ensure:

ca) the probability of failures and deviations from normal operating conditions shall be as low as reasonably achievable,

cb) DBC4 and DEC plant states shall be prevented to a reasonably achievable level, furthermore

cc) no cliff edge effect can arise;

d) the manageability of the condition of the nuclear power plant shall be ensured by technical means in such a way that in the event of a failure or deviation from normal operating conditions the necessity to operate the systems providing safety functions shall be as limited as possible;

e) the control of nuclear power plant conditions shall be highly reliable even under conditions requiring the operation of the systems that provide safety functions, and shall not require human intervention in the preliminary phase of the process.

3.2.1.1800. It shall be ensured as far as reasonably achievable that:

a) events that challenge the integrity of the barriers are prevented, and the endangering circumstances are tolerated;

b) concurring failure of more than one barrier is avoided;

c) a barrier shall not fail due to the failure of another barrier or another system component; furthermore

d) the detrimental consequences of human errors during operations or maintenance are avoided.

Other general design requirements

3.2.1.1900. Systems providing safety functions shall be designed in such a way that the safety functions are performed as reliably throughout the lifetime as required in the design.

3.2.1.2000. In the designs sufficient reserves shall be provided for the defects of design methods and means, for the manufacturing and installation tolerances, for postulated failures and for the conservatively estimated rate of degradation processes as a result of ageing mechanisms during the design lifetime.

3.2.1.2100. Systems, structures and components that are important to safety shall be designed according to proven standards of nuclear industry. The standards selected for the design process shall be preliminarily defined, their applicability shall be justified.

3.2.1.2200. Systems, structures and components providing safety functions shall be designed by using such construction methods that have been previously tried and tested. For other instances such technologies and products shall be used, the applicability of which is evaluated and verified. In case of new design solutions, which differ from the accepted solutions of the engineering practice, the applicability shall be substantiated from safety aspect with adequate research, tests, and analyses of experience from other applications. New solutions shall be tested before implementation. The operation of the system and components shall be monitored during operations for final validation of suitability.

3.2.1.2210. It shall be demonstrated that the component important to nuclear safety is error-free or that the in-service inspections and tests applied are suitable to detect any possible failure, and the so detected failure can be managed.

3.2.1.2300. A labelling/tagging system shall be implemented to identify systems, structures and components.

3.2.1.2400. During design, experience accumulated during the design, construction and operation of nuclear power plants and relevant research results shall be taken into account.

3.2.1.2500. During design, the safety analysis methods shall be applied as defined in this decree from the early stages of the design.

3.2.1.2600. Systems, structures and components shall be designed in a way that fabrication, installation, construction, inspection, maintenance and reparation is ensured.

3.2.1.2700. The design shall facilitate the possibility of decommissioning of the nuclear power plant, minimize activation of the elements and shall provide for decontamination, access and considerations to management of decommissioning.

3.2.1.2800. The requirements for nuclear safety, security and safeguards shall be implemented in an integrated way and by considering the synergies.

3.2.1.2900. In the case of a nuclear power plant with multiple units, a justified level of independence of the units shall be ensured.

3.2.2. Design basis for safety

Categorization of nuclear power plant conditions and occurrences

3.2.2.0100. Conditions that deviate from normal operation shall be categorized into design basis or design extension condition categories.

3.2.2.0200. Based on their frequency, normal operation, as well as the events leading to the conditions comprised in the design basis of the nuclear power plant, shall be assigned to the operating conditions listed in the following table.

	A	B	C
1.	Operating condition	Description	Frequency of event (f [1/year])
2.	DBC1	normal operation	–
3.	DBC2	anticipated operational occurrences	$f \geq 10^{-2}$
4.	DBC4	design basis accident	$10^{-2} > f \geq 10^{-5}$

3.2.2.0300. The following categories of the extended design basis shall be distinguished:

a) complex accident (DEC1), or

b) severe accident (DEC2).

Safety classification

3.2.2.0400 to 3.2.2.2100.

3.2.2.2110. The systems, structures and components shall be categorized into safety classes on the basis of their effects on safety and their functions. Classification

for earthquakes as a special hazard factor shall be handled in accordance with the independent system detailed in Section 3.3.6. The analyses supporting safety classification of the systems, structures and components shall be based primarily on deterministic methods supplemented with probabilistic methods and engineering judgement, as necessary.

3.2.2.2120. Safety functions shall be grouped into three safety classes on the basis of the expected consequences of the damage they may sustain. The safety classification of systems, structures and system components shall be carried out on the basis of the function in the highest class (bearing the lowest number) implemented by them.

3.2.2.2130. Safety Class 1 shall include:

a) fuel assemblies, and

b) safety functions and systems, structures and system components providing them, the failure or defect of which may lead to such an event that directly endangers the ability of the nuclear reactor to reach immediate subcritical condition or cool down, and requires the immediate actuation or operation of systems or components eliminating design basis accident basis accidents.

3.2.2.2140. Safety Class 2 shall include the safety functions and systems, structures and system components providing them, including the electrical and control and instrumentation systems and system components required for their operation, the actuation at the appropriate time or continuous operation of which is required in order to avoid DEC plant states resulting from design basis events. They are also responsible for ensuring the subcriticality and cooling of the nuclear reactor when events affecting nuclear safety occur or for preventing the discharge of radioactive materials released from the nuclear reactor as a result of an event occurring within the containment and affecting nuclear safety. Systems, structures and system components that ensure the subcriticality, the maintenance of the integrity and the necessary cooling of fresh and irradiated fuel assemblies stored outside the cooling system of the nuclear reactor shall also be included in this category.

3.2.2.2150. Safety Class 3 shall include the safety functions and systems, structures and system components performing them, which:

a) prevent design basis accidents, and if possibly being inoperable during a design basis accident, it will not influence the course of the breakdown, or

b) ensure that radiation sources outside the nuclear reactor do not present additional radiation exposure to the operating personnel and the population, or

c) by their operation, prevent the necessity to actuate systems in Class 2,

d) if inoperable, hinders the monitoring of operation of the technology within its safe parameter range or the preservation of such information, or

e) are systems, structures or system components to provide such functions that mitigate the radiological consequences of DEC1-2 plant states, prevent or hinder their evolution, and provide information in the case of DEC1-2 plant states.

3.2.2.2160. Non-safety Class 4 shall include all functions and systems, structures and system components performing functions that do not belong to Safety Classes 1, 2 or 3.

3.2.2.2161. The primary system components of systems performing safety functions shall belong to the same safety class as the system itself.

3.2.2.2162. Auxiliary systems that are required for the performance of the safety function of a system, structure or system component on which classification is based shall be included in the same class as the system itself.

3.2.2.2163. Building structures shall also be included into safety classes. For the classification of building structures, the safety functions that can be assigned to the building structures as well as the systems, structures and system components important to nuclear safety, which are jeopardised by their deterioration or loss of the function, shall be taken into account. Of the safety functions so specified, the one included in the highest class shall form the basis for the classification of the building structure.

3.2.2.2164. Control and instrumentation equipment, together with their subsystems, shall be included in the safety class in accordance with the highest class safety function performed by them.

3.2.2.2165. Design requirements based on national and international standards and proven engineering practices shall be assigned to the safety classes of systems, structures and system components and shall be consistently applied.

3.2.2.2166. The process of safety classification applied during design shall be documented to a level of detail that the results can be verified by independent reviews.

Design basis of the nuclear power plant

3.2.2.2200. For the design all those initiating events shall be postulated that may influence the safety of the nuclear power plant. Of these events the ones to be incorporated into the design basis shall be selected by a deterministic method or deterministic and probabilistic methods.

3.2.2.2300.

3.2.2.2400. When defining the design basis, reasonably conservative assumptions shall be applied to compensate for uncertainties.

3.2.2.2500. For each operating condition, a set of design limits shall be determined for the physical parameters of the nuclear safety related systems, structures and system components. The design limits shall be consistent with the nuclear safety requirements and applied standards.

3.2.2.2600. The limiting conditions and requirements to be used for the design of nuclear safety related systems, structures and components shall be derived from the initiating events resulting in DBC1-4.

3.2.2.2700. Among the postulated initiating events all those occurrences shall be considered that:

a) are related to the site of nuclear power plant and its surroundings and have an environmental origin;

b) are intentional, but not purposefully directed against the nuclear power plant, or are the result of unintentional human actions within or outside of the plant site; or

c) derive from the operation of the nuclear power plant, or the failure of its systems, structures and components.

3.2.2.2800. All events that may have radiological consequences and cannot be excluded on the basis of Section 3.2.2.3400 shall be included in the design basis. Those postulated initiating events shall also be included that occur during low power state or when the nuclear reactor is shutdown and disassembled. Such foreseen occurrences taking place outside of the nuclear reactor shall also be included in the design basis.

3.2.2.2900. During the design of the nuclear power plant all possible internal and external hazards shall be determined.

3.2.2.3000. The following external hazards shall at least be considered in the design of the nuclear power plant:

a) extreme wind load,

b) extreme external temperatures,

c) extreme precipitation conditions,

d) lightning,

e) floods, icy floods, summer floods, and low water level,

f) the danger of damage to upstream and downstream facilities,

g) flying objects moved by wind,

h) extreme cooling water temperatures and icing,

i) geological characteristics used to justify suitability of the site (in particular earthquake characteristics, and soil liquefaction susceptibility),

j) crash of a military or civilian aircraft,

k) transport or industrial activities near the plant site,

l) disturbances in the connecting external electric grid including total and lasting failure of the electric network,

m) such buildings on the site or in the vicinity of the site that may present fire, explosion or other dangers to the plant,

n) other fire started off-site,

o) electromagnetic interference, and

p) biohazards.

3.2.2.3010. Among the external hazard factors, those included in the design basis shall be selected on the basis of a site-specific analysis.

3.2.2.3020. In the case of hazard factors of natural origin, the design basis events shall be compared to historical data and it shall be demonstrated that past extreme events have also been taken into account with a sufficient margin during design.

3.2.2.3100. The following internal hazards shall at least be considered in the design of the nuclear power plant:

a) loss of coolant accidents;

b) break in the main steam- and main feedwater system;

c) uncontrolled decrease of primary flow rate;

d) uncontrolled increase or decrease of the main feedwater flow rate;

e) uncontrolled increase or decrease of the main steam flow rate;

f) unintentional opening of the pressurizer valves;

g) unintentional operation of the emergency core-cooling systems;

h) unintentional opening of the steam generator safety valves;

i) unintentional closing of the main steam isolation valves;

j) steam generator tube rupture;

k) unintentional movement of the control rods;

l) uncontrolled withdrawal or ejection of the control rods;

m) instability of the active core;

n) malfunction of the chemical and volume control system;

o) break of a pipe connected to the primary cooling loop of the nuclear reactor that is partially outside of the containment, or the damage to a heat exchanger tube;

p) accidents related to the handling, moving and storing of the nuclear fuel;

q) dropping of a heavy load when using lifting equipment;

r) consequences of fire, explosion and internal flooding, and the initiating events caused by these;

s) conditions potentially triggering initiating events, such as missiles, including dislodged turbine parts, release of dangerous medium from broken systems, vibration, whipping movement of a broken pipe, jet impact; and

t) overvoltage or the instability of the electricity grid.

3.2.2.3200. All realistic combination of the individual occurrences shall be considered during design, including external and internal events, which may lead to DBC4 or DEC plant states. The event combinations to be taken into account in the design shall be selected by taking into account both engineering considerations and probabilistic analyses.

3.2.2.3300.

3.2.2.3400. For the design, the following can be excluded from the scope of postulated initiating events:

a) internal initiating event due to the failure of a system, structure or component, and/or human error, if the frequency of the occurrence is less than 10^{-5}/year;

b) event resulting from external human activity typical of the site, if the frequency of the hazard factor is less than 10^{-7}/year, or if the hazard factor is at such a distance, that it can be justified that it will not have an effect on the nuclear power plant unit; and

c) initiating events occurring due to a recurring external hazard factor of natural origin, with a frequency of less than 10^{-4}/year, or external hazard factor of natural origin for which it can be demonstrated that they are not able to pose a physical hazard to the power plant.

3.2.2.3500. At a power plant site with several nuclear power plant units, for the design of the whole nuclear power plant as well as for the individual nuclear power

plant units it shall be considered that some external hazard factor s may affect all nuclear power plant units simultaneously.

3.2.2.3510. In the case of a nuclear power plant having more than one unit, the possibility of the common cause failure of safety systems commonly applied by the units shall be examined during the design.

3.2.2.3600. In case of such a site, where more nuclear power plant units are operating or in the vicinity of which there is another nuclear facility, the effect of each unit and facility on all other units and facilities, for all operating conditions of the facilities as well as for all circumstances resulting from all postulated hazard factors shall be analyzed. For the analyses of the effects, the construction, commissioning and decommissioning lifecycle phases shall also be considered.

3.2.2.3700. Design solutions shall ensure that following DBC2 to 4 the nuclear power plant unit reaches controlled state, then safe shutdown state as fast as reasonably possible. Controlled state shall be achieved within 24 hours, at the latest, safe shutdown state shall be achieved within 72 hours, at the latest.

3.2.2.3710. The stability of, and changes in external factors affecting the nuclear safety of nuclear power plant units shall be forecasted for their whole lifetime.

Extension of the design basis

3.2.2.3800. In accordance with the defence-in-depth concept, for the extension of the design basis the events resulting in DEC plant states shall be considered and selected in such scope that the probabilistic safety criteria defined under Sections 3.2.4.0600 and 3.2.4.0900 can be fulfilled, while the reasonably achievable measures to prevent or mitigate consequences can be defined and applied. The events and combination of events leading to DEC plant states to be considered shall be selected by deterministic analyses, probabilistic methods and engineering judgement. Out of the analysis methods for demonstration of safety that shall be selected which is the most appropriate or the most appropriate combination for the examined case.

3.2.2.3810. The DEC analyses shall take into account all available validated data and, if it is possible, connections shall be established between the severity of the hazard factors, especially the extent, duration and occurrence frequency. If it is possible, the maximum, but still grounded severity of the hazard factors shall be determined.

3.2.2.3900. For the extension of the design basis the following shall at least be considered, if it is not yet included in the design basis and if it is applicable for the specific nuclear power plant type:

a) station blackout,

b) loss of systems performing reactor shutdown functions during a DBC2 operating condition,

c) break of a steam line with partial damage to the heat-exchanger surface of the steam generator,

d) events that bypass the containment and result in direct releases to the environment,

e) total loss of feedwater,

f) loss of coolant and total loss of an emergency core-cooling system type,

g) uncontrolled level decrease during natural circulation with partially filled loop or refuelling operating condition,

h) total loss of one or more auxiliary systems of the equipment providing fundamental safety functions,

i) loss of cooling of the active core during removal of residual heat,

j) loss of cooling of the spent fuel pool,

k) uncontrolled dilution of boric acid,

l) simultaneous rupture of several heat exchange tubes of a steam generator,

m) loss of systems required for the long-term management of a postulated initiating event,

n) loss of the ultimate heat sink, and

o) other events resulting in fuel melting.

3.2.2.3910. In the selection of events leading to DEC1 plant states, all events or event combinations about which it cannot be established with high certainty that the probability of their occurrence is very low and may lead to conditions that have not been taken into account in the design basis shall be taken into account. In the selection of the events the following should be considered:

a) events that occur during the possible operating conditions,

b) events that occur for the effect of internal and external hazard factors,

c) common cause failures,

d) impact of the nuclear facilities in the vicinity, in case of site with multiple units the mutual impacts of the units, and

e) those events that may impact all facilities in the vicinity together with the mutual effects assumed among them.

3.2.2.3920. All DEC2 plant states shall be identified.

3.2.2.3930. The DEC analyses and designs shall identify all reasonably achievable measures by which severe accidents can be prevented. Irrespective of the success of the identified measures, preparations shall also be made for severe accidents. As part of the analyses and design, all reasonably implementable solutions by which the consequences of severe accidents can be limited shall also be identified.

3.2.2.3940. In the analysis of DEC events and the determination of the reasonably practicable safety improvement measures:

a) only well-founded methods and assumptions may be applied;

b) the reproducibility of the analysis shall be ensured even in cases where engineering judgements were taken into account during the analysis as well as all uncertainties relating to the analysis and their effects shall be taken into account;

c) all preventive or consequence-mitigating measures by which the resistance of the power plant can be increased with regard to the conditions not taken into account in the design basis shall be identified;

d) the potential radiological effects of DEC events on and off site shall be examined, assuming that the emergency response measures are successful;

e) the location and structure of the power plant, the capabilities of the equipment, the conditions associated with the event reviewed and the efficiency of the planned emergency response measures shall be taken into account;

f) it shall be demonstrated that sufficient margins are available for avoiding the cliff edge effect endangering a fundamental safety function;

g) it shall be shown that the results of Level 1 and 2 probabilistic safety analyses have been taken into account;

h) where relevant, phenomena occurring during severe accidents shall be taken into account;

i) final conditions or, where possible, safe conditions as well as the required operating time of the systems, structures and system components connected to them shall be defined;

j) the most effective ways of ensuring the fundamental safety functions shall be identified and assessed;

k) those events shall also be considered, which simultaneously impact more units, and redundant or diverse systems, structures and components, or impact the site or regional infrastructure, off-site services and measures, and

l) it shall be demonstrated that in the case of a multiunit nuclear power plant, the resources of common use are available in a due quantity, which shall also be confirmed by an on-site inspection.

3.2.2.3950. Alternative power supply option shall be provided to avoid a station blackout. An alternative power supply option shall be provided to avoid a station blackout. The alternative power source shall be independent and physically separated from safety power supply and its activation time shall be consistent with the mission time of the uninterrupted power supply.

3.2.2.4000.

3.2.2.4100. For the extension of the design basis, the accident management functions and the capabilities of the systems providing such functions shall be considered to ensure that the consequences of a DEC2 plant state can be appropriately mitigated according to criteria for large or early releases defined under Section 3.2.4.0900.

3.2.2.4110. It shall be demonstrated that during DEC1 plant state the radioactive releases are minimized to the reasonably achievable level. During DEC2 plant state the extent and duration of radioactive releases shall be limited to the reasonably achievable level in order that

a) appropriate time is available for implementing the protective measures necessary off the site,

b) long term contamination of large areas can be avoided.

3.2.2.4200. Characteristics of DEC1 and DEC2 plant states shall be used to derive such limiting conditions and requirements, for which the systems, structures and components meant to controlling the events resulting in DEC plant states shall be designed.

3.2.2.4300. Implementation of specific design solutions or preventive accident management capabilities shall ensure that the occurrence frequency of the following accidents with catastrophic energy release in the reactor vessel or within the containment is infinitesimal:

a) reactivity accidents with prompt criticality, including heterogeneous boric acid dilution,

b) steam explosion, and

c) hydrogen detonation.

3.2.2.4310. In order to minimise uncertainties and to increase the robustness of the nuclear power plant unit, during the demonstration of practical elimination,

demonstration based on physical impossibility shall be preferred to demonstration on a probabilistic basis.

3.2.2.4400. During the design the accident management functions and the accident management systems for pressure reduction and hydrogen removal shall be determined to such extent that high pressure processes leading to fuel melting and early containment damages can be avoided.

3.2.2.4500. The mitigating functions for consequences of DEC2 plant states and systems providing these functions shall be determined to such extent that in a severe accident the molten core can be retained and cooled down within the containment.

3.2.2.4600.

3.2.2.4610. The required means of accident management shall be designed and accident management guidelines shall be devised for the efficient mitigation of the consequences of beyond design basis events analysed in detail, including severe accident processes resulting in a complete fuel meltdown, in such a way that any hazard posed to the environment and the population remains below a predefined, manageable level if the procedures and means of accident management work successfully.

3.2.2.4620. The special design requirements set for safety systems shall be applied to the means of accident management only to the extent reasonably achievable. The means of accident management shall not adversely affect the fulfilment of the design basis safety functions.

Principles of design for safety

3.2.2.4700. During the design of the nuclear power plant unit the initiating events resulting in DBC2 to 4 shall be identified. Conservative methods shall be used to define the effects of these events on nuclear safety related systems, structures and components. The initiating events shall be categorized into representative groups. The design requirements, the effects to be considered, and the events and the threshold values can be also determined by grouping, using an enveloping principle.

3.2.2.4800. During the management of the processes following initiating events such solution shall be applied in the order defined below, which ensures to a reasonable extent that:

a) the initiating event cannot have a significant effect on safety, or the change resulting from an event increase safety due to the inherent safety characteristics of the systems;

b) after the initiating event, the nuclear power plant remains safe due to the passive safety features or systems that continuously operate in the condition of the initiating event;

c) following the initiating event, the nuclear power plant returns to a safe shutdown condition by the operation of those safety systems that are meant to control the event; and

d) following the initiating event, the nuclear power plant returns to a safe shutdown condition through the implementation of special procedures.

3.2.2.4900. Should immediate intervention be required after an initiating event, it shall be ensured that the intervention automatically takes place to prevent more severe consequences. Operator intervention shall only be applied if it is justified by safety analyses that the interval between the detection of the event and the necessary intervention is sufficiently long. For operator interventions to control the initiating event the appropriate administrative, operational, emergency operating and accident management procedures shall be provided.

3.2.2.5000. The failures of systems, structures and components designed for normal operation purposes shall not hinder the provision of safety functions.

3.2.2.5100. Failure following an initiating event resulting in DBC2 to 4 shall not cause the loss of a safety function required to control the initiating event. Other failures following the initiating event shall be taken into account as part of the initiating event.

3.2.2.5200. During design the possibility and consequences of unintentional operation of system components and possible failures shall be considered.

3.2.2.5300. It shall be ensured with appropriate design that all physical barriers perform their functions during DBC1 and 2 operating conditions.

3.2.2.5400. With appropriate design it shall be ensured that in the case of any event resulting in DBC4, at least one of the physical barriers performs its function by preventing the release of radioactive materials from fuel elements.

3.2.2.5500. During the design the operator interventions, external services necessary for safe operations, external power supply, and ultimate heat sink autonomy requirements shall be defined. It shall be demonstrated that the resources supporting the safety functions are available with high reliability at the site, until their external replacement can not be ensured.

3.2.2.5600.

3.2.2.5700. Systems categorised into nuclear safety categories shall be designed that if scheduled preventive maintenance or testing of these systems is required during normal operations, then the nuclear power plant unit need not be shut down.

3.2.2.5800. During design simplicity and clarity shall be promoted. The use of passive design solutions is preferable to active solutions.

3.2.3. Demonstration of safety

Basic requirements

3.2.3.0010. Safety analyses shall demonstrate that the defence-in-depth concept is considered in the design of the plant.

3.2.3.0100. The design and analysis tools, models and model parts used for the justification of the fulfilment of general safety requirements of the design basis, as well as the input data shall be verified and validated. The validation of analysis tools shall be submitted by using the appropriate internationally available data – experimental results. The verification of the analysis models shall also be performed by a person or workgroup independent of the person or workgroup performing the analysis or design.

3.2.3.0200.

3.2.3.0300. The applicability of the methods applied and data used for the definition of the design basis or the analysis of the considered events shall be validated by using physical parameters, experiments or other methods. To compensate the remaining uncertainties, to a reasonable extent justified by safety analysis, conservative assumptions shall be used first of all by selecting conservative initial and boundary conditions.

3.2.3.0400. Sensitivity studies shall be performed to evaluate the uncertainty of assumptions, applied data and calculation methods. Where the results of the analysis prove to be sensitive to the assumptions of the model, further calculations are required by using methods and procedures independent of the previously used methods and procedures.

3.2.3.0500. The analyses justifying safety shall be documented in a way and to such extent that during the whole lifetime of the nuclear power plant these analyses may be repeated, independently reviewed, and modified to an extent necessary for modifications. Furthermore, the ratio of the applied conservatisms and the ratio of the margins available based on the analysis may be reviewed and re-evaluated.

3.2.3.0600. During the whole lifetime of the nuclear power plant the suitability of all interventions or modifications of nuclear safety related systems, structures and components that deviate from the authorized conditions shall be demonstrated with

deterministic safety analysis or a combination of deterministic and probabilistic safety analyses.

3.2.3.0700. The design basis, the extended design basis and their substantiation shall be periodically reviewed at the completion of the design, as well as during the whole lifetime of the nuclear power plant, when significant new safety information is received and based on the results of deterministic and probabilistic calculations or engineering judgement, modifications shall be implemented if necessary. The identified defects and possible safety improvements shall be evaluated and the necessary actions shall be taken in time.

3.2.3.0710. During the review, the following shall be taken into account:

a) changes affecting the nuclear power plant unit or its operation in the design or implementation phase and during its operation;

b) any new technical and scientific knowledge about the behaviour of the nuclear power plant unit and possible defects, which significantly influence safety;

c) a change in any properties of materials due to ageing or other effects, which has not been taken into account previously;

d) the international development of safety standards; and

e) the arising of significant, new safety information.

Deterministic safety analysis

3.2.3.0800. For all events included in the design basis or in the extension of the design basis the fulfilment of relevant acceptance criteria shall be verified by deterministic safety analyses.

3.2.3.0900. During the analysis of events resulting in DBC2-4, only the systems providing safety functions shall be considered. The performance of these systems shall be estimated as the least favourable regarding the analysed system. Systems, structures or system components that affect the series of events and have no safety function shall only be considered if they amplify the effect of the initiating event.

3.2.3.1000. In the analyses of events resulting in DBC2 to 4 human error or the single failure of a safety system that most significantly defines the outcome of the specific event and results in the most severe consequences shall be assumed. However there is no need to assume the failure of a passive design solution if it can be justified that its probability is very low or that it is not influenced by the initiating event.

3.2.3.1010. In the DBC2-4 analyses, besides the initiating events resulting the plant state, the stuck of the most effective control rod shall be assumed as an aggravating circumstance.

3.2.3.1100. The initiating events resulting in DBC2 operating conditions shall also be analysed with the scenario that systems performing the shutdown function required during the operating condition are lost. During the evaluation of a scenario the criteria for the combined initiating event shall be used.

3.2.3.1200. For stresses and pressure tests in DBC1 operating conditions, for initiating events resulting in DBC2 to 4, as well as for any heat stresses due to pressure developing during event chains with frequency over 10^{-5} 1/year the fulfilment of acceptance criteria for the integrity of the reactor vessel shall be evaluated.

3.2.3.1300. In the analyses of events resulting in DBC2 to 4 the operator interventions shall only be considered based on conservatively defined time requirement. In case of operator intervention within the 30 minutes timeframe the analysis defining the uncertainties shall confirm that the possible operator interventions can be performed in the available time.

3.2.3.1400. In the analyses of events resulting in DEC1 and DEC2 plant states the method of best estimate shall be used. The inoperability of any system, structure or system component shall be presumed if the failure of the system, structure or system component is very likely, as a result of the initiating event or the course of the accident.

Probabilistic safety analysis

3.2.3.1500. To define the exact risk of the nuclear power plant, to verify the fulfilment of relevant acceptance criteria, to evaluate the consistency and coherence of the design as well as to determine the suitability of the extended design basis a probabilistic safety analysis shall be performed. Probabilistic safety analyses shall be used to demonstrate that due margins are available to avoid cliff-edge effects.

3.2.3.1600. For the design of a nuclear power plant unit, including the systems for storage and manage spent fuel, level 1 and level 2 probabilistic safety analysis shall be developed, which considers all possible operating conditions, system configurations and all of the postulated initiating events for which it cannot be demonstrated by any other method that their contribution to the risk is insignificant. In the level 1 and 2 probabilistic safety analyses, considering the state-of-the-art results of science and technology, the external hazards shall be taken into account. Where it is not possible, proven alternative analysis solutions shall be used to assess

the contribution of the external hazard factors to the overall risk represented by the nuclear power plant.

3.2.3.1700. In the probabilistic safety analysis important functional, territorial dependencies, dependencies of physical situation of system components, dependencies from operation, maintenance and other common cause failures, especially missiles, effects of liquid and steam jets, internal fire and floods, as well as the accidents of nearby industrial facilities and the effects of human activities shall be considered.

3.2.3.1800. Within Level 1 and 2 probabilistic safety analyses the uncertainty and sensitivity evaluations shall also be performed, and their results shall be taken into account in all applications.

3.2.3.1900. The probabilistic safety analysis shall realistically model the performance of the nuclear power plant, for which the relevant design data, operational and accident-related instructions, accident management guidelines or drafts shall be considered, including human interventions and potential human errors. The appropriateness of the operating times assumed in the probabilistic safety analyses shall be demonstrated.

3.2.3.2000. Human reliability analyses shall be performed, considering those aspects that may influence the activities and performance of operating personnel in the different operating conditions of the nuclear power plant unit.

3.2.3.2100. In analyses regarding the definition of success criteria for systems and human interventions the best estimate method shall be used. Where the best estimate method cannot be used, the distortion effect resulting from the conservatism of the assumptions shall be evaluated.

3.2.3.2200. For the calculations reliable, credible, primarily facility, secondarily facility-type, type-specific reliability data shall be used. The source of data and the volume of sample shall be documented. Should the source data change, the differences between the design data and the operating conditions shall be considered and evaluated. Where no useful statistical data is available substantiated estimates shall be used.

3.2.3.2300. The probabilistic safety analyses shall be prepared according to the designed, afterwards the actual maintenance, testing and inspection practice of the systems, structures and system components. The fulfilment of requirements regarding probabilistic safety analysis results shall be demonstrated by taking into consideration the effect of maintenance, tests and inspections on system, structure and system component reliability.

3.2.3.2400. The probabilistic safety analysis shall be prepared, documented and maintained by using the available international experience and validated methods, and in accordance with the quality assurance system of the licensee.

Final Safety Analysis Report

3.2.3.2500. Safety Report is required to substantiate the regulatory licensing procedures prior to the construction, commissioning, and operation of a nuclear power plant unit. In the Safety Report, information regarding compliance with the requirements for the implementation, commissioning and operation of the nuclear power plant unit shall be put into an integrated system.

3.2.3.2600. The Final Safety Analysis Report shall be prepared based on the following formal requirements:

1. applicable legislations, regulations and standards, and demonstration of compliance with them,

2. general design principles for the nuclear power plant unit and methods applied to satisfy the fundamental safety objectives,

3. primary elements of the design documentation, introducing the site, the composition and normal operation of the nuclear power plant, the design basis, and the analyses demonstrating the fulfilment of the required safety level,

4. determination of the site boundaries by EOV coordinates, the defining characteristics of the site regarding safety,

5. the safety functions, the systems, structures and components providing aforementioned functions, the principles for safety classifications, the design basis for systems, structures and components, and their operation under every operating condition,

6. safety analyses to demonstrate the fulfilment of safety criteria and release limits for radioactive materials in case of DBC1-4 and DEC1-2 to evaluate the safety of the nuclear power plant, as well as, in the case of DBC1-4, the demonstration of the fact that appropriate safety margins are available,

7. measurement and instrumentation systems performing safety functions, active electronic protection systems, support and registration systems for operating personnel,

8. safety aspects of the operating organisation and management system of the nuclear power plant,

9. the commissioning programme of the nuclear power plant and the considerations for the programme, the presentation that the commissioning plan can

sufficiently demonstrate that the nuclear power plant unit will operate according to the plans and safety regulations,

10. accident prevention procedures and accident management guidelines, inspection procedures, training requirements and training for personnel, procedure for the feedback of operating experience and the relevant research results, and a comprehensive ageing management programme,

11. maintenance, testing and monitoring programmes, and the considerations upon what they are based,

12. the technical substantiation of operational limits and conditions,

13. radiation protection policy, radiation protection strategy, radiation protection methods and regulation,

14. the design basis and suitability of on-site nuclear emergency preparedness and response, cooperation and coordination with off-site organisations that play a role in nuclear emergency response,

15 on-site management system for radioactive waste,

16. aspects of final shutdown and decommissioning considered for design and operations,

17. analyses according to Section 3.2.2.3700 and Section 3.2.3.2610,

18. in the case of a multiunit nuclear power plant, or nuclear facilities located near each other, the possible technical, organisational and administrative interactions between the units and facilities, and

19. description of the organisational relations affecting nuclear safety of the nuclear power plant, human factors, structure of the management system and evaluation of the safety culture, and

20. determination of the necessary and sufficient personnel in DBC1-4 and DEC1-2.

3.2.3.2610. In the descriptions, analyses and findings included in the Final Safety Analysis Report, the site as a whole shall also be examined in order to take into account hazard factors that:

a) may affect all facilities within a short period of time, or

b) may arise from harmful interactions between facilities.

3.2.3.2620. In the case of a site with a multiunit nuclear power plant or if there is another operating nuclear facility in the vicinity and the facilities share human or other resources, it shall be demonstrated that the expected safety functions are still fulfilled in the case of all units and facilities.

3.2.3.2700. The licensee shall have all documentations available that are not publicly accessible and have been referenced or considered in the Final Safety Analysis Report.

3.2.4. Acceptance criteria for safety analyses

3.2.4.0100. For the processes originating from initiating events resulting in DBC2-4 it shall be demonstrated that the dose determined for 1 person of the reference group of the population is not exceeded:

a) for processes originating from initiating events resulting in DBC2 the value of public dose constraint, and

b) for processes originating from initiating events resulting in DBC4, 5 mSv/event.

3.2.4.0200. Initiating events resulting in DBC2 operating conditions shall not cause doses exceeding 1 mSv/event/person outside the controlled area of the nuclear power plant, in operational areas authorized for human staying.

3.2.4.0300. Initiating events resulting in DBC4 shall not cause a dose exceeding 10 mSv effective dose or 100 mGy dose for the thyroid outside the controlled area of the nuclear power plant and in operational areas authorized for human presence.

3.2.4.0400. In case of initiating events resulting in DBC2 operating conditions the radioactive contamination in the controlled area shall be of such type and rate, which can be managed and eliminated by the use of operational methods, systems, structures and components.

3.2.4.0500. Initiating events resulting in DBC2 to 4, with the assumption of single failure and no other independent failures, shall not induce such a consequence that violates the safety criteria for the specific operating condition.

3.2.4.0600. With consideration to all designed operating conditions and postulated initiating events, excluding sabotage, the frequency of core damage shall not exceed 10^{-4}/year.

3.2.4.0700.

3.2.4.0800.

3.2.4.0900. For all initial operating conditions and effects, excluding sabotage and earthquake, the collective frequency of severe accident event sequences resulting in large or early large releases shall not exceed 10^{-5}/year, but with every reasonable modification and intervention 10^{-6}/year shall be targeted. The fulfilment of criteria shall be demonstrated by Level 2 probabilistic safety analyses.

3.2.4.1000. The design shall confirm by deterministic safety analyses that the initiating events resulting in DBC2 operating conditions will not lead to the loss of function of any barrier even with the assumption of a single failure.

3.2.4.1100. The integrity of the reactor pressure vessel against brittle fracture shall be maintained by ensuring that real actual transition temperature is less than the maximum critical transition temperature determined by appropriate analysis of the initiating events resulting in DBC2-4.

3.2.4.1200. Following initiating events resulting in DBC2 to 4 the control and safety instrumentations controlling reactivity, the nuclear fuel assemblies, as well as the structural elements of the nuclear reactor shall not be damaged or deformed to such extent that the movement of control and safety instruments to terminate the fission chain reaction becomes impossible.

3.2.4.1300. Following initiating events resulting in DBC2 to 4 the nuclear fuel assemblies, the primary circuit of the nuclear reactor, and the connecting systems shall remain in such a condition that the short- and long-term cooling and management of the irradiated nuclear fuel can be ensured, furthermore the systems necessary for heat removal shall be able to perform their function both on short- and long-term.

3.2.4.1400. For events resulting in DBC2 the criteria ensuring the integrity of the fuel rods shall be defined during design by defining limits for the temperature of the nuclear fuel, the critical heat flux and the temperature of the cladding. For DBC4 design basis accidents to fulfil criteria for long-term cooling and management the acceptable maximum degree and type of fuel damage shall be determined.

3.2.4.1500. To perform a safety function, criteria for maximum pressure, maximum and minimum temperatures, thermal and pressure transients, degradation and stresses depending on the temperature range shall be defined for systems, structures and system components confining radioactive releases or performing retaining physical barrier functions during their whole lifetime.

3.2.4.1510. Recommendations for the fracture mechanical analysis of pressure equipment, the reactor pressure vessel and the containment and for taking into account the ageing processes are set forth in guidelines.

3.2.4.1600. To fulfil nuclear safety requirements criteria shall be defined for the temperature, pressure and leakage rate of the containment throughout its lifetime.

3.2.5. Operational limits and conditions

3.2.5.0100. During the design process the limits and conditions for the systems, structures and components shall be defined that ensure that the nuclear power plant

can be operated in accordance with the design objectives documented in the Final Safety Analysis Report and in conformance to the nuclear safety requirements.

3.2.5.0200. The operational limits and conditions shall be so defined that by adhering to them the situations leading to DBC4 can be prevented; in case of possible accidents the consequences can be mitigated. When defining safety limitations conservative approach shall be used to account for the uncertainties of the safety analyses.

3.2.5.0300. Each operational limit and condition shall be defined based on design considerations and safety analyses of the nuclear power plant, and the results of the commissioning tests.

3.2.5.0400. When defining the operational limits and conditions the following subsequent safety levels shall be considered:

a) safety limits,

b) threshold values for startup of systems providing safety functions, also

c) limits and conditions for normal operations.

3.2.5.0500. The operational limits and conditions shall cover all operating conditions, including power operation, shut-down and refuelling conditions, as well as the transition conditions between the previously listed conditions, furthermore the temporary situations during maintenance, tests and surveillance of system components.

3.2.5.0600. To guarantee safety margin shall be kept between the safety limits and the parameters of systems providing safety functions for which the values are defined in the Operational Limits and Conditions document– by appropriate conservative approach or consideration for the uncertainties of the safety analyses.

3.2.5.0700. The Operational Limits and Conditions document shall contain the limits for operational parameters, and regarding systems important to nuclear safety the minimum required number of operable system components that need to be in operational or standby condition in the various DBC1 operating conditions. It shall also contain the interventions required by the operating personnel and the allotted time for the intervention for cases when there is a deviation from the operational limits and conditions.

3.2.5.0800. The maximum allowable length of time for the inoperability of systems, structures and components important to nuclear safety as well as the cycle times for in-service tests and inspections of these systems, structures and components shall be based on analysis results. When determining cycle times, the balance between the

risk of inoperability due to maintenance and tests and the increased reliability due to these activities shall be taken into account.

3.2.5.0900. As part of the Operational Limits and Conditions document and the requirements regarding necessary and sufficient personnel for safe operations shall be determined.

3.2.5.1000. Prior to commissioning of the nuclear power plant, the preliminary version of the Operational Limits and Conditions document shall be developed, its content shall ensure that the systems, structures and components operate according to the design assumptions and objectives of the Safety Analysis Report.

3.2.5.1100. The preliminary version of the Operational Limits and Conditions document shall be reviewed based on the experience gained during the commissioning and shall be modified and finalized in accord with the Safety Analysis Report.

3.2.5.1200. Regulations regarding the modification of the Operational Limits and Conditions document or the temporary deviation from its provisions shall be defined in an internal procedure. The adequacy and acceptability of deviations shall be demonstrated in every instance by deterministic safety analysis or a combination of deterministic and probabilistic safety analyses.

3.3. SPECIAL DESIGN REQUIREMENTS

3.3.1. Design of safety class systems

3.3.1.0100. During the design of safety class systems, structures and system components to fulfil the required design criteria primarily redundancy, diversity, physical separation, and separation of electrical power supply, functional separation and independence, as well as – if required – independent data link and failure-proof design principles shall be applied. These systems shall be designed by using reliable, qualified system components, and by developing independent auxiliary systems, if needed.

3.3.1.0200. During the design of safety class systems, structures and system components to a reasonably achievable degree passive, inherently safe solutions shall be applied, which ensure that failure of systems, structures and system components – even without external interventions – lead to safe conditions.

3.3.1.0300. The failure of a system, structure or system component important to nuclear safety shall not cause the failure of a system, structure or system component classified to a higher safety level.

3.3.1.0400.

3.3.1.0500. The systems, structures and components shall be designed to external effects of natural origin to a frequency of 10^{-4}/year, in case the system component may have a safety function in the given situation.

3.3.1.0600. The safety systems, structures, components, and their auxiliary systems shall be protected as much as possible from the effects of internal and external hazard factors, and from the interaction between the failed systems, structure and system components.

3.3.1.0610. Potentially harmful interaction of the simultaneously operating systems shall be assessed and avoided as appropriate. During the assessment consideration shall be taken to physical connections and the effect of intentional or inadvertent operation on the environmental conditions and the effect of the changed environmental conditions to the other component.

3.3.1.0700. The possibility of common cause failure shall be considered during the definition of where and how the principles of redundancy, diversity, physical separation, and functional separation shall be applied to provide the required function and reliability.

3.3.1.0800. During design the requirement of single failure shall be applied. The possibility of inadvertent operation of a system component shall be considered a possible mode of failure. The failure of a passive design solution shall be considered, unless it can be demonstrated that it is highly unlikely or does not influence the given function.

3.3.1.0900. Systems included in Safety Class 2, except for systems performing a barrier function, shall have a stand-alone emergency power supply for each redundant branch, and the planned redundancy and independence shall be at least such that:

a) a single defect occurring in the system cannot cause the loss of the protection function, and

b) the removal of any individual system component from operation should not cause the loss of the minimum redundancy assumed in the analyses.

3.3.1.1000. It shall be ensured that the operability of systems in Safety Classes 1 and 2 can be inspected during operations.

3.3.1.1100. The actuation and operation of systems included in Safety Class 2 shall be ensured with either automated systems or passive systems, that within 30 minutes following an initiating event resulting in DBC2-4 no operator intervention is needed. If operator intervention is designed to provide a function within 30 minutes after an initiating event it shall be demonstrated that the operator intervention

cannot be replaced by automatic operation or the use of passive systems, also it shall be demonstrated that the designed intervention can be performed by an operator.

3.3.1.1200. If the probabilistic safety objectives can only be ensured by using systems of extreme high reliability, then these functions shall be provided diversely.

3.3.1.1300. The appropriate design of the system executing the automatic shutdown of the nuclear reactor and controlling the systems providing active safety functions shall ensure that in case of events resulting in DBC1 or DBC2 to 4 the operating personnel cannot prevent the automatic safety actuation from their operating control positions, while being able to perform the necessary interventions.

3.3.1.1400. Programmed systems performing safety functions, beyond the general requirements for programmed systems, shall fulfil the following requirements:

a) such hardware and software tools shall be used that have references fulfilling the strictest quality assurance requirements,

b) the complete development process, including the review, testing and implementation of the design modifications - shall be systematically documented and evaluated,

c) to validate the reliability of computer-based systems, the systems shall be reviewed by experts independent of the designer and the supplier, furthermore

d) if the necessary reliability level of a system cannot be justified, the relevant safety functions shall also be ensured by diverse means.

3.3.1.1500. Appropriate margins shall be kept between the values of safety limits and the settings of the systems providing safety functions.

3.3.1.1600. During the design, production and maintenance of systems, structures and system components with a safety classification it shall be ensured that their quality and the reliability of safety functions provided by these systems, structures and system components is appropriate to their safety class.

3.3.1.1700. For each safety class the following shall be defined:

a) the appropriate requirements and standards to be applied during design, production, assembling and inspection,

b) the requirement of power supply from a backup energy source,

c) the assumption of availability or unavailability of systems important to nuclear safety in deterministic safety analyses,

d) quality requirements, and

e) requirements for environmental resistance qualification.

3.3.1.1800. Commercial products shall not be applied in safety class 1. Exceptions are the special purpose components, such as pipelines and valves to be installed at deaerator, drain, measurement intake locations.

3.3.2. Design for lifetime

Design lifetime

3.3.2.0100. The design lifetime of the nuclear power plant shall be defined, and the lifetime of which system component performing a safety or physical barrier function defines or limits this design lifetime.

3.3.2.0200. By analysing the degradation processes that limit the design service lifetime it shall be demonstrated that the lifetime of non-replaceable system components and those system components not intended to be replaced that perform passive safety or physical barrier function is at least as long as the design lifetime of the whole nuclear power plant, also taking into account the loads and ageing processes with the required margins during the whole lifetime.

3.3.2.0300. It shall be defined that during the design lifetime under what conditions can the nuclear safety requirements be fulfilled.

3.3.2.0400. If the lifetime of a system, structure or component is shorter than the designed lifetime of the nuclear power plant the refurbishment or replacement of that system, structure or component shall be ensured.

3.3.2.0500. In case of systems, structures and components that provide functions until or during the decommissioning phase the time for decommissioning shall also be included in the design lifetime of these systems, structures and components.

Requirements regarding structural materials

3.3.2.0600. In the design of systems, structures and components important to nuclear safety such structural materials shall be used:

a) which have been tested, qualified for environmental resistance, and fulfil the design and environmental requirements,

b) the quality classification and characteristics of which are within the threshold values set in the specifications or standards used during the design,

c) in the case of systems, structures and system components exposed to neutron radiation,

ca) their materials are the least susceptible to activation, and in case of becoming activated, the activated parts remain in place, and

cb) their stress corrosion resistance does not deteriorate even as a result of radiation,

d) if the system components are included in Safety Class 1 and are exposed to neutron radiation, the change in their material properties is the least possible and can be monitored throughout their lifetime,

e) the degradation processes of which are known in the given media and circumstances, the degradation does not hinder the function during the design lifetime,

f) for which such surface can be manufactured, which can be the most decontaminated during operation and decommissioning, furthermore

g) which are fire-resistant or their flammability can be appropriately limited.

3.3.2.0610. When pressure equipment and pipelines are to be designed, special care shall be taken for the design specifications of welding applied during manufacture and assembly as a special process (which can be corrected to a limited extent), in particular, for the following:

a) applicable welding methods,

b) weld type,

c) specification of added metals used for welding corresponding to the raw materials used,

d) specification of the scope of weld testing methods, and

e) specification of the quality assurance conditions of welding:

ea) requirements set for manufacturers and installers,

eb) requirements set for welders and material testers, and

ec) requirements set for the quality certification documentation of welding.

3.3.2.0700. During design, it shall be demonstrated by analysing the degradation processes limiting the lifetime that

a) the strength properties of materials even with the ageing effects can withstand the maximum stresses calculated for DBC1-4 while considering the safety margins for the operating conditions if the system component concerned perform safety functions in the given operating condition; and

b) in critical structures the fracture mechanics requirements are also fulfilled.

3.3.2.0800. During design the criteria for catastrophic failure shall be fulfilled when selecting materials. All typical fracture mechanisms shall be analysed for the relevant system components.

3.3.2.0900. During design when selecting structural materials according to material and product standards the inspections, material testing and certification requirements shall be defined.

3.3.2.1000. In case of new materials and manufacturing methods a qualification process is required, which verifies the suitability for the purpose and fulfilment of the requirements.

3.3.2.1100. It shall be ensured that the physical-chemical properties of the materials used in the containment prevent significant hydrogen production during events resulting in DBC2 to 4.

3.3.2.1200. During design the following requirements shall be fulfilled regarding structural materials:

a) in case of austenitic casts to be welded the content of delta-ferrite shall be limited and checked,

b) in case of austenitic casts that are hard to inspect the resistance against thermal ageing shall be analysed,

c) the use of copper alloys is prohibited for system components in contact with the media of feedwater, main steam- and the condensate systems,

d) in steam systems and high water flow-rate systems materials resistant to erosion corrosion shall be used, furthermore

e) in case of carbon-steel system elements being in contact with water the wall thickness tolerance determined in strength analyses shall be applied for general corrosion processes.

3.3.2.1300. During design when selecting materials the following aspects of decommissioning shall be considered:

a) long term storage at the nuclear power plant defined in the decommissioning strategy,

b) resistance against the chemical substances used in the nuclear power plant,

c) material of the decontaminable surfaces and the system of cleaning and decontamination chemicals and technology shall be so selected that the desired cleanliness and radiation conditions to manage it, can be preserved until the end of the service life of the system furthermore

d) in case of materials activated during operations – in accordance with the schedule of decommissioning – the shortest possible half-life.

Chemistry

3.3.2.1400. For the nuclear power plant unit the water control of the primary and secondary circuit systems, as well as the auxiliary and service systems shall be designed in such a way that:

a) the chemical composition and conditioning of the applied process media and auxiliary materials shall be consistent with the structural materials and construction;

b) corrosion effects shall remain below the designed values and shall guarantee the integrity of the system components;

c) the amount of radioactive materials in the media shall at all times be at the lowest reasonably achievable level; and

d) it shall be able to remove gases dissolved in the primary circuit in DBC1 operating conditions.

3.3.2.1500. The suitability of the cooling and work media shall be verified with calculations and analysis while considering the design lifetime of the nuclear power plant.

3.3.2.1600. A sampling system shall be designed to monitor the water parameters of safety importance, the changes in unfavourable water chemistry and corrosion processes, the accumulation of corrosion materials and their activity, furthermore if a fuel cladding becomes inhermetic it can be timely detected. The design shall ensure that the sampling system provides representative sample and reaction-free regarding safety.

3.3.2.1700. For each system the removal process of corrosion products, radioactive contamination and other contamination shall be designed, appropriate methods shall be defined and tools shall be designed.

3.3.2.1800. The concentrations of chemicals used for controlling water systems, the parameters influencing the corrosion of the water systems, and the level of contaminants and corrosion products shall so be determined, that they have the least adverse effect on the applied structural materials in all operating conditions of the nuclear power plant unit at specific temperature, pressure and flow conditions.

3.3.2.1900. During the design of water systems, the effect of corrosion parameters and products on structural materials and physical processes (e.g. heat transfer) shall be analysed. Concentration limits shall be defined for corrosion products and the acceptable amount of deposits shall be determined in systems, structures and

system components important to nuclear safety that do not endanger safe operation. Appropriate measures, methods and procedures shall be defined to prevent exceedance of the limits and to retrieve the normal values of the limits are exceeded.

3.3.2.2000. When controlling the concentration of chemicals correcting the pH-effect of concentration changes of the neutron absorbent, reactivity control material and for parameters influencing corrosion the effects of radiolysis shall be considered.

3.3.2.2100. Water purification systems shall ensure that the amount and concentration of radioactive materials released into the environment shall remain below the limits and at the lowest reasonably achievable level for every operating condition. The amount and activity of radioactive waste produced during cleaning processes shall remain at the lowest reasonably achievable level.

3.3.2.2200. The capacity of water purification systems shall guarantee that the amount of corrosion products in the systems are at a level approved in the design and appropriately low.

3.3.2.2300. Such cleaning technology shall be applied that ensure that the passive protective layer on the surface of the affected structural materials remains or regenerates.

Environmental qualification of equipment

3.3.2.2400. During design for DBC the environmental conditions and effects due to external and internal hazard factors shall be determined under which the systems, structures and system components shall perform their safety and physical barrier functions. In the extent defined in the design the environmental effects for extended design basis conditions shall also be defined.

3.3.2.2500. Qualification processes shall verify that the systems, structures and system components important to nuclear safety are able to perform their functions during the lifetime of the nuclear power plant under the environmental conditions occurring during events resulting in DBC1 to 4 if their operation is required under these conditions.

3.3.2.2600. The environmental resistance of passive metallic and concrete system components shall be ensured by design. If required the environmental resistance shall be verified by analyses.

3.3.2.2700. The suitability of non-metallic, non-concrete system components and active system components shall be verified with individual or type qualification.

3.3.2.2800. During the design of a system component and its first qualification, the in-service ageing mechanisms shall be considered and it shall be verified that the

system components are able to reliably perform their functions even at the end of their designed lifetime.

3.3.2.2900. In the designs of the system components the method and conditions of maintaining qualified state shall be defined.

3.3.2.3000. Qualification for flooding and fire is required if they may occur at the installation place of the system component and these events shall not be ruled out if single failure criteria is applied to verify performance of safety functions.

3.3.2.3100. It shall be evaluated whether electromagnetic effects endanger the performance of any safety function. It shall be ensured that the safety functions are not influenced by such effects.

3.3.2.3200. If a system component has a function in DBC4 or DEC plant states , then it shall be qualified for the loads caused by the given operating condition.

3.3.2.3300. During the qualification of systems, structures and system components that perform accident management or mitigate its consequences , their operability for the required period of time shall be demonstrated for the conditions and loads assumed in DEC1-2 plant states.

Maintenance, review and inspection

3.3.2.3400. For all systems, structures and components important to nuclear safety the programme of in-service inspections, reviews and material testing programs, and the mode and frequency of testing of structural integrity, leaktightness and functional tests, and the designer requirements for planned preventive maintenance and other maintenance strategies shall be determined.

3.3.2.3500. Parameters to decide on operability and suitability shall be defined. For these parameters acceptance criteria shall be provided, the compliance with which shall be measured and monitored during inspections, tests. If deviations from the acceptance values are detected the required actions shall be defined, including the modification of maintenance programmes.

3.3.2.3600. If inspections cannot be performed due to limited access or covered structure, then either design solutions are required to compensate for the limited access or it shall be demonstrated that operations can be maintained for the design lifetime without inspections or surveillance.

3.3.2.3700. The cycle time of functional tests, the review frequency, the inspection and maintenance modes and conditions for systems, structures and components important to nuclear safety shall be defined and substantiated so that

a) it is consistent with the design principles and construction of the system, structure component,

b) it ensures that the safety function is reliably performed during the test, review, maintenance of the system, structure or component, furthermore

c) the removal of the system, structure or component from operation for test, review or maintenance can be tolerated from the nuclear safety point of view, and the frequency of test, review or maintenance shall not result in the decrease of nuclear safety.

3.3.2.3800. During design the requirements for the manufacturer and acceptance inspections of the system components shall be defined. The inspection methods during manufacturing shall conform to the in-service inspection methods in order to ensure comparability. Special requirements shall be defined for the manufacturer inspections of those system components for which in-service inspection cannot be performed during operations due to limited access or activation of system components.

Ageing management

3.3.2.3900. The ageing processes shall be identified, as well as their characteristics for all safety classified system components. The data and methods shall be provided to set up the system and ageing management programme to be performed during operations. The ageing management system of the designer shall be conform to the maintenance programmes, the qualification of tests, the qualification of system components for environmental resistance and the programmes maintaining the qualified state.

3.3.2.4000. During the design of systems, structures and components important to nuclear safety the anticipated ageing effects and their consequences shall be evaluated. It shall be verified that the ageing processes of structural materials, the uncertainties of the “0” condition and ageing processes considered, do not hinder the systems, structures and components to perform their functions during their design lifetime.

3.3.2.4100. During the design of systems, structures and components important to nuclear safety the change of properties of the selected structural materials due to ageing processes shall be evaluated. The allowed lifetime, integrated operation period and cycle times of usage for systems, structures and components shall be determined.

3.3.2.4200. During the design, clear operation indicators and criteria shall be defined for systems, structures and components important to nuclear safety in order to determine their ageing processes, operability conditions and remaining lifetime.

3.3.2.4300. For systems, structures and components important to nuclear safety ageing management provisions shall be defined. The provisions shall include:

a) the ageing locations and anticipated ageing processes at that locations for systems, structures and components important to nuclear safety,

b) the estimation of anticipated development of ageing processes,

c) maintenance, surveillance, testing and monitoring activities for managing ageing processes, furthermore

d) the definition of actions to mitigate ageing and deterioration processes, and their unfavourable effects.

3.3.2.4400. For those parts of pressure retaining equipment and pipelines in the primary circuit which are exposed to neutron radiation or other ageing processes, a surveillance programme shall be established and performed to monitor the ageing processes in the applied materials.

3.3.3. Design of pressure retaining equipment and pipeline

3.3.3.0100. During the design, the operating conditions and mechanical loads and load cycles, including the effects triggered by external and internal hazard factors, under which the given pressure equipment and pipeline may operate, shall be defined.

3.3.3.0200. The calculations substantiating the design and suitability of system components shall be performed in a unified way according to the standards and requirement system accepted in the nuclear industry in accordance with the safety classification of the systems, structures and system components. Calculations substantiating the design, verification analyses performed for each load, and the circumstances and assumptions during design shall be presented.

3.3.3.0300. The use of pressure retaining equipment and pipelines designed according to different standards and requirements shall be avoided. If the use of such equipment or pipeline is necessary, special analysis is needed to substantiate the fitting and assembly of the pressure retaining equipment or pipeline designed according to different requirement systems.

3.3.3.0400. The containment shall be designed as pressure retaining equipment, and the option of regular inspection of its pressure retaining capability shall be ensured.

3.3.3.0500. It shall be demonstrated that the toughness of materials of system components in Safety Classes 1 and 2, is in compliance with the load. No new crack shall occur in the material in DBC1-4. It shall be verified that the fractures already existing in the material are resistant to unstable propagation, thus it is ensured that the regular in-service inspections timely discover any defects.

3.3.3.0600. During the design of pressure retaining equipment and pipeline, the change of physical and mechanical material properties due to the effects of neutron flux shall be considered.

3.3.3.0700. During the design of pressure retaining equipment and pipeline it shall be ensured within the frame of applied standards, that

a) the number of joints are minimised, also

b) welded joints are used between the pipe elements, except where

ba) releasable joints are required due to operating conditions, or

bb) welding is prohibited, or

bc) it can be justified that the failure of the releasable joint does not result in the increase of uncontrolled leakage or loss of primary or secondary circuit coolant.

3.3.3.0800. Welds shall only be applied after special analysis in individual, substantiated cases in locations subjected to bending stress and where stress is concentrated. For welding of pressure retaining equipment and pipeline full penetration welds shall be used.

3.3.3.0900. During the design of systems, structures and system components important to nuclear safety mechanical and flow induced vibrations and the deterioration processes caused by them shall be considered. The systems, structures and system components shall be designed in a way that minimises vibrations. During commissioning it shall be demonstrated that the rate of vibrations does not exceed the acceptable rate of the design.

3.3.3.1000. The pressure retaining equipment and pipeline shall be provided to the extent defined by its safety function with controlling and measuring devices to control pressure, temperature, flow rate, level and chemical composition of operating media, and displacement and leaktightness.

3.3.3.1100. The number, position and type of valves installed in a system shall be defined to allow for:

a) setting of normal operation routes and parameters,

b) performance of safety functions,

c) performance of in-service inspection programmes and function tests, also

d) the exclusion of system components for maintenance and repair.

3.3.3.1200. The pressure retaining equipment and pipeline shall be fitted with pressure relief device if the pressure may exceed the acceptable level. Pressure relief devices shall be designed so that the amount of radioactive material released into the environment during their operation shall be the lowest reasonably achievable.

3.3.3.1300. If a system, structure or system component important to nuclear safety is connected to a system or system component which operates at a higher pressure level , than the system, structure or system component shall be designed to the pressure values of the latter one or by design solutions it shall be ensured that even in the case of a single failure the pressure of the system, structure or system component designed for lower pressures does not exceed the design values.

3.3.3.1400. The results of the strength analyses shall demonstrate that:

a) the lifetime of the tested equipment or pipeline is sufficiently long, taking into account the loads and ageing processes expected during its whole design lifetime;

b) the structural materials correspond to the maximum loads calculated in DBC1-4, taking into account ageing and the criteria set for the operating conditions; and

c) the value of the stress intensity factor does not exceed the fracture toughness associated with the resulting temperature anywhere in the structure, taking into account plastic deformation.

3.3.3.1500. The requirements and standards for the design of pressure equipment and pipelines shall be applied in accordance with the safety class of the given system, structure or system component.

3.3.3.1600. Strength analyses shall be carried out for demonstrating the conformity of all load-bearing components, pressure systems and system components categorized in safety classes. In the dimensioning of pressure systems and system components manufactured abroad, foreign calculation methods may be used if they are nuclear industrial standards or general industrial standards that may also be applied in nuclear areas. Strength calculations may be carried out only within one set of specifications.

3.3.3.1700. The data used in strength analyses shall come from a conservative approach, and shall be collected in accordance with the selected standards. The effects leading to the degradation of the structural materials shall be taken into account.

3.3.3.1800. Protection against brittle fracture shall be examined in the case of system components where necessary.

3.3.3.1900. It shall be shown by means of strength analyses that the load on the analysed system components remain below the acceptable load value in DBC1-4.

3.3.4. Design of buildings and building structures

3.3.4.0100. During the design of the buildings of the nuclear power plant, the general regulations with respect to architectural and technical design shall be applied while the nuclear safety requirements shall also be taken into consideration.

3.3.4.0200. It shall be ensured that the buildings and building structures of the nuclear power plant, in accordance with their safety classifications, bear the loads occurring in DBC1-4 and those occurring under DEC1, meaning the extension of the design basis, also withstand environmental effects in accordance with the compliance criteria specified for the given operating mode.

3.3.4.0300. Where possible, appropriate sampling and monitoring opportunities shall be established, in order that the compliance of the building structures is continuously controllable throughout their lifetime.

3.3.4.0400. The safety class buildings shall be designed for stress caused by safety earthquake, including the appropriate design of the foundation and the effects of geotechnical hazards caused by safety earthquake. The stress on these buildings characterised by safety class, which occurs during the course of an earthquake, shall be minimised through appropriate structural development. In the event of a safety earthquake, interactions with the neighbouring buildings shall be excluded.

3.3.4.0500. The design for earthquakes shall be performed on the basis of the accepted methodological provisions and standards with regard to the safety class buildings and building structures.

3.3.4.0600. The basis for the determination of the design input necessary for the earthquake resistance of the buildings and building structures is the design input response spectrum derived from the free surface response spectrum belonging to the safety earthquake. The effect of soil movement at the building foundation level shall be calculated from that.

3.3.4.0700. The appropriate load bearing capacity of the support structures of the buildings for loads caused by soil movements, corresponding with the safety earthquake shall be verified through dynamic analyses. The methodology used for dynamic analyses and the complexity of the modelling shall be in correspondence with the risk of the nuclear power plant, and with the safety class and function of the

building structure, and the purpose of usage of the expected calculation results within it.

3.3.4.0800. When modelling the soil-building interaction, the building impregnation, the depth, stratification and dynamic features of the considered soil and the uncertainty shall be managed.

3.3.4.0900. The monitoring of the load bearing capacity shall be performed in accordance with the accepted standards of the nuclear industry. The realisation of limits with regard to the movement and changes in shape deriving from the constructional development of the building structures shall be evaluated.

3.3.4.1000. The design of groundwork shall be performed in accordance with the relevant standards, taking into consideration the effects of the earthquake belonging to the design basis of the nuclear power plant.

3.3.5. Organisation

3.3.5.0100. During the arrangement of system components, the requirements of redundancy, diversity and independence shall be taken into account in order to avoid common cause failures.

3.3.5.0200. The arrangement shall ensure that the events in the design basis and the interactions of the individual buildings and systems cannot cause an unacceptable damage to the nuclear power plant.

3.3.5.0300. The redundant systems important to nuclear safety shall be designed with appropriate physical separation. This requirement shall be applied during modifications, taking into account the existing technical conditions.

3.3.5.0400. The transportation routes for vehicles within the nuclear power plant shall be so designed that the potential fall of the loads being lifted do not endanger the performance of the safety function of any other system, structure or component, or such vehicles shall be designed, with which it may be ensured that the dropping of the loads could result in DBC4 at most.

3.3.5.0500. The placement of systems, structures and system components shall be designed such that it provides the opportunity for the performance of inspection, maintenance, repair, replacement of spare parts and dismantling with minimisation of the doses. Opportunity shall be provided for monitoring through visual, non-destructive inspection, cleaning, washing and repair of the base material and the welded joints. This requirement shall be applied during modifications, taking into account the existing technical conditions.

3.3.5.0600. The routes approaching the workplaces and the escape routes shall be designed so that the operating personnel can move easily even in protective

equipment. Unobstructed routes of appropriate size and load bearing capacity shall be provided for the machine transportation of radioactive or contaminated objects. The rooms used for the storage of tools and instruments, and for preparation for work processes, shall be established at an appropriate distance from the significantly exposed locations while taking into account radiation protection considerations.

3.3.5.0700. The logistics background, services and instruments, including roads, water supply, fire water network and on-site communication instruments necessary for the safe operation of the nuclear power plant unit shall be designed and installed so that they are able to perform their functions both in DBC1 to 4 to the extent required for handling the operating conditions.

3.3.5.0800. The nuclear power plant unit shall be designed so that, if necessary, the operating personnel are able to enter the rooms of the containment whilst ensuring that the containment remains continuously closed.

3.3.5.0900. The buildings of the nuclear power plant shall be designed so that in the event of emergency, the rescue of persons remaining on site of the nuclear power plant can be conducted in a quick and safe manner.

3.3.5.1000. When arranging the cables of redundant systems providing safety functions, the principle of physical separation shall be applied. The electric and instrumentation cables shall be separated. This requirement shall be applied during modifications, taking into account the existing technical attributes.

3.3.5.1100. The redundant safety class systems, influencing the management of the effects of external and internal hazard factors shall be placed so that the effect cannot hinder the performance of safety functions of all redundant components simultaneously.

3.3.5.1200. In accordance with the fire protection plans, the work areas and corridors shall be provided with emergency lighting. The escape routes shall be clearly marked. The danger warning systems shall reach all members of the personnel, and the noise level and the design of protective devices shall be taken into account during design.

3.3.5.1300. In DEC1-2 plant statess, it is allowed to use interconnected support systems between the individual units if it can be demonstrated that it helps restore a given safety function during accident management. No interconnection may be allowed between units that would, in the case of any of the blocks, increase the probability or severity of consequences.

3.3.5.1400. All such components, the manual operation of which may be necessary to manage the given initiating event or during recovery, shall be placed in a way that

the intervention can be carried out under the expected environmental conditions, or alternative solutions shall be ensured.

3.3.6. Specific hazard factors

Earthquake

3.3.6.0100. The site-specific safety earthquake shall be characterised according to the mean seismic hazard curve, with the free surface response spectrum and corresponding acceleration-time function, taking into account the non-linear transfer of surface layers. Based on the response spectrum, which forms the standard design input during the course of design process, monitoring and qualification of the safety earthquake, shall be determined.

3.3.6.0110. The systems, structures and system components of the nuclear power plant shall be included in earthquake safety classes according to the safety functions they fulfil during a safety earthquake.

3.3.6.0120. The active and passive systems, structures and system components that are required for shutting down the nuclear reactor, keeping the nuclear reactor in a subcritical state, cooling or removing heat for a prolonged period and are essential for monitoring the critical parameters or ensuring that limits of radioactive releases applicable to design basis accident conditions can be met shall be included in Earthquake Safety Class 1 and 2, respectively.

3.3.6.0130. Buildings having a safety function or their building structures shall be included in Earthquake Safety Class 2.

3.3.6.0140. Systems, structures and system components that jeopardise the function of system components included in Classes 1 and 2 through their possible damage arising as a result of an earthquake and the effects triggered shall belong to Earthquake Safety Class 3. Considering the quantity of radioactive materials stored and the potential consequences of a failure, systems, structures and system components as a result of the failure of which significant radioactive releases may occur or damage to which would prevent the safe management of the nuclear power plant after an earthquake shall be included at least in Earthquake Safety Class 3.

3.3.6.0150. System components that do not belong to any of the three earthquake safety classes shall belong to Non-earthquake Safety Class 4.

3.3.6.0200. Regardless of the seismic conditions of the site, the peak ground acceleration value of the safety earthquake on the free surface shall not be less than 0.1g.

3.3.6.0300. The nuclear power plant shall be designed in such a way that the fundamental safety functions are also performed in the event of a safety earthquake,

and that the nuclear power plant can reach controlled, safe shutdown conditions following the earthquake even if a single failure of systems, structures and system components is assumed.

3.3.6.0400. The systems, structures and system components performing safety functions and participating in the implementation of earthquake protection shall be designed and qualified in such a way that they shall maintain their required operability and function in the event of a safety earthquake. The design and qualification shall be performed in accordance with the safety class and the nuclear standards and testing procedures.

3.3.6.0500. The design shall be performed according to the safety class, based on nuclear standards.

3.3.6.0600. The protection of systems, structures and system components participating in the implementation of earthquake protection shall be ensured against damage and interactions of system components having no safety or physical barrier functions, which occur as a result of a safety earthquake.

3.3.6.0700. It shall be provided that even in the event of a small excess of spectral and peak acceleration values of the safety earthquake the immediate loss of function of the systems, structures and system components is prevented.

3.3.6.0800. During the construction of systems, structures and components and the development of nodes and anchorages it shall be ensured that the structure possesses energy dissipating ability whilst operating in the flexible-ductile range.

3.3.6.0900. The rigid damage mode shall be excluded by the appropriate choice of material and construction solutions. The interaction and collision of neighbouring systems, structures and system components and the surrounding support structures shall be prevented.

3.3.6.1000. The loads combined with the loads generated by the safety earthquake shall be determined taking into consideration the functions of systems, structures and system components. During design for earthquakes, the loads arising in the operational, shutdown, maintenance, refuelling or DBC2 operating conditions of the nuclear power plant shall be combined with the loads generated by the safety earthquake. The compliance criteria may relate to stress, deformation, displacements and operability, as well as their combination in accordance with the nuclear standards regarding the given safety class. The concurrence of events resulting in DBC4 and the safety earthquake shall not be assumed as independent events. The secondary effects of the safety earthquake shall also be taken into account during the design.

3.3.6.1100. During the design of the systems, structures and components, the response spectrum and acceleration-time function characteristic for the point of erection shall be considered as authoritative, which shall be formed according to the norm taking into consideration the design input determined for site-specific safety earthquake, the dynamic response of the building and the soil-building interaction.

3.3.6.1200. The management of the effect of the earthquake shall not be dependent on the availability of external services, such as the electrical network connection, fire-fighting or logistic services.

3.3.6.1300. The nuclear power plant unit shall be designed and equipped with a seismic alarm system categorised into the Safety Class 2, based on the signal of which either automatic protective operations should be launched or the operator should take the necessary actions. The characteristics of the earthquake associated with the operations and actions shall be determined in both cases. If a system is established which triggers an automatic protective operation in the event of an earthquake, then its structure, redundancy, diversity, physical separation and reliability shall be in compliance with the requirements of that protective system.

3.3.6.1400. The nuclear power plant unit shall be designed and equipped with a seismic activity registering system classified into Safety Class 3. The processing of its signal allows the effects of the earthquake and the safety of further operation to be evaluated. The characteristics of the earthquake and the characteristics which are necessary for the evaluation of the condition of the nuclear power plant and form the basis for the evaluation of the continued safe operation shall be specified in the design.

3.3.6.1500. Special emergency operating and accident management procedures and actions shall be developed for the event of an earthquake. The organisation of the operation and service of the nuclear power plant, the condition assessment, the scope of inspections following an earthquake, their methods and the conditions of restart shall be regulated in the procedures and action plans.

3.3.6.1600. It shall be ensured that in the event of an operational basis earthquake having the same frequency as the operational events, the operations shall continue either undisturbed or if the nuclear power plant shuts down, it shall remain in a condition that can be restarted following the quake.

3.3.6.1700.

Special internal hazard factors

3.3.6.1800. As part of the inspection of the initiating events, the special internal hazard factors, such as flooding, fire, explosion, high energy pipe break shall be

identified, the occurrence of which may influence the performance of function of the safety or isolating barrier.

3.3.6.1900. The rooms exposed to internal hazard, and those potentially concerned systems, structures and system components with safety functions within these rooms shall be identified. The effect of the investigated events shall not hinder the performance of the safety functions.

3.3.6.2000. In the event of flooding it shall be ensured that the flooding media can be appropriately collected and safely diverted.

3.3.6.2005. A comprehensive strategy shall be prepared to manage the external hazard factors within the design basis, that ensures the compliance with the requirements determined in Section 3.2.1.0900.

Natural hazard factors

3.3.6.2010. In the case of events of natural origin existing in the long term, preparations shall be made for relieving the personnel required for taking measures and for replacing the necessary equipment.

3.3.6.2100. Regarding each type of hazard factor being characteristic of the site and associated with the natural phenomena and processes in the design basis, the design parameters forming the design input shall be specified on the basis of the hazard curve, taking into account the screening criterion applicable to the given hazard factor. The analysis shall be performed by deterministic methods, and based on the state-of-the-art results of science and technology by probabilistic methods. The analysis shall take into account all available, validated data and, if possible, connections shall be established between the severity of the hazard factors, especially the extent and duration. If it is possible, the maximum, but still justified severity of the hazard factors shall be determined. Design basis design parameters and key properties shall be so specified that they shall ensure the avoidance of the cliff edge effect from the side of design inputs.

3.3.6.2110. During the analysis of external hazard factor:

a) all relevant site and regional data, especially historical data, shall be taken into account, ,

b) special attention shall be paid to the hazard factors that can change in time,

c) acceptability of the used methods and assumptions shall be justified, and uncertainties influencing the results shall be estimated.

3.3.6.2120. If the occurrence frequency of any of the hazard factors of natural origin cannot be estimated with an acceptable low uncertainty, then such an enveloping or equivalent event shall be selected for which safety is justified.

3.3.6.2200. The safe operation of the nuclear power plant shall also be ensured under circumstances of natural external hazard factors. The reasonably assumable combination of the natural hazard factors shall be taken into account. The effect on the safety functions arising from the failure of systems, structures and system components without safety function due to natural hazard factors shall be taken into consideration.

3.3.6.2300. In the case of systems and organisational solutions designed to prevent the effects of external hazard factors, the situation shall be taken into account when access to the site or the service and operation of the systems face permanent difficulties.

3.3.6.2310. The comprehensive management strategy shall comply with Sections 3.2.1.2000., 3.2.2.5800. and 3.3.2.3200., and with the following aspects:

a) predictability and evolution of the anticipated events in time shall be taken into account,

b) appropriate tools and procedures shall be ensured to make it possible that during and after the events taken into account in the design basis the condition of the plant can be confirmed,

c) preparations shall be made for such events that affect more units, more systems, structures and components at the same time; in the case of a redundant system it shall be assumed that all trains are affected; effect on the regional infrastructure, off-site services and protective actions shall also be considered,

d) in the case of a multiunit nuclear power plant the necessary resources shall be ensured also for such events, where common equipment and services are to be used; this shall not unfavourably influence the protection against the events within the design basis.

3.3.6.2320. Condition monitoring and alarms shall be available to forecast the possible hazard factors, if it can be forecasted. Where it is justified, an alarm threshold shall be determined to be able to timely perform the appropriate actions. Furthermore, such intervention thresholds shall be determined, at which the pre-planned post-event interventions shall be performed.

External man-made hazard factors

3.3.6.2400. If radio frequency or microwave electromagnetic radiation source having significant energy density can be detected on the site or in its vicinity, then

their effect on the systems, structures and system components important to nuclear safety shall be examined. If the potential for such an effect exists, then appropriate protective actions shall be implemented.

3.3.6.2500. The external hazard factors in relation to human activity belonging to the design basis and their effect on those systems, structures and system components having safety functions shall be specified. Should these effects influence the performance of the safety function, protection against these effects shall be provided. The protection may also be provided through administrative tools, i.e. restricting any human activity which poses a danger, however, technical solutions for protection shall be preferred against these effects, if such solutions can reasonably be accomplished.

3.3.6.2600 to 3.3.6.3100.

3.3.6.3200. The potential effects of public road and water transport activities in the vicinity of the nuclear power plant and the risks arising from it shall be analysed, with special regard to the transport of hazardous materials.

3.3.6.3300. The parameters of all permanent or temporary facilities that may become the source of fire or explosion shall be identified and determined on the site of the nuclear power plant and in its vicinity, and it shall be evaluated to what extent it poses a hazard to the nuclear power plant. If necessary, appropriate precautionary measures shall be taken.

3.3.7. Fire protection

3.3.7.0100. Those systems, structures and system components important to nuclear safety shall be so designed and positioned that the frequency and the effects of fire are minimal. It shall be ensured that the nuclear power plant can be shut down both during and following a fire, and that the residual heat can be removed, that radioactive material can be prevented from release into the environment and the operating mode of the nuclear power plant can be monitored. In the buildings encompassing systems, structures and system components important to nuclear safety, the rooms comprising the redundant or diverse systems, structures and system components shall be established as separate fire compartments. If this is not accomplishable, fire cells equipped with active and passive fire protection equipment shall be applied in accordance with the fire risk analysis.

3.3.7.0110. Buildings containing equipment important to safety shall be designed by taking into account the results of the fire risk analysis.

3.3.7.0200. Each fire compartment shall be equipped with a fire alarm. The fire signal provided shall be informative in the unit control room with respect to the exact

location of the fire. These systems shall be supplied with an uninterruptible safety power supply and appropriate fire-proof cabling.

3.3.7.0300. Built-in or mobile, automatic or manual extinguishing systems shall be installed, which shall be so designed and placed that the failure or unintentional operation thereof does not affect significantly the ability to perform the safety functions of systems, structures and system components important from the point of view of nuclear safety.

3.3.7.0400. The fire extinguishing system shall cover the areas within the nuclear power plant important from the point of view of safety. The coverage shall be verified by fire risk analysis.

3.3.7.0500. The ventilation systems shall so be arranged that in the event of fire each fire compartment performs its separation function.

3.3.7.0600. Those parts of the ventilation systems which are situated outside of the fire compartments, shall possess the same fire resistance qualification as the fire compartment or their insulation shall be provided by fire flaps of the appropriate category.

3.3.7.0700. The places where fire might cause radioactive release, shall be equipped with fire alarm and, where necessary, with built-in fire-extinguishers. The arrangement, the fire protective separations, the ventilation systems and the built-in fire extinguishers in such locations shall be so designed and installed that the spread of contamination can be prevented and the fire loads are the smallest reasonably achievable. Where combustible material is used during radioactive waste management, such built-in extinguishers shall be applied, where the extinguishing material complies with the applied combustible material.

3.3.7.0800. The possibility and potential effects of self-ignition of radioactive waste shall be analysed.

3.3.7.0900. During the storage and use of explosive materials it shall be ensured that the protection of the relevant system components is proportional to the danger of the material.

3.3.8. Decommissioning

3.3.8.0100. The requirements relating to the final shutdown and decommissioning of the nuclear power plant unit shall also be taken into consideration during the course of the design process.

3.3.8.0200. It shall be provided that the radiation exposure of the persons remaining on the site of the nuclear power plant and the population, as well as the radioactive release are kept at the lowest reasonably achievable level, and the

prevention of radioactive contamination of the environment during decommissioning shall also be provided. In order to achieve the that, such design solutions shall be applied which enable the optimisation of expectedly arising radiation exposures during the decommissioning and to keep the quantity and activity of the generated radioactive waste at a reasonably low level.

3.3.8.0300. In the design phase, measures shall be initiated in order to mitigate radioactive leakages and releases, in order to achieve this:

a) the quantity of covered pipelines, channels and system components embedded into concrete, laid in the ground shall be limited in the walls and floors, monitoring opportunity shall be provided in the case of the covered system components,

b) the quantity of tanks, shafts and sewage water pipes potentially containing radioactive agents shall be limited, and

c) the pipelines, tanks and shafts embedded into concrete shall be manufactured from corrosion-resistant steel.

3.3.9. Human factors

3.3.9.0100. The working areas and working environment of the operating personnel and the human-machine relations shall be analysed from an ergonomic aspects and from the point of view of potential false interventions. The plans shall be prepared taking into consideration the results of the analyses.

3.3.9.0200. The human-machine relations and ergonomic establishment of systems and system components shall be so designed that, taking into consideration the assumed physical environment and the expected psychical condition, the appropriately trained personnel are able to successfully complete their tasks within the expected period of time if necessary.

3.3.9.0210. Appropriate simulation devices shall be designed for facilitating the preparation of the personnel concerned for handling DBC1-4 and DEC 1-2.

3.3.9.0300. During the course of the design process, the analysis of tasks falling under the responsibility of the operating personnel and associated with the performance of safety functions shall be conducted. The scheduled operator interventions and their ability to be executed with appropriate reliability shall be validated, with special regard to the management of DBC4 and DEC 1-2 plant states. For the cases of DBC4, the main instrument of validation is a full-scope simulator. The results of tests conducted on this shall be taken into consideration during the development of procedures and plans for initial training and refreshment training for personnel.

3.3.9.0400. Ergonomic design requirements shall be specified for the design, manufacture and qualification of the operator interfaces in the conceptual design period.

3.3.9.0500. Operating, instrumentation, information technology and process professionals shall be involved to support the design and monitoring of human-machine interfaces, such as control panels and screens.

3.3.9.0600. In order that the members of the operating personnel possess complete information, to the extent corresponding to their positions, which can be efficiently processed in each operating mode of the nuclear power plant, appropriately qualified measuring instruments and traditional or computerised displays shall be placed in the relevant working areas. It shall be provided that the instrumentation enables the measurement of each parameter significant with respect to the reactor core, the reactor cooling systems and the performance of the containment function, the availability of the information necessary for the reliable and safe operation of the nuclear power plant unit, and the automatic recording of measured or derived parameters important in terms of safety.

3.3.9.0700. Appropriate communication systems shall be designed for the purpose of information flow and transfer of instructions between the different locations. The communication systems shall also provide the appropriate mobility necessary for the performance of mobile activities. Communication connections shall be provided with such external organisations, which provide activity that may be necessary during the DBC1 to 4 and DEC1 and DEC2.

3.4. DESIGN OF SYSTEMS AND SYTEM COMPONENTS OF KEY IMPORTANCE

3.4.1. Design of the nuclear reactor and the active core

Integrity of the nuclear reactor and the active core

3.4.1.0100. All potential influencing effects shall be taken into consideration during the design of the structure of the active core and internal components of the nuclear reactor. The safe operability shall be verified by taking into consideration especially the deformations and stress caused by radiation, chemical and physical processes, static and dynamic mechanical loads and temperature, as well as the manufacturing tolerances and the changes occurring during the lifetime.

3.4.1.0200. The active core shall be safely supported and secured to the internal structures of the reactor vessel and through them to the vessel. Its design shall prevent the unplanned displacements and vibrations leading to damage of the entire core structure and components within the structure.

3.4.1.0300. The nuclear reactor and its structural components shall be so designed that it can only be assembled one way and the replacement in the wrong order or inappropriate placement of a system component is not possible.

3.4.1.0400. The construction or the manufacturing process shall provide opportunity for the appropriate inspection of the structure and parts of the fuel assemblies prior to their placement into the active core. Instruments shall be provided for their inspection following irradiation.

3.4.1.0500. The nuclear reactor and the active core shall be so developed that in case of events resulting in DBC1 to 4, the mechanical failures of the systems, structures and system components of the nuclear power plant unit and the physical behaviour of the coolant of the nuclear reactor may not hinder the shutdown, the maintenance of subcritical condition and the cooling of the nuclear reactor.

3.4.1.0600. The measuring instruments installed in the active core shall ensure sufficiently accurate and continuous determination of parameters necessary for monitoring the fulfilment of the criteria and limitations of the operation. The necessary parameters shall be provided based on regularly obtained measurement information or by the combination of measurements and calculations.

3.4.1.0700. The nuclear characteristics of the active core shall be such that changes in temperature, loss of the coolant, boric acid dilution or geometric changes in the active core in DBC1-4 and DEC1 may not cause reactivity increase to an uncontrollable extent.

3.4.1.0800. In the shutdown mode and during the refuelling of the nuclear reactor it shall be ensured that during the placement or removal of fission material or absorbents the subcriticality continuously remains at the prescribed level.

3.4.1.0900. During the design of the active core and its components, the stable, self-regulating operation of the active core shall be ensured in DBC1-2, and the possibility that it can be kept in a safe shutdown condition shall be provided in DBC and DEC 1plant states.

3.4.1.1000. The construction of the active core shall ensure that following an event resulting in DBC1 to 4, the fuel assemblies can be removed by operational instruments from the nuclear reactor.

3.4.1.1010. Components that measure the neutron flux distribution in the reactor core and its changes shall be ensured in such a manner that provides the proper level of controllability of the parameters of the conditions and limits related to the neutron flux distribution in the core and its changes.

3.4.1.1020. At any state of the reactor core the occurring neutron flux distributions shall be inherently stable. The demands for a control system serving the maintenance of the shape, level and stability of the neutron flux distribution shall be minimum in all operating conditions.

Control of reactivity

3.4.1.1100. The shutdown of the nuclear reactor and the control of reactivity shall be provided by at least two such systems that operate according to different principles, and either of them shall be able by itself to shut down the nuclear reactor from DBC1 to 4. At least one of the shutdown systems shall be automatic and quick-acting which, if the pre-determined criteria are met, interminably shuts down the nuclear reactor with high reliability regardless of the activities of operating personnel. All shutdown and control systems shall be single failure tolerant, even in the case of failure of any electric power supply or the inability to operate the control rod of the highest worth.

3.4.1.1110. The shutdown equipment shall be suitable to avoid each foreseen reactivity increase that could lead to inadvertent criticality during the shutdown, in shutdown state or during refuelling.

3.4.1.1120. Instrumentation and instrument tests shall be designed to ensure that the shutdown equipment are in the position determined for the given operating conditions.

3.4.1.1200. The reactivity control of the active core shall be achieved with such combination of fuel enrichment, control and safety rods, dissolved and burnable reactor poisons, which ensure the avoidance of a relatively quick significant increase in reactivity in DBC1-4.

3.4.1.1300. The protection signals shutting down the nuclear reactor shall be so developed that at events resulting in DBC2 to 4, the protective operation occurs when the limit value of either one of two different, independent physical features, which individually measure with appropriate redundancy, is exceeded. The outcome of the event sequences initiated from events resulting in DBC2 to 4 may not be significantly dependent on which physical parameter triggers reactor protection.

3.4.1.1310. The reactor protection shall be fail safe and shall be capable of overwriting the non-safe intervention of the control system.

3.4.1.1400. By the appropriate design of the systems controlling the reactivity and shutting down the nuclear reactor, it shall be ensured that in DBC1 to 4 the exceeding of the safety limits with regard to the temperature of the nuclear fuel and coolant, and to other physical parameters is excluded.

3.4.1.1500. During the design of reactivity control equipment due attention shall be provided for the wear-out and the irradiation effects, including burn-up, change of physical conditions and gas generation.

3.4.1.1600. The systems controlling the reactivity and shutting down the nuclear reactor shall be designed in such a manner that the extent and speed of reactivity increase cannot exceed the design limit even in the case of operation outside the design.

3.4.1.1610. Subcriticality shall be ensured and shall be maintained in all operating conditions of the spent fuel pool.

Design of the fuel assemblies

3.4.1.1700. The entire life cycle of the fuel assemblies shall be planned, and the fulfilment of the nuclear safety criteria shall be verified in each phase, all the expected effects shall be taken into consideration, from the arrival of fresh fuel assemblies to the interim storage of spent fuel assemblies, including the management and transportation processes.

3.4.1.1710. The nuclear fuel shall be so designed as not to preclude the possibility of recycling or safe final disposal.

3.4.1.1800. Under the conditions of normal operation, the leakage of fission products from the irradiated fuel rods shall be kept at the lowest practically possible level.

3.4.1.1900. During design, methods shall be provided for the identification and special treatment of faulty fuel assemblies.

3.4.1.2000. The fuel assemblies, taking into consideration the maximum permitted burnout, shall tolerate all effects of deterioration processes without a failure exceeding the extent permitted by the design.

3.4.1.2100. It shall be provided by appropriate design that the flow induced vibrations and movements do not damage the fuel rods.

3.4.1.2200. Different fuel assemblies may only be introduced following the demonstration of the fulfilment of the design requirements. In the absence of relevant reference, problem-free application in a similar nuclear power plant, under the same usage conditions, the application of Lead Test Assemblies is necessary.

3.4.1.2300. In the case of a fuel element type different from the one used before, the validation of models describing the behaviour of the nuclear fuel, the specification of design requirements of the fuel assembly and compliance with design criteria shall be verified by experimental results.

3.4.1.2400. In the case of the use of a fuel element type different from the one used before or the modification of the chemical or physical properties of fuel and the cladding and mechanical components, in addition to the specifications in Sections 3.4.1.1700 to 3.4.1.2200, the following shall be presented to demonstrate safety:

a) the results of experiments and references based on which the individual design limits have been determined, and

b) the results of bench test measurements demonstrating the ability to comply with the strength requirements of the structural elements of fuel assemblies..

3.4.2. Design of the main circulation loop

3.4.2.0100. The system components in the main circulation loop shall bear all static and dynamic loads which affect these system components in the DBC1 to 4 and DEC1 of the nuclear power plant in such a manner that the safety and physical barrier functions are performed in accordance with the criteria assigned to the operating mode.

3.4.2.0200. The effects expected during the operation on the system components during their lifetime, including all the uncertainties which are present in the determination of the initial condition of the system component features and the potential deterioration due to ageing shall be taken into account during the design. Accordingly, the system components of the main circulation loop shall be designed with sufficient margin, while it must also be verified that the robust design does not lead to disadvantages in DBC4 and DEC plant states.

3.4.2.0300. The main circulation loop, as a system that stores the primary circuit heat transfer medium under pressure shall be designed in such a way that:

a) the potential of catastrophic failure shall be excluded;

b) in the event of break of connecting pipelines, the closure of the main circulation loop shall be ensured by installing two fittings for closure in each pipeline that are positioned near the primary water circuit; and

c) the continuous monitoring of the integrity of the main circulation loop must be provided for.

3.4.2.0400. During the selection of materials for the main circulation loop, the activation of structural materials during operation shall be decreased to a minimum, with special regard to the decommissioning aspects of the nuclear power plant.

3.4.2.0500. In the case of internal structural components of the main circulation loop, the potential of such failures, which may result in the damage of other main circulation loop components due to lose parts, shall be decreased to a minimum.

3.4.2.0600. The steam generators shall be so designed that they function as an appropriately reliable barrier from both the primary and the secondary circuit sides. The leakage potential from the primary into the secondary circuit shall be limited to a minimum during design and instruments shall be provided to monitor and localise the leakages.

3.4.2.0700. The heat-exchanger tubes of the steam generators shall be welded into the tube sheet from the primary side. The heat-exchanger tubes shall be expanded in order to decrease the gap between the tubes and the secondary side of the tube sheet.

3.4.2.0800. The heat-exchanger tubes of the steam generators shall be fixed in order to decrease the damage caused by vibrations. The tube supports shall be designed to cause the least wear by and deposits from the operational media between the heat-exchanger tubes and the support. The heat-exchanger tubes shall be made of wear-resistant material.

3.4.2.0900. The heat-exchanger tube bundles of the steam generators shall be designed to allow for sufficient reserve available to compensate for plugged and clogged heat-exchanger tubes to the end of the design lifetime.

3.4.2.1000.

3.4.2.1100. The size of the water and steam volumes of the steam generators shall be determined with sufficient reserve in order to enable observance of operational limitations specified for the primary and secondary circuits in each mode of normal operation.

3.4.2.1200. The size of water and steam spaces of the pressurizer shall be determined with sufficient reserves in order to enable observance of operational limitations specified for the primary circuit in each operational mode of normal operation.

3.4.2.1300. The primary circuit shall be supplied with appropriate overpressure protection. Pressure control systems shall be designed to manage the effect of changes in volume due to temperature changes in the primary circuit coolant, while also considering the following requirements:

a) the system components of the main circulation loop shall be protected against unacceptable excess pressure even in cold condition,

b) for the management of the greater pressure transients excludable pressure relief system components shall be designed, also

c) the decrease of pressure in accident situation shall be ensured.

3.4.2.1400.

3.4.3. Heat transfer

3.4.3.0100. All the forms of heat generation and heat transfer occurring in the active core of the nuclear reactor shall be determined and analysed with respect to quality and quantity. Continuous heat removal to the necessary extent and transfer to the ultimate heat sink shall be provided by the application of the heat transfer systems and system components.

3.4.3.0200. The cooling of the active core shall be ensured by the following:

a) forced circulation shall be provided for the transfer of the generated heat or residual heat under operating conditions ranged from nominal power of the nuclear reactor to the cooled down condition; and

b) natural circulation cooling of sufficient efficiency in the main circulation loop shall be ensured that provides the diversion of residual heat from the active core when forced circulation is shut down.

3.4.3.0300. In order to provide continuous cooling:

a) pipelines connected to the reactor vessel below the top of active part of the nuclear fuel shall be avoided, and in case the connection of smaller pipes below this level is unavoidable then it shall be verified that in shutdown modes the reactor vessel cannot be emptied below the top of active part of nuclear fuel,

b) by the arrangement of the system components of the main circulation loop it shall be provided that in filled up condition free water surface exists only in the pressurizer,

c) by the arrangement of the path of the main circulation loop it shall be ensured that the decrease of the primary coolant level below the hot leg nozzles is not necessary for the drainage or maintenance of steam generators.

d) by their removal it shall be ensured that non-condensable gases cannot hinder the natural circulation, also

e) the opportunity for removal of corrosion products and depositions shall be ensured to avoid blockage of the flow routes and thereby endanger the cooling of the active core.

3.4.3.0400. The steam generators shall be so designed that they provide the appropriate cooling of the nuclear reactor in DBC1-4 and DEC1.

3.4.3.0500. Under DBC2-4, the removal of residual heat from the reactor, the spent fuel pool and the containment shall be ensured by stand-alone and diverse equipment even in the case of a single failure and a station blackout. It shall be

ensured that under DBC2-4, the limits set for the fuel elements and for the pressure equipment and pipelines of the primary circuit are not exceeded.

3.4.3.0510. At least one of the technical solutions designed for the removal of the residual heat from the reactor and the spent fuel pool shall fulfil its function also during DEC events caused by external hazard factors.

3.4.3.0520. It shall be demonstrated that if the cooling of the fuel elements planned for DBC1-4 ceases to exist, there is sufficient time for starting an alternative cooling of the fuel elements.

3.4.3.0600. In the case of systems containing irradiated fuel assemblies such as the shutdown nuclear reactor or the spent fuel pool, such solutions shall be used that allow for passive heat transfer.

3.4.3.0700. If the capability of transferring the residual heat to the ultimate heat sink cannot be demonstrated for every operating condition with high reliability, then a secondary ultimate heat sink and systems required for its operation shall be provided, which ensure through their locations and design solutions that the heat removal safety function is not lost as a result of external hazard factors.

3.4.4. Unit main and backup control room and technical support centre

3.4.4.0100. A main control room shall be established within the unit of the nuclear power plant, from where the activities aimed at normal operation of the nuclear power plant unit, its maintenance in safe mode or its return to such mode can be performed in DBC1 to 4, DEC1 and DEC2. The most up-to-date ergonomic aspects and principles shall be taken into consideration during the design of the unit main control room.

3.4.4.0200. Sufficient displaying and archiving and intervention instruments shall be available for operating personnel in the unit main control room for DBC1 to 4, DEC1 and DEC2 for the following purposes:

a) appropriate monitoring of the condition of the nuclear power plant unit and its systems, structures and system components,

b) clear and timely indication of any changes with a significant effect on safety,

c) identification of any automatic protective operation and if not started, their subsequent launch, and

d) providing a comprehensive picture of the processes of the nuclear power plant unit.

3.4.4.0300. A backup control room shall be established at the nuclear power plant unit at a location functionally independent of, and separated from the unit main

control room both physically and with regard to its electrical system. Instrumentation and control instruments sufficient for monitoring the condition and interventions shall be installed for the case if the normal operation of the unit main control room became impossible for any reason, to:

a) enable the nuclear reactor to be shut down and cooled down and to keep it in a safe shutdown condition for unlimited time; and

b) provide for residual heat removal from the nuclear reactor and other systems containing irradiated fuel assemblies and continuous monitoring of the important parameters of the nuclear power plant unit.

3.4.4.0400. The operability of the unit backup control room shall be provided by regular inspection.

3.4.4.0500. It shall be provided that during the internal or external events of DBC1 to 4 and DEC1 and DEC2, the unit main control room and the backup control room cannot become unsuitable for usage simultaneously, and the long term habitability of the unit main control room and the backup control room by the operating personnel shall be provided.

3.4.4.0600. The reception and display of the necessary information shall be provided in the main control room and the backup control room, enabling timely assessment of the condition of the nuclear power plant unit and the critical safety functions in DBC2 to 4 and DEC1, DEC2.

3.4.4.0700. A continuous and uninterruptible power supply shall be provided for the systems and system components of the unit main and backup control rooms which perform safety functions.

3.4.4.0800. Such technical solutions shall be applied which exclude the possibility of simultaneous operation of the systems and system components from the unit main control room and the backup control room. When either control room is in use, the signals arriving from the other control room shall be excluded. The unauthorised use of the backup control room shall be prevented.

3.4.4.0900. The identification of potential events within or outside the unit main and backup control rooms, which may directly endanger the personnel present or the continuous use of the control room, shall be managed with priority. During the design process such reasonably achievable measures shall be defined, which minimise the effects of such events.

3.4.4.1000. The unit main and backup control rooms shall be situated in separate fire compartments to enable the safe shutdown of the nuclear reactor and the

maintenance of safety functions necessary in shutdown mode also in the event of fire occurring in the surrounding rooms.

3.4.4.1010. An appropriate passageway shall be provided between the main and backup control rooms.

3.4.4.1100. The following requirements shall be taken into consideration during the design of the unit main and reserve control rooms:

a) stable and balanced division of tasks and sufficient informational instruments shall be provided for the operating personnel,

b) the logical functional classification of the displayed information and the intervention instruments shall be provided, with special regard to ensuring that the classification of information and interventions is not contradictive, and

c) it shall be ensured that insignificant or irrelevant information is not displayed.

3.4.4.1200. The following requirements shall be taken into consideration during the design of the unit main control room in accordance with Section 3.4.4.0100:

a) option for screen-based monitoring of the systems and processes and high-capacity information technology instruments supporting the operating personnel shall be provided,

b) the unified overview of the actual condition and main parameters of the nuclear power plant unit shall be ensured in a clearly visible and easily interpretable manner for the unit control room personnel, also

c) the following shall be provided in the safely reachable and manageable proximity of the personnel:

ca) availability of instruments necessary for external and internal communication,

cb) the results of radiation protection measurements of technological processes and emissions,

cc) information from fire alarm systems and the operation of fire extinguisher systems of priority importance,

cd) instruments necessary for the performance of maintenance tasks and issuance of maintenance permits,

ce) availability of the documentation of the unit main control room,

cf) instruments for access control and restriction of to the unit main control room,

d) unambiguous sequence shall be set between the alarms, and

e) the number of alarm systems and alarms transmitted by the process computers shall be minimized.

3.4.4.1300. The following requirements shall be taken into consideration during the design of the backup control room:

a) a safe access route shall be established between the unit main control room and the backup control room taking into consideration the anticipated instances of use of the backup control room,

b) the human-machine interface solutions of the backup control room shall be constructed similarly to the unit main control room considering the functions, and

c) the following shall be provided in the backup control room:

ca) appropriate situation of the personnel necessary for operation,

cb) availability of instruments necessary for external and internal communication,

cc) information and intervention instruments necessary for the tasks to be performed from the backup control room, and

cd) availability of the documentation of the backup control room.

3.4.4.1400. A technical support centre independent of both the main and backup control rooms shall be established on the site, from which technical support can be provided to the operating personnel in the DEC1 and DEC2 of the units. At the centre, access shall be provided to the operating parameters and the radiation data of the nuclear power plant and its immediate vicinity. The centre shall be provided with devices suitable for communication with the unit main control room, the backup control room and all locations of the power plant important to accident management. The centre shall remain operable and safely usable by the personnel under the DEC1 and DEC2 of the units.

3.4.5. Electrical systems and instrumentation and control

Electrical systems and equipment

3.4.5.0100. It shall be ensured that the electric power supply system of the nuclear power plant unit is able to supply the safety class systems and system components with electrical power necessary for operation, assuming single failure and the loss of off-site voltage.

3.4.5.0200. It shall be ensured that the electrical transients, starting from both the internal and the external network, affect the systems of the nuclear power plant unit to a minimum extent.

3.4.5.0300. The electric power supply of systems and system components important to nuclear safety shall be designed according to their safety class and graded requirements.

3.4.5.0400. The permitted electric load of the electrical systems and system components in DBC1 to 4 shall not exceed their nominal load capacity. The limitations with regard to the electric load of the systems and system components shall be given in the design specification. Based on these, the quantity, quality and output of the power sources required for the operation of the safety systems shall be determined, taking into account any common cause defects and the necessary period of operation.

3.4.5.0410. Appropriate power supply shall be provided for the cases of DEC in accordance with the necessary interventions and timeframe established by DEC analyses, taking into account external hazard factors.

3.4.5.0500. The design basis shall contain appropriate actions for the management of events occurring in the normal electrical power supply system of the nuclear power plant unit, so that the safety of the nuclear power plant unit can also be guaranteed in such situations.

3.4.5.0600. In addition to safety classification, the power supply systems and system components shall also be categorised with respect to the allowed loss of electric power supply. The electricity supply network of the nuclear power plant unit shall be designed on the basis of this approach.

3.4.5.0700. The features of uninterruptible power supply and the duration of allowed loss of essential energy supply shall be determined by safety justification. The batteries performing a function under DEC1 and 2 shall have sufficient capacity until they can be recharged or another power supply solution can be provided.

3.4.5.0800. When operational power supply is lost or its parameters exceed the acceptable range, the systems of safety electric power supply shall automatically switch to backup supplies within appropriate time.

3.4.5.0900. For the power supply of the systems and system components important to nuclear safety, interlinked electrical connections can only be established in such a way that incorrect operational or maintenance actions cannot result in unintentional loss of function.

3.4.5.0910. In the case of a nuclear power plant having more than one unit, direct electrical connection shall be provided between the units to the reasonably practicable extent in such a way that the spread of possible defects from one unit to another should be practically eliminated.

3.4.5.0920. A power source shall be designed, which is:

a) independent physically and in terms of system technology of the emergency power source designed for handling DBC2-4, and

b) able to provide appropriate power supply to prevent DEC2 and to mitigate their consequences in the event when both the external and internal electricity supplies are completely lost.

Instrumentation and control

3.4.5.1000. Instrumentation suitable for the measurement of parameters necessary for monitoring fundamental safety functions shall be ensured, thus ensuring the availability of information necessary for the reliable and safe operation of the nuclear power plant unit and the management of events resulting in DBC1 to 4 and DEC1 and 2. The automatic recording of all relevant measured and derived parameters important to nuclear safety shall also be ensured.

3.4.5.1100. Monitoring and measurement instrumentation shall be provided for the observation of those locations where radioactive materials are present and for the measurement of their quantity in all such locations where they may be released into the environment.

3.4.5.1200. The instrumentation and control configuration, operation logic or the associated data of systems and system components important to nuclear safety shall not be modified by such maintenance or test solutions which are not designed for that specific function or are not under strict administrative supervision.

3.4.5.1210. The applied instruments shall be validated and appropriately maintained, and shall be tested with the determined frequency.

3.4.5.1300. The signals of protection operations or important parameter deviations shall be supplied with sound alarms both in the unit main and backup control rooms. The signals of protective operation can be acknowledged only by the intervention of the operating personnel even after the termination of the exceeded limit.

3.4.5.1400. Instrumentation associated with safety parameters shall ensure the recognition of the faulty condition of both the measurement and the processing system.

3.4.5.1500. Appropriate control instruments shall be applied to maintain operational parameters within the specified range.

3.4.5.1600. Such instrumentation, data processing, display and archiving system shall be established, which is independent of any other data processing, display and archiving system to the extent reasonably achievable and is suitable to provide

information regarding the condition of the nuclear power plant unit even under the environmental circumstances of DEC2 plant state, to the extent of internal instructions and the guide developed for such situations.

3.4.5.1700. The instrumentation and control engineering systems shall ensure:

a) the safe automatic shutdown of the nuclear reactor and the activation of safety systems when specified parameters are reached,

b) sufficient and appropriate information for the operating personnel about the condition of the nuclear power plant,

c) intervention and monitoring instruments

ca) for the supplementation of failed automatic operations,

cb) for manually or automatically taking the nuclear reactor into safe shutdown mode and for maintaining such mode under the circumstances of DBC1 to 4 and DEC1,

cc) for those safety interventions which do not belong to the scope of automatic safety operations, and

cd) for manual interventions necessary for accident management, furthermore

d) appropriate data storage and recording system to facilitate the investigation of the details of any transient or incident at a later time.

The batteries performing a function under DEC1-2 plant states shall have sufficient capacity until they can be recharged or another power supply solution can be provided.

3.4.5.1800. It shall be ensured that the reactor protection system detects DBC1 to 4 and DEC1 and it shall ensure accordingly:

a) shutdown of the nuclear reactor,

b) operation of system components performing the appropriate safety function, also

c) activation of supporting functions.

3.4.5.1900. The specification of the technological function of the instrumentation and control systems shall be in compliance with the following criteria:

a) it shall identify the control task in accordance with the technological purposes and requirements,

b) it shall assign an unambiguous identification code to each control task,

c) it shall include the control tasks in safety classes on the basis of the importance of the given task in terms of safety and shall assign them to the appropriate levels of defence in depth,

d) it shall set the diversity requirements for the functions,

e) it shall specify response times for the functions,

f) it shall specify the safe condition or position for every output, which the output should assume in the case of its detected defect,

g) it shall determine the tasks which require operator intervention in DBC of the nuclear power plant in such a manner that the operating personnel are able to perform them,

h) it shall use a formal descriptive method and in the interest of transparency, it shall have multiple levels and an appropriate structure,

i) it shall envisage an automated system for formal monitoring and verification,

j) it shall contain the information necessary to perform operator tasks and to monitor the automatic tasks,

k) it shall set accuracy requirements for operating standards and the display of analogue values, and

l) simulation methods shall be determined for programmable instrumentation and control systems in Safety Class 2 for their functional monitoring and validation.

3.4.5.2000. The design and implementation of the instrumentation and control systems and system components shall be carried out in accordance with the selected standards applicable to systems and system components of the relevant safety class and differentiated requirements.

3.4.5.2100. The human and automatic interactions between the instrumentation and control systems and the outside world shall be determined in the form of logical and physical interfaces. The designed interactions shall not hinder the performance of automatic safety functions.

3.4.5.2200. The subsystems of the instrumentation and control systems in Safety Class 2 shall be redundant to an extent sufficient for the fulfilment of the required failure tolerance. The functionality of redundant resources shall be as identical as possible whilst applying the intended diversity.

3.4.5.2300. The principle of defence in depth shall be applied during the assignment of the functions of the programmable instrumentation and control systems to the subsystems. The non-safety functions or those in a lower safety class shall not be built into a safety class or higher safety class subsystem . Should this not be possible,

it shall be verified by safety analysis that the subsystem performing a function in a lower safety class does not hinder in any way the performance of any function in a higher safety class.

3.4.5.2400. In case of connections between programmable instrumentation and control systems in different safety classes, it shall be verified that the system in the lower class has no influence on the operation of the system in the higher class. In the case of connections between programmable instrumentation and control systems in the same safety class, it shall be verified that the failure of one of the systems does not hinder the performance of the autonomic safety function of the other.

3.4.5.2500. The criteria relating to the accuracy, response time, event sequence determination, processing capacity reserve and communication capacity reserve of the programmable instrumentation and control systems shall be specified consistent with the design basis of the nuclear power plant.

3.4.5.2600. The tolerance of single failure shall continuously be maintained in terms of each safety function performed by a programmable instrumentation and control system being in Safety Class 2. Loss of function is impermissible even in case of maintenance or periodic testing. It shall be verified that the applied architecture complies with the reliability criteria.

3.4.5.2700. All components of the programmable instrumentation and control system in Safety Class 2 shall possess automatic self-check ability. If a failure is detected during self-check, if necessary, the outputs of the subsystem shall be directed in a pre-determined condition towards the direction of safety.

3.4.5.2800. Manually initiated testing opportunity shall be provided for the detection of those failures of a programmable instrumentation and control system categorised into Safety Class 2 which cannot be detected by self-check and for the demonstration of the operability of safety functions. The appropriateness of the testing cycle shall be demonstrated by the combined application of deterministic and probabilistic safety analyses.

3.4.5.2900. In the case of programmable instrumentation and control systems in Safety Class 2, the potential for common cause failures shall be minimised by the application of functional or system component level diversity to the appropriate extent. The necessary extent of diversity shall be deduced from the required reliability criteria. It shall be verified by analysis that the probability of common cause failures is sufficiently low with the selected solution.

3.4.5.3000. Criteria shall be specified according to the design basis of the nuclear power plant, for the probability of operation failure when actuation is requested and,

in the case of programmable instrumentation and control systems in Safety Class 2, relating to the frequency of false actuation.

3.4.5.3100. The safety class systems and components of instrumentation and control systems shall be fully tested in the given environment, with the preliminary determination of the testing and acceptance criteria:

a) during the development phase, verification, validation and a concluding testing plan shall be elaborated for Safety Class 2 safety class programmable systems and components realized on computer platform, microprocessor platform, or via programmable electronic components or complex electronic components of other technology. The verification, validation and testing plan shall be implemented during the development and before the commissioning,

b) in the case of Safety Class 2 safety class systems and components, the program or logic of which is still changeable after the first commissioning, the further developments and modifications becoming necessary during the operating lifecycle phase and during the design of modifications according to the regulations, the verification, validation and the concluding testing plan shall be elaborated again, and shall be implemented before re-commissioning with the involvement of the designer, manufacturer and the user or operator,

c) during the development phase, verification, validation and a concluding testing plan shall be elaborated for Safety Class 3 or lower safety class programmable systems and components realized on computer platform, microprocessor platform, or via programmable electronic components or complex electronic components of other technology. During the development of modifications according to the regulations, a validation and a concluding testing plan shall be elaborated and shall be implemented before re-commissioning,

d) safety functions and the systems fulfilling them shall be tested at the manufacturer, examination or qualification laboratory under the conditions characteristic for the facility. The tests shall cover the aspects of the interconnected hardware, software and system integration, furthermore the initiating events taken into account during the design for the facility that necessitates safety and other functions,

e) information technology systems related to complex electronic components shall be qualified according to the significance interpreted for safety, and

f) the verification, validation and testing shall be documented, and shall be available to use by the operator and the authorities during the licensing and commissioning proceedings.

3.4.5.3200. Appropriate design solutions and measures shall ensure that the programmable instrumentation and control systems can only be accessed, both physically and logically, only by those persons for whom it is necessary to perform a specific task and at a level and with the options that are necessary to perform the task.

3.4.5.3300. When a commercial product is applied, it shall have specific and type identification and appropriate qualification to verify that the product complies with the criteria derived from the design basis.

3.4.5.3400. The instrumentation shall provide information regarding the condition of critical safety functions, the condition of process systems required for handling the operating condition even under the circumstances of DBC1-4 and DEC1 and DEC2.

3.4.5.3500. With regard to the instrumentation and control of the nuclear power plant unit, by making difference between the rigidly wired devices, including the logics manufactured with semi-conductor based circuits, and the programmable devices, the physical opportunities for modification of accesses, function, programs and data shall be determined. These opportunities shall be eprioritized from the aspect of feasibility and the level of knowledge required for the modification and the interventions shall be designed accordingly.

3.4.5.3510. In the design of programmable instrumentation and control devices the relevant parts of the Design Basis Threat and the provisions of the government decree on physical protection requirements for various applications of atomic energy and the corresponding system of licensing, reporting and inspection shall be taken into account.

3.4.5.3520. During the design the physical protection aspects of the programmable systems shall be taken into account. If there is a contradiction between nuclear safety and physical protection aspect during design of programmable systems, the nuclear safety aspect takes priority.

3.4.5.3600. Abnormal operation of the computers shall be detected. It shall be ensured that the program and constant data files are checkable with reliable data read from read-only data carrier and produced during installation. If it is feasible a credibility check of the data read from the technology should be provided.

3.4.5.3700. Systems and devices related to operating executable units of the protection and safety systems, and those being important to nuclear safety and collecting and displaying data influencing the decisions of the operating personnel shall be protected against external information technology influence that can modify or prevent fulfilment a safety function.

3.4.5.3800. The opportunities of physical access, placement of data forwarding devices and data cables shall be established in accordance with the physical protection zones.

3.4.5.3900. The necessary administrative system and the safety protocols of the associated internal procedure and access shall be elaborated:

a) implementation of maintenance necessary in the systems,

b) necessary modification of the digital systems,

c) reparation of the revealed program and data errors, and

d) checking, in and out transport of the data carriers.

3.4.5.4000.

3.4.6. Containment and its systems

Construction and integrity of the containment

3.4.6.0100. During the design of the containment the following shall be realised:

a) physical barrier function restricting the release of fission products and the function ensuring the monitored release of fission products;

b) shielding function protecting against ionising radiation under DBC1-4; and

c) the protection function against external events.

3.4.6.0200. For the performance of physical barrier and monitored release function of the containment:

a) the leakage of the containment shall be limited at such value at which the releases can be controlled at the lowest reasonably achievable level under DBC2-4, and the compliance with the specifications of Sections 3.2.4.0100 to 3.2.4.0500 can be ensured,

b) in the case of DEC1plant state, radioactive releases shall be minimised to the extent reasonably achievable,

c) in the case of DEC2 plant state, the release of radioactive materials shall be limited both in time and quantity in order to ensure that:

ca) sufficient time is available for introducing population protection measures, if necessary,

cb) the long-term contamination of large areas can be avoided,

d) the concentration of radioactive aerosols and radioiodine shall be reduced in the containment atmosphere,

e) leaktight valves shall be installed to ensure leaktight closing of pipelines penetrating the wall of the containment,

f) in order to retain the physical integrity of the containment, the climate of the containment in normal operation shall be appropriate and the normal operational ventilation system of the containment shall be suitable to provide the pressure in accordance with the design,

g) the in-service testing of containment leakage shall be ensured,

h) heat removal from the containment, protection of the structure against overpressure and the handling of flammable gases generated shall be ensured in all operating conditions,

i) the cleaning of the atmosphere of the containment or the filtering of gaseous media released from the containment shall be provided,

j) the containment elements shall maintain the effect of direct radiation originating from the included systems, structures and system components at the lowest reasonably achievable level of personnel performing work within the containment and those outside the containment, and

k) the destructive effect of core melting on the structural integrity of the containment shall be prevented or shall be limited to the extent reasonably achievable.

3.4.6.0300. During the implementation of the protective function against external events it shall be ensured that

the building structure and internal structural elements of the containment as well as the process systems of the containment are designed and are so resistant against the effects of external hazard factors to be taken into account that they ensure the integrity and operability of main circulation loop systems, structures and system components containing the primary circulation loop heat transfer medium and of the systems designed to prevent fuel damage when external events occur, whilst keeping leakage limits of the containment and the global integrity of the structure.

3.4.6.0400. The functions of the containment can be provided by either one or two separate containment structures.

3.4.6.0500. Processes resulting in DBC2 to 4 and events resulting in DEC1 and 2 shall be taken into consideration during the design of the containment, in accordance with the acceptance criteria specified for the relevant operational mode. General principles for pressure retaining equipment and pipelines shall be applied for the strength design of the containment while taking into consideration the material properties and the features of the load bearing structure.

3.4.6.0600. The containment shall be so designed that it enables

a) regular monitoring of the pressure retaining capacity of the containment,

b) leakage monitoring at service pressure,

c) performance of pressure tests,

d) monitoring the condition of the containment and its ability to perform its function, and

e) periodic and local testing of leakage of penetrations, manholes and airlocks having flexible sealing and expansion fittings.

3.4.6.0700. The method and frequency of containment monitoring shall be specified.

3.4.6.0800. Containment penetrations of appropriate size shall be provided between internal rooms or spaces, in order to prevent that pressure difference and the high flow-rate of the media in the containment does not cause damage in the structure or any other system component.

3.4.6.0810. The number of penetrations through the containment wall shall be kept to a practical minimum and all penetrations shall meet the same design requirements as the containment structure itself. The penetrations shall be protected against reaction forces caused by the movement of pipes or accidental loads such as those due to missiles caused by external or internal events, jet forces and pipe whip.

3.4.6.0900. The entry of the operating personnel into the containment shall be accomplished by such interlocked airlocks which can ensure that at least one door of the airlock is in closed position in DBC1 to 4.

3.4.6.1000. The functionality criteria for the containment airlocks for DEC1 and 2 shall be determined.

3.4.6.1010. Safety provisions shall be determined for the personnel entering the containment.

3.4.6.1020. Containment openings for the movement of equipment or material through the containment shall be designed to allow quick and reliable closure in the event that isolation of the containment is required.

3.4.6.1100.

3.4.6.1200. The material of claddings and coatings shall be selected and its application shall be specified in accordance with the function of the containment. Their application, abrasion and failure shall not influence the performance of the safety functions.

3.4.6.1210. The loss of the structural integrity of the containment shall be practically eliminated. To this end, equipment stored on or off site may also be used for controlling the conditions prevailing in the containment.

Process systems of the containment

3.4.6.1300. The containment as a system shall comprise the following:

a) all important parts of the primary circuit,

b) systems capable of controlling pressures and temperatures,

c) isolation elements, and

d) instruments serving for the management and removal of fission products, hydrogen, oxygen and other materials released into the containment atmosphere.

3.4.6.1400. The heat removal system of the containment shall ensure the quick reduction of the pressure and temperature in the containment following a loss of coolant event, and then it shall ensure their maintenance at a reasonably achievable low level, assuming single failure.

3.4.6.1500. The containment heat removal system shall be so designed that the in-service inspection of the components necessary for the provision of the integrity and performance of the system can be implemented.

3.4.6.1600. Technical solutions shall be applied in the design of the containment for DEC1 and 2, for the monitoring and control of pressure and temperature in the containment, as well as for the management of combustible gases. The leaktightness of the containment shall not decrease in a significant extent during a reasonable period following such events.

3.4.6.1610. The cross-sections of openings between containment compartments shall be of such dimensions as to ensure that the pressure differential occurring during pressure equalization under accident conditions does not result in unacceptable damage to the pressure retaining structures or to systems that are important in mitigating the effects of DBC4 and DEC.

3.4.6.1700. The pipelines penetrating the containment wall shall be supplied with two reliable and independently operated serial isolation valves , one being placed within the containment and the other outside of it. The isolation valves shall be either supplied with remote operation or interlocked in closed position. Status signals about their position shall be displayed in the unit control room. The valves shall be placed as close as possible to the containment wall. The specification of the isolation valves shall be determined by taking into consideration all operating conditions belonging to the design basis of the nuclear power plant.

3.4.6.1800. The containment isolation shall be possible even in DEC1-2 plant states. In those shutdown states, when timely isolation cannot be performed, the fuel damage shall be avoided. If an event leads to an environmental release by bypassing the containment, such design solutions shall be provided that prevent any damage to the fuel elements.

3.4.6.1900. The ventilation systems of the containment shall be so designed that

a) they provide an habitable environment for work of the operating personnel in the rooms which can be accessed in DBC1;

b) they provide conditions in line with the qualification of the equipment located in the rooms of the nuclear power plant unit;

c) they limit the spread of materials harmful to health and ensure the reduction of the concentration of harmful material in the air to a level below the official limit value that is considered a threat to health; also

d) they ensure appropriate ventilation and separation according to the needs of different rooms, the separation of ventilation routes in order to eliminate or reduce the risk of danger sources to a level below the acceptable value.

3.4.6.2000. The cleaning of the containment atmosphere shall be so performed that the systems which provide the management and monitoring of the fission products, hydrogen, oxygen and other material potentially released into the containment atmosphere, ensure the reduction of the quantity and concentration of the fission products released into the environment, assuming single failure, as well as the control of concentration of hydrogen and oxygen in the containment atmosphere, in order to provide the integrity of the containment.

3.4.6.2100. The cleaning system of the containment atmosphere shall be so designed that it enables the appropriate in-service inspection of the important components in order to ensure system integrity and performance.

3.4.6.2200. Appropriate protection shall be provided against fire in the containment. However, the arrangement of the fire barriers cannot hinder the function and operation of the containment.

3.4.7. Auxiliary and support systems

Essential service water system

3.4.7.0010. The reliability of the auxiliary and support systems shall satisfy all requirements set against the safety systems supplied by them and their capability to function shall be testable.

3.4.7.0100. The heat removal from systems, structures and system components important to nuclear safety and the maintenance of their temperature at the designed level under normal operation and accident conditions shall be provided by the essential service water system. Single failure shall be assumed at the design of the system.

Ventilation and air conditioning systems

3.4.7.0200. The ventilation and air conditioning systems of the nuclear power plants shall ensure the prevention or reduction of the dispersion of radioactive materials within the facility or their release into the environment, and the climate conditions necessary for the operating personnel or equipment, which maintain the qualified state.

3.4.7.0210. In the case of rooms containing system components important to nuclear safety, it shall be examined what effect the failure of the ventilation and air conditioning system has on their operation.

3.4.7.0300. The following shall be ensured by the ventilation and air conditioning systems which limit the spreading of radioactive materials:

a) the extent of air exchange in a room shall be proportionate to the extent of the concentration of radioactive materials moving with the air,

b) the direction of air flow shall be oriented from the less contaminated areas towards the more contaminated areas, also

c) the number and arrangement of the systems shall ensure the separation of ventilation of the more contaminated rooms from the less contaminated rooms.

3.4.7.0400. During the design of the ventilation systems, the following shall be ensured as general requirements:

a) taking into consideration external effects and climatic conditions such as external fire or explosion, extreme wind speed, risk of obstruction due to snow or other kinds of contamination, high humidity, risk of entry of chemicals,

b) performance of fire protection and fire restriction functions, also

c) the ventilation systems, if necessary, shall be suitable for the removal of smoke generated in case of a fire, the restoration of normal air conditions, at the same time the spreading of fire through the ventilation systems shall be prevented.

Lifting equipment

3.4.7.0500. The design of the lifting equipment and lifts shall comply with the requirements and criteria with regard to earthquake resistance, lifting, against dropping, design and testing processes.

3.4.7.0600.

3.4.7.0700. The lifting equipment affecting safety or physical barrier functions shall be designed by applying a special nuclear design standard.

3.4.7.0800. The design of the lifting equipment shall demonstrate the fulfilment of the earthquake resistance, lifting, dropping, design and trial requirements and criteria.

3.4.7.0900. The lifts affecting safety or physical barrier functions shall be designed by applying a special nuclear design standard.

3.5. RADIATION PROTECTION

3.5.1. Basic requirements

3.5.1.0100. During design the three principles of radiation protection: justification, optimization, and dose limitation shall be applied.

3.5.1.0200. When planning radiation protection controlled and supervised zones shall be designated. Room atmosphere, surface contamination, and radiation sources shall be controlled within and between zones. Appropriate equipment shall be designed and measures shall be taken to control the dispersion of radioactive contamination.

3.5.1.0300. Such work environment shall be provided by design in every area of the nuclear power plant unit where operating personnel can be present under DBC1-4 that conforms to the principle that the radiation exposure of the personnel shall be kept as low as reasonably achievable.

3.5.1.0400. When designing activities in radiation dangerous areas the radiation exposure of individuals shall be limited so that the potential combinations of radiation exposures shall not exceed either the effective dose or the equivalent dose limits of the organs and tissues.

3.5.1.0500. Protection measures shall be optimized in order to keep the individual doses, the number of exposed people and the possibility of exposure as low as reasonably achievable within the individual dose limits considering dose constraints specified for the nuclear power plant.

3.5.1.0600. Normal and potential radiation exposure shall be analysed throughout the nuclear power plant considering DBC1-4, DEC1-2 in order to estimate the radiation exposure regularly or potentially affecting the population as well as people at the site of the nuclear power plant.

3.5.1.0700. Each dose estimate shall be reasonably conservative considering the uncertainties of internal and external radiation dose calculations. Available measurements shall also be used for calculations.

3.5.1.0800. The highest annual individual dose and the average collective dose shall be described.

3.5.1.0900. The occupational radiation exposure of workers in radiation-free work positions at the site shall be determined based on evaluation of the expected maximum dose typical of the site.

3.5.1.1000. The radiation exposure of the population living around the site shall be determined based on calculated dose values which apply to the critical group and which also take into account external and internal radiation exposures from artificial sources, except radiation from medical exposure.

3.5.1.1100. Design objectives shall be established to determine the collective dose for the operating personnel based on health physics requirements – in possession of available experience.

3.5.1.1200. During the design process it shall be calculated how the operation of a given system contributes to the radiation exposure of the personnel. When estimating radiation exposure contributions from radioactive nuclides present in the air and of surrounding systems shall be taken into account.

3.5.1.1300. Radiation exposures occurring during the scheduled inspection and maintenance of a system as well as the repair and replacement of its components shall also be evaluated. Those systems that significantly contribute to the radiation exposure of operating personnel while adhering to the aimed design dose shall be identified.

3.5.1.1400. Systems, structures and components shall be designed in a way that allows for the operation of the nuclear power plant without being present or working at high radiation areas.

3.5.1.1500. Remotely controlled equipment shall be designed and constructed to handle high activity objects.

3.5.1.1600. Continuous and intermittent radiation monitoring shall be used to control the proper functioning – from a dosimetry point of view – of system components emitting radiation. The scope of radiation monitoring and the number of continuous and intermittent measurements shall be determined by considering normal and potential radiation exposure.

3.5.1.1700. The draining and air venting devices of systems, structures and system components that transport and contain radioactive materials shall be designed in a way that allow separate control of the radioactive materials.

3.5.1.1800. A dose evaluation system shall be designed for the operation of the nuclear power plant that

a) regularly provides measurement and analysis of personnel radiation exposure along with the dose evaluation system of the authority,

b) is suitable to verify that dose limits are observed at the frequency of the received dose information,

c) provides appropriate data for the optimization of radiation protection, furthermore

d) ensures prompt detection of dose limit excess.

3.5.2. Decontamination

3.5.2.0100. Decontamination options shall be provided wherever the radiation exposure of operating personnel can be reasonably decreased. The need for decontamination shall be minimized by preventing leakage of radioactive materials and by installing closed-circuit draining, deaeration and overflow pipes.

3.5.2.0200. It shall be ensured that the material, design, and construction of system components that come functionally in contact with radioactive materials or are exposed to radioactive contamination allow for decontamination and complete removal of the decontaminating solution. The decontamination process shall be designed to ensure that the surface quality of the affected system components meet the requirements even after decontamination.

3.5.2.0300. The inspection and, if required, decontamination shall be ensured of controlled areas, reusable protective clothing of the persons entering and exiting the controlled areas as well as objects exiting and entering the controlled areas.

3.5.2.0400. The licensee shall prepare for the decontamination of potentially contaminated transport containers and other packaging materials.

3.5.2.0500. Where necessary, decontamination made by remotely operated devices shall be designed.

3.5.2.0600. The place and resource needs of decontamination shall not decrease the level of nuclear safety.

3.5.2.0700. A new decontamination technology or in the case of a chemical decontamination technology a new chemical agent shall be introduced only after justified by safety analysis. The safety analysis shall contain:

a) the management method of the generated radioactive waste;

b) justification that the decontamination can be performed without dcompromising the safety functions of the facility;

c) justification that the radioactivity can be removed, including the physical and chemical properties of the contamination;

d) in the case of introduction of a new chemical decontamination technology or new chemical agent

da) justification of its use;

db) results of corrosion analysis of structural materials including demonstration by tests and the evaluation of the results.

3.5.2.0800. The decontamination process shall be optimized at least in terms of:

a) amount of secondary wastes generated;

b) radiation exposure of the personnel; and

c) effectiveness of decontamination.

3.5.2.0900. Regarding decontamination of rooms and equipment of nuclear facilities, as minimum, the planned direction of dispersion of contamination between rooms and equipment shall be taken into account together with the limitations on use of chemicals and technologies in the given room.

3.5.2.1000. For those equipment and tools, which can be safely transported, a room shall be designed for the decontamination, where the process can be performed without impact on nuclear safety.

3.5.2.1100. In the case of those rooms, where release of contaminated water can occur, decontaminable surfaces shall be designed and the dispersion of contamination shall be prevented. In these rooms, appropriate boundary surfaces and solutions to direct the dispersion shall be applied to limit the contaminated surfaces, quick drainage and collection of the discharged liquid.

3.5.2.1200. Management of the potentially dry up and contaminated surfaces shall be designed.

3.5.3. Radiological control equipment

3.5.3.0100. Appropriate equipment shall be designed to monitor radiation conditions. This equipment shall be able to provide accurate measurements under DBC1 to 4 and provide information in designated areas even under DEC1 and DEC2. The equipment shall be designed at least for the following functions:

a) to measure the dose rates of designated rooms and locations of the nuclear power plant,

b) to monitor areas regularly used by operating personnel if these areas may be restricted during certain operating conditions,

c) to indicate dose rates under DBC3-4,DEC1-2,

d) to measure isotope concentration of gas and liquid samples from technological systems and from the environment under DBC1-4, DEC1-2,

e) to regularly monitor environmental releases under DBC1-4, DEC1-2,

f) to measure radioactive surface contamination, and

g) to determine the external and internal radiation exposure as well as the surface contamination of operating personnel.

3.5.4. Biological protection

3.5.4.0100. Biological protection shall be designed at every area of the nuclear power plant unit where direct radiation or the accumulation of radiation material may be expected due to chain reaction.

3.5.4.0200. When selecting materials for biological protection, the following shall be considered:

a) characteristics of radiation,

b) shielding and mechanical properties of materials, and

c) probable ageing processes due to the environmental stresses present at the specific location.

3.5.5. Radioactive releases

3.5.5.0100. Appropriate systems shall be developed in the nuclear power plant unit for controlling gaseous and liquid radioactive materials in order to keep the release and concentration of radioactive materials below the allowed threshold values and as low as reasonably achievable. The number of release locations shall be designed to be as few as reasonably possible. Integrated control of releases shall be ensured.

3.5.5.0110. In the rooms, where such system, structure or component exists that contain radioactive liquid, the elimination of planned or unplanned spill of the liquid shall be designed.

3.5.5.0200. Terrain conditions, weather conditions, and distances of buildings and stacks shall be considered when designing positions and constructions of release

locations. Aerodynamic properties of releases and their compatibility with ongoing operations in nearby buildings shall also be considered.

3.5.5.0300. A weather station shall be designed in the proximity of the site to ensure availability of meteorological data whenever required in the extent and frequency specified in the design. Meteorological data shall be available wherever it is required for designed processes and procedures.

3.5.5.0400. To monitor the surrounding of the site the measurement of dose rates, as well as activity concentration of radioactive aerosols and iodine isotopes shall be ensured by a telemetry and sample collection network.

3.6. MANAGEMENT AND STORAGE OF NUCLEAR FUEL AND RADIOACTIVE WASTE

3.6.1. General Requirements

3.6.1.0100. The appropriate management, transport and storage of nuclear fuel and radioactive waste shall be ensured within the site of the nuclear power plant. During the design the storage, transportation, packaging and lifting requirements shall be defined.

3.6.1.0200. The storage capacity and requirements for the management and storing of nuclear fuel and radioactive waste within the plant site shall be defined in accordance with the national strategy regarding the management and final repository of spent fuel and radioactive waste and the activities related to management of radioactive wastes shall be determined in accordance with the parliament resolution on the national policy for spent fuel and radioactive waste management and the government resolution on the national programme.

3.6.1.0300. Passive safety solutions shall be applied to a reasonably achievable extent when designing on-site storage.

3.6.1.0400. During the on-site management and storage of nuclear fuel and radioactive waste equipment shall be available that provides appropriate treatment for all possible conditions of the nuclear fuel assembly and radioactive waste.

3.6.1.0500. Appropriate equipment and packaging shall be available for management of spent fuel and radioactive waste packages that show signs of deterioration.

3.6.1.0600. The systems potentially containing nuclear material or other radioactive material shall be designed to prevent uncontrolled release of radioactive material to the environment, prevent criticality and overheating, ensure that the radioactive releases are kept under the release limits, at the reasonably achievable level, and to facilitate the mitigation of radiological consequences of abnormal events.

3.6.2. Management and storage of nuclear fuel

3.6.2.0100. For fresh nuclear fuel assemblies such transportation, management, and storage systems, structures and components shall be established which:

a) prevent criticality with sufficient safety margins,

b) prevent the development of increased stress in the fuel assemblies due to management,

c) prevent the possibility to fall or other damages or impairments of the fuel assemblies,

d) ensure control inspections of the fuel assemblies,

e) provide the opportunity for removing mechanical contaminations of the fuel assemblies,

f) ensure identification of fuel assemblies at every storage site, and

g) the logistic system excludes the potential loss of a fuel assembly.

3.6.2.0150. Penetration of any liquid to the fresh fuel storage shall be prevented.

3.6.2.0200. Besides the requirements for systems, structures and components used for the management, transport, and storage of fresh fuel assemblies for systems and system components used for the management, transport, and storage of irradiated nuclear fuel the following additional requirements shall be fulfilled:

a) the removal of residual heat shall be ensured in each operational condition,

b) the fall of heavy objects onto fuel assemblies shall be prevented,

c) the visual inspection of irradiated fuel assemblies as well as the inspection and qualification of the integrity of fuel assemblies shall be ensured,

d) for fuel elements or fuel assemblies with assumed or obvious defects, a storage appropriate to their condition shall be provided,

e) it shall be prevented that the irradiated fuel assemblies become uncovered even in the case of the leakiness of the underwater storage system and the connected cooling system, and one shall be able to replace the amount of water required for heat removal.

f) decontaminability of the fuel management and storage areas shall be ensured,

g) appropriate concentration of the solved neutron absorber shall be ensured, and

h) maintenance and dismantling of the fuel assembly moving and storage devices shall be ensured.

3.6.2.0210. The availability of an external water source required for the alternative cooling of the spent fuel pool and the equipment and technologies used for setting the appropriate boric acid concentration shall be ensured.

3.6.2.0300. When determining required storage capacity for irradiated fuel assemblies, it shall be ensured that the necessary amount of fuel assemblies can be unloaded from the nuclear reactor in accordance with the procedure of planned management of fuel assemblies in the nuclear reactor.

3.6.2.0400. The designer shall verify the mechanical and chemical compatibility of the applied nuclear fuel and the systems and system components of the nuclear power plant designed for their control.

3.6.2.0500. In the DBC1-4 of the spent fuel pool, the following shall be provided:

a) inspection of irradiated fuel assemblies as required,

b) equipment for the water chemistry and radiological monitoring of the storage media,

c) water purification, leak collector and leak monitoring systems, as well as

d) control and monitoring systems for the level and temperature of the storage pool.

3.6.3. Management and storage of radioactive waste

3.6.3.0100. Systems, structures, system components, and procedures shall be designed for the management and on-site storage of radioactive waste.

3.6.3.0200. Complex waste management documentation shall be composed to regulate and control the path of radioactive materials.

3.6.3.0300. Systems managing radioactive waste and the applied processes shall be designed to ensure that the waste as an end-product fulfil the requirements for transport, interim storage, as well as, if known, the consignment criteria for final repository.

3.6.3.0400. For efficient waste management, radioactive waste shall be classified and separated according to the states of matter. In the determination of classification aspects the requirement to keep the amount of waste at a minimum shall be considered. Further aspects shall include half-life, physical and chemical properties, radionuclide composition, activity concentration and volume.

3.6.3.0500. The representative isotope content and activity of radioactive waste shall be determined by nuclide specific measurements; in case of radionuclides that are difficult to measure it shall be determined theoretically. The generated radioactive waste shall be classified.

3.6.3.0600. Liquid radioactive waste shall be classified based on activity concentration. Their physical and chemical properties shall be considered during processing. Storage tanks and containers shall have suitable ventilation, pressure relief option, and equipment for collecting leakage.

3.6.3.0700. Storage shall be designed at the power plant in a way that waste packages can be controlled and recovered if needed.

3.6.3.0800. In the determination of storage capacity it shall be considered to provide appropriate reserves that can ensure additional capacity for unanticipated events.

3.6.3.0900. The container types used for interim storage and final disposal of radioactive wastes shall ensure the isolation of the radioactive waste from the environment for a specified storage duration.

3.6.3.1000. Management of radioactive wastes needing special treatment, especially radioactive waste containing considerable amount of alpha emitters, furthermore flammable, explosive, corrosive, toxic and other dangerous materials, shall be designed.

3.6.3./A. Management of airborne radioactive wastes

3.6.3.1100. Systems, structures and components suitable for the management of airborne radioactive wastes shall be designed to comply with the respective limits and keep the releases at a minimum.

3.6.3.1200. Volatile radioactive wastes shall be removed from the gaseous radioactive wastes to the extent reasonably achievable.

3.6.3.1300. Measures shall be designed to avoid the generation of flammable or explosive compounds or to remove them.

3.6.3./B. Management of liquid radioactive wastes

3.6.3.1400. In the design of liquid radioactive waste processing systems the composition and properties of the liquid shall be taken into account.

3.6.3.1500. The different type of wastes shall be appropriately separated and the most effective method of processing shall be selected to achieve the principal of justification.

3.6.3.1600. Matrix materials suitable for waste conditioning and appropriate barrels and containers shall be designed.

3.6.3.1700. Appropriate tank capacity shall be available for the storage of radioactive media to keep the environmental release at a minimum.

3.6.3./C. Management of solid radioactive wastes

3.6.3.1800. Suitable waste management procedures shall be designed in line with the principal of keep the wastes at a minimum.

3.6.3.1900. In the case of mobile conditioning equipment, measures shall be designed to avoid spread of contamination.

3.7. DESIGN OF ON-SITE NUCLEAR EMERGENCY RESPONSE

3.7.1.0100. The nuclear emergency response procedures shall be designed based on the analysis results of DBC4 and DEC1-2, taking into account that these operating conditions may occur in all reactors and nuclear facilities of the given site at the same time. The scope of the analysis shall provide sufficient information to define nuclear emergency response actions.

3.7.1.0200. The hazard sources identified during design shall be included in emergency design categories based on their potential severity. Among hazard sources, risk factors indirectly associated with the nuclear reactor shall also be taken into account, in particular, accident situations relating to the handling of spent fuel, spent fuel pools, the management of radioactive wastes and radioactive sources used on the site, as well as off-site risk factors, in particular, the potential severe and very severe accident situations of a nuclear facility close to the site. During preparation the ability to eliminate the most severe emergency situation defined by analyses shall be achieved. It shall be demonstrated that the preparation ensures in every postulated initiating event and possible emergency situation the timely execution of appropriate response actions – classification, notification, activation and nuclear emergency response measures.

3.7.1.0300. An emergency command centre shall be established for the personnel participating in emergency response. Sufficient instrumentation and tools shall be available for the management of necessary actions during the emergency situation, and for the communication with the locations and on-site and off-site organisations responsible for nuclear emergency response.

3.7.1.0400. The emergency command centre shall be supplied with a redundant and diverse communication systems that are suitable to alert the on-site and off-site organisational units responsible for nuclear emergency response and the off-site nuclear emergency response organisations as well as to communicate with the main and backup control rooms, other important locations of the nuclear power plant and off-site nuclear emergency preparedness and response organisations.

3.7.1.0500. Personnel in the emergency control centre shall be protected against the circumstances of the emergency situation. The option to check the functioning of the emergency control centre shall be ensured. The emergency control centre shall be located that it can be accessed in the postulated emergency situations. Should the use of the emergency control centre become impossible a reserve emergency control centre shall be established at a sufficient distance from the nuclear power plant, which fulfils the requirements for emergency control centres.

3.7.1.0600. A local alarm system shall be installed which is suitable to alarm all people on the site. In order to execute emergency preparedness tasks safe escape routes shall be established which are simply, understandably and durably signalled and reliably lit and the other necessary conditions to safely use these routes shall be provided. Escape routes shall be designed to fulfil the requirements of industrial safety, radiation protection, fire protection and security.

3.7.1.0700. Shelters shall be installed for personnel participating in nuclear emergency response which conform to the regulations of civil protection and the number of people involved in the nuclear emergency response activities.

3.7.1.0800. When equipment required for nuclear emergency response is designed, the need to perform justified work in highly radioactive areas and the indispensible, related on-site transporting shall be taken into account.

3.7.1.0900. Systems, structures and components required for managing emergencies shall be designed in such a way that they are operable and fulfil their functions even in the long run in all operating conditions, including DEC1-2.

3.7.1.1000. If emergency response includes the use of mobile equipment, then fixed connection points shall be established, which can also be used in DEC1 and 2 from physical and radiological points of view.