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/A to Government Decree No. 118/2011 (VII.11.)

Nuclear Safety Code

Volume 3a

Design requirements for new nuclear power plant units

3a.1. INTRODUCTION

3a.1.1 Scope of the Code

3a.1.1.0100. The purpose of the Code is to set design principles and design requirements for the nuclear power plant as a nuclear facility and the systems, structures and components comprising it, which are important to nuclear safety.

3a.1.1.0200. The provisions of this Code shall apply to setting the design requirements for nuclear power plant units defined in Item 161 of Volume 10, provided with water cooling and operating with thermal reactors, to be constructed in the territory of Hungary.

3a.2. GENERAL DESIGN REQUIREMENTS

3a.2.1 Basic design requirements

3a.2.1.0100. The licensee shall operate such a management system that regulates the complex process of design guarantees the quality of and harmony between the designs and the fulfilment of the nuclear safety requirements.

3a.2.1.0200. The compliance of the designs, including the means of design, the design data and the results, shall be subjected to review by an organisation independent of the designer.

3a.2.1.0300. The design process shall be specified in the early stage of design through the identification of all design requirements. The designer’s specifications and tasks required for meeting the requirements shall be determined in detail on the basis of the identified requirements.

3a.2.1.0400. The design of the nuclear power plant can be carried out only by such a design organisation that holds qualifications valid for the special design area as specified by law or, in the absence thereof, specified by the licensee and is entitled to perform such activities.

3a.2.1.0500. The licensee can also charge a design organisation with coordination of the design verification and design management tasks of the nuclear power plant.

3a.2.1.0600. The licensee shall ensure that the level of detail and elaboration of the designs corresponds at least to the scope required for carrying out the regulatory licensing procedures associated with the given life cycle stage.

3a.2.1.0700. The design basis for systems, structures and components important to nuclear safety shall be specified and documented systematically. The technical requirements shall be laid down in the design specifications.

3a.2.1.0800. It shall be ensured that the licensee possesses all design information required for maintaining its responsibility for the safe operation of the nuclear power plant. The licensee shall be able to perform or ensure the performance of activities aimed at the safety of the nuclear power plant and to make decisions on safety throughout the lifetime of the nuclear power plant.

3a.2.1.0900. It shall be ensured that in the case of systems, structures and components of the nuclear power plant, the demonstration of the fulfilment of the basic design requirements can be verified.

3a.2.1.0910. In the case of programmable systems, unless otherwise provided by the given requirement, the requirements for the systems, structures and components shall be related to the combination of the hardware and software participating in the performance of the function fulfilled.

I. Provision of the fundamental safety functions

3a.2.1.1000. The fundamental safety functions shall be fulfilled in the case of DBC1 to 4. After a DEC1 plant state, the fundamental safety functions shall be fulfilled to the extent required for bringing the nuclear reactor in a controlled, safe shutdown condition, while after a DEC2 plant state of the power plant, to the extent required for bringing it in a safe condition after a severe accident.

3a.2.1.1100. Systems shall be designed for the fulfilment of the fundamental safety functions.

3a.2.1.1200. In order to fulfil the fundamental safety functions, all safety functions and the systems, structures and components fulfilling them shall be identified for all operating conditions, including normal operation, by safety and other analyses.

3a.2.1.1300. It shall be ensured that the residual heat is transferred to the ultimate heat sink in such a way that the frequency of the loss of the heat removal function should be lower than 10^{-7}/year.

II. Application of the defence in depth principle principle

3a.2.1.1400. It shall be ensured with independent protection levels that possible failures and abnormal operation can be detected, compensated and managed. In addition to the requirements under Section 7, the supplementary requirements specified in Sections 3a.2.1.1500 to 3a.2.1.2000 shall be met during the application of the five levels of defence in depth.

3a.2.1.1500. During design, multiple physical barriers shall be applied for preventing an uncontrolled release of radioactive materials into the environment.

3a.2.1.1600. In order to apply the defence in depth principle, the following four physical barriers shall be distinguished:

a) fuel matrix;

b) fuel element cladding;

c) boundary of the primary circuit of the reactor;

d) containment system.

3a.2.1.1700. The protection of the barriers shall be ensured. The fulfilment of the safety functions and the acceptance criteria shall be ensured by design solutions even in the case of damage to any level of protection.

3a.2.1.1800. During the design of the nuclear power plant, in harmony with the defence in depth principle:

a) it shall be ensured by design solutions that the fundamental safety functions can be achieved by the maintenance of the barriers and the mitigation of the consequences of failures or deviations from the normal operating condition;

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

c) it shall be ensured that the adverse consequences of human error occurring during operation or maintenance are avoided,

d) the manageability of the condition of the nuclear power plant shall be ensured by technical means in such a way that in the case of failures or deviations from the normal operating condition, the need for the systems performing the safety function should be the lowest possible; and

e) it shall be ensured that the manageability of the condition of the nuclear power plant is highly reliable even in conditions requiring the operation of systems performing safety functions, and does not require intervention by the operating personnel at an early stage of the process.

3a.2.1.1900. The levels of defence in depth shall be established by taking into account the following:

A	B	C	D	E
Level of defence in depth	Objective	Means to be applied	Radiological consequences	Relevant operating state / condition
1.	Deviations from the normal operating condition and prevention of failures	Conservative design, implementation and operation to a high standard; maintaining the main operating parameters between the prescribed limits	No off-site radiological effects exceeding the regulatory limits	Normal operation (DBC1)
2.	Management of deviations from the normal operating condition and failures	Control and safety protection systems; other surveillance methods		Anticipated operational occurrences (DBC2)
3. 3.a.	Management of design basis accidents in order to limit radioactive releases and to	Safety systems, emergency operating procedures	No or only minimum off-site radiological effects	Design basis accident (DBC3-4)
3.b.	prevent fuel melting	Added safety features for the elimination of complex accidents, emergency operating procedures, on-site emergency response measures		Complex accidents (Postulation of multiple failures) (DEC1)
4.	A practical elimination of large or early releases, management of severe accidents involving a fuel melting in order to limit off-site releases	Supplementary safety features to limit fuel melting, accident management guidelines, on-site emergency response measures	An off-site radiological effect may warrant the introduction of protective measures limited in space and time for the population	Severe accident (DEC2)
5.	Mitigation of radiological	On- and off-site emergency	An off-site radiological effect	Very severe accident

	consequences of a significant release of radioactive materials	response measures; intervention levels	warrants protective measures for the population	

3a.2.1.2000. The following shall be ensured to the extent reasonably practicable:

a) prevention of events jeopardising the integrity of barriers and toleration of hazard factors;

b) avoidance of the failure of more than one barrier at the same time;

c) avoidance of the failure of one barrier as a result of the defect of another barrier or other system components;

d) the design of the barriers shall be conservative, and they shall be implemented to high quality norms in order for

da) the possibility of failures and deviations from the normal operating condition to be as low as reasonably achievable,

db) DBC3-4 and DEC plant states shall be excluded at a reasonably achievable level, and

dc) the cliff edge effect to be avoided.

III. Other general design requirements

3a.2.1.2100. Systems, structures and components providing safety functions shall be so designed that the safety functions are performed as reliably throughout the lifetime as required in the design.

3a.2.1.2200. In the designs, sufficient margins shall be provided for the errors of design methods and means, the manufacturing and installation tolerances, uncertainties, assumed failures and for the conservatively estimated rate of degradation processes caused by ageing mechanisms occurring during the design lifetime.

3a.2.1.2300. Systems, structures and components important to safety shall be designed by applying standards adopted in the nuclear industry. The group of standards to be used in the design process shall be preliminarily defined, and their applicability shall be demonstrated.

3a.2.1.2400. Systems, structures and components important to safety shall be designed by using design methods that have been previously tried and proven under similar conditions. In other cases, such technologies and products shall be used, the applicability of which has been examined and demonstrated. In the case of new design solutions, which differ from well-established solutions in engineering practices, the applicability shall be demonstrated from a safety point

of view by appropriate research, tests and analysis of experience from other applications. New solutions shall be tested before commissioning. The operation of systems, structures and components shall be monitored during their operation for confirming the demonstration of suitability.

3a.2.1.2410. It shall be demonstrated that the component important to nuclear safety is error-free and that the in-service inspections and tests applied are suitable to detect the possible failures, and the so detected failure can be managed.

3a.2.1.2500. A marking system, which clearly identifies locations within the system technology, shall be implemented to identify systems, structures and components.

3a.2.1.2600. During design, the experience accumulated during the design, implementation and operation of nuclear power plants and relevant research results shall be taken into account.

3a.2.1.2700. During design, the safety analysis methods defined in this Decree shall be applied from the early stage of design.

3a.2.1.2710. The safety analysis shall demonstrate that the defence-in-depth concept is taken into account in the design of the plant.

3a.2.1.2800. Systems, structures and components shall be so designed that the possibility of fabrication, installation, construction, inspection, maintenance and repair can be ensured.

3a.2.1.2900. During design, the possibility of decommissioning of the nuclear power plant shall be ensured, which shall be carried out by minimising the activation, providing for decontaminability, providing accessibility and taking into account the controllability of decommissioning.

3a.2.1.3000. The nuclear safety, physical protection and safeguards requirements shall be implemented in an integrated manner and by taking into account interactions.

3a.2.1.3100. In the case of a nuclear power plant with more than one unit, the independence of the units shall be ensured to the reasonable extent.

3a.2.2. Design basis for safety

I. Categorisation of nuclear power plant conditions and events

3a.2.2.0100. Conditions that deviate from normal operation shall be divided into design basis and design extension condition categories.

3a.2.2.0200. Based on their frequencies, normal operating conditions as well as the events leading to the conditions considered in the nuclear power plant design

basis shall be assigned to the operating conditions listed in the following table. The frequencies of events leading to the various conditions shall be demonstrated by analyses.

	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.	DBC3	low frequency design basis accidents	$10^{-2} > f \geq 10^{-4}$
5.	DBC4	very low frequency design basis accidents	$10^{-4} > f \geq 10^{-6}$

3a.2.2.0300. Two categories of the extended design basis shall be distinguished:

a) complex accident (DEC1), or,

b) severe accident(DEC2).

3a.2.2.0400. It shall be demonstrated by probabilistic safety analyses for every design basis accidents that the multiplication product of the frequency of a given initiating event and the probability of failure of any safety function required for meeting the acceptance criteria for DBC4 during a transient caused by the given initiating event does not exceed 10^{-6}/year.

II. Safety classification

3a.2.2.0500. An importance analysis shall be carried out for the functions specified on the basis of the requirement under Section 3a.2.1.1200 by taking into account the following:

a) consequence of failing to achieve the safety function,

b) consequence of inadvertent operation of the safety function,

c) frequency of initiating events requiring the implementation of the safety function,

d) the role of the safety function in ensuring a controlled or safe condition.

The analyses shall be primarily based on deterministic methods, complemented with probabilistic methods and engineering jusdgement.

3a.2.2.0600. In the process of classifying the safety functions into levels, it shall be identified to which of the levels of the defence in depth the given function can be assigned, primarily in order to allow an evaluation of the independence of the levels of defence.

3a.2.2.0700. Safety functions shall be assigned to safety levels as follows:

a) The safety functions that are required to bring the nuclear power plant unit from DBC2-4 to a controlled condition shall be assigned to Level F1A;

b) The following safety functions shall be assigned to Level F1B:

ba) those that are required to bring the nuclear power plant unit from DBC2-4 to a safe shutdown condition and to maintain that safe shutdown condition for at least 24 hours,

bb) the functions that replace the F1A functions after these functions fail and help maintaining it beyond DBC in DEC1 plant state and

bc) all normal operation functions that, if lost, may directly result in DBC3 or 4.

c) The following functions shall be assigned to Level F2:

ca) the safety functions that are required after DBC2-4 to maintain the safe shutdown condition of the nuclear power plant unit for at least 72 hours after the initial 24 hours,

cb) safety functions taken into account in the extended design basis, and those that provide information in such operating conditions, except those that belong to Subitem *bb)*,

cc) safety functions that serve avoiding accident not related to the active core of the nuclear reactor.

cd) all normal operation functions that, if lost, may result in a DBC2 and, directly, in a reactor protection operation.

3a.2.2.0710. Systems, structures and components (including passive design solutions and physical barriers) arising from basic design solutions, the reliable operation of which in normal operation affects nuclear safety, shall be identified primarily by deterministic methods, supplemented with probabilistic methods and engineering judgement. They shall be categorized in a safety class directly on the basis of their nuclear safety importance, without assigning them to safety functions.

3a.2.2.0800. The functions of physical barriers shall be assigned to levels in accordance with Sections 3a.2.2.0900 to 3a.2.2.1100 on the basis of the activity retained by the barrier and the possibility of isolation of the barrier.

3a.2.2.0900. Barriers that cannot be isolated and that retain potentially highly contaminated media and the failure of which may result in a significant release of radioactive materials shall be assigned to Level B1. Fuel rod cladding, the pressure boundary of the primary circuit and the containment shall belong to this level.

3a.2.2.1000. Barriers that can be isolated and retain potentially highly contaminated media or barriers that cannot be isolated but retain mildly contaminated media shall be assigned to Level B2. Secondary circuit steam and water loops as well as system components containing the release of radioactive materials following an accident shall belong to this level.

3a.2.2.1100. Barriers that can be isolated and retain mildly contaminated media shall be assigned to Level B3. System components containing radioactive materials during normal operation as well as systems of the containment important to nuclear safety, which are not directly connected to the cooling circuit of the nuclear reactor or the atmosphere of the containment during normal operation or accidents, shall belong to this level.

3a.2.2.1200. In accordance with Sections 3a.2.2.1300 to 3a.2.2.2300., the systems, structures and components of the nuclear power plant shall be included in safety classes and a non-safety class on the basis of their effects on safety and their highest level safety function and the basic design solutions based on the consequences of their failure.

3a.2.2.1300. The following shall be included in Safety Class ABOS 1:

a)

b) those of the systems, structures and components fulfilling F1A functions, for which, in the case of the failure of the function, the importance analysis under Section 3a.2.2.0500 shows a serious consequence, i.e. the release limits exceed the values specified for the design basis or the values of the main physical parameters exceed the acceptance criteria for the design basis.

c) the Level B1, unisolatable barriers, and other components identified based on Section 3a.2.2.0710, the failure or defect of which may lead to an event

ca) that cause exceedance of release values specified for DBC4, or

cb) the primary circuit parameters of which exceeds the relevant acceptance criteria for DBC4.

3a.2.2.1400. The following systems, structures and components shall be included in Safety Class ABOS 2:

a) those that provide Level F1 safety functions and were not included in Safety Class ABOS 1,

b) those of the systems fulfilling a function under Section 3a.2.2.0700 *c) ca)*, for which, in the case of failure of the function, the importance analysis under Section 3a.2.2.0500 shows a serious consequence, i.e. the release limits exceed the values specified for the design basis, and the values of the main physical parameters exceed the acceptance criteria for the design basis,

c)

d) those that provide subcriticality, integrity and appropriate cooling for the fresh and irradiated fuel elements stored outside of the cooling system of the nuclear reactor, or

e) the Level B2 isolatable barriers, and other components identified on the basis of Section 3a.2.2.0710, the failure or defect of which in DBC1 leads to a DBC3 or 4 on the basis of acceptance criteria and where the radiological and dose limits exceed those set for DBC2.

3a.2.2.1500. The following systems, structures and components shall be included in Safety Class ABOS 3:

a) those that provide a Level B3 isolation function,

b) those that implement F2 safety functions and were not included in Safety Class ABOS 2,

c) those that play a role in preventing DBC3-4, and if their possible inoperability during a DBC3 or 4, will not influence the course of the accident,

d) those that ensure that radiation sources outside the nuclear reactor do not cause excess radiation exposure for the persons present on the site of the nuclear power plant and the population,

e) those that, through their operation, prevent the necessity to activate systems included in Safety Class ABOS 1 or 2,

f) those that, if inoperable, hinder the monitoring of the operation of the technology within its safe parameter range or the storage of such information, or

g) the components providing B3 isolation function, and

other components identified on the basis of Section 3a.2.2.0710, the failure or defect of which in DBC1 leads to a DBC3 or 4, and the radiological and dose limits do not exceed those set for DBC2.

h)

3a.2.2.1600. All systems, structures and components that do not have a safety function and is not a basic design solution shall be categorized into Non-safety Class ABOS 4.

3a.2.2.1700. The systems, structures and components identified on the basis of Section 3a.2.2.0710, the failure of which affects the boundary conditions of the risk analysis and the analysis of external hazard factors, in particular, fire area or inundation boundaries shall be categorized into at least Safety Class ABOS 3.

3a.2.2.1800. Systems providing sufficient and reliable information to those participating in DEC1-2 accident situations, including monitoring and emergency response communications systems, shall be categorized into safety classes.

3a.2.2.1900. Methods substantiated by safety analyses and using operating experiences shall be applied for categorization of passive systems into safety classes.

3a.2.2.2000. The systems, structures and components, classified on the basis what said above, shall be analysed in detail in order to allow the identification of the subsystems (including instrumentation and control and energy supply subsystems), structural components and parts that affect or do not affect or jeopardise the implementation of the safety function serving as a basis for the classification of the given system, structure or component.

3a.2.2.2100. The auxiliary systems of systems included in safety classes shall be considered as part of the basic system, and shall be included in the safety classes accordingly. The requirements regarding reliability, redundancy, diversity, independence, and separability for testing, which are defined for the relevant basic system, shall be applied to these auxiliary systems.

3a.2.2.2200. During the integrated application of classification according to various considerations, the safety functions required for averting the individual external and internal hazard factors and their reasonable combinations shall be identified, and the safety functions shall be assigned to levels depending on potential on- and off-site effects.

3a.2.2.2300. During and following an event triggered by hazard factors of external and internal origin, in particular, fire, flooding, earthquake, electromagnetic interference and air pollution, it shall be ensured that the nuclear power plant remains under control and, if necessary, is brought to a safe shutdown condition. The systems, structures and components shall also be classified according to their ability to resist hazard factors of external and internal origin, but at least regarding seismic safety, and appropriate and graded requirements shall be applied during design on the basis of Section 3a.3.6.

3a.2.2.2400. The systems, structures and components ensuring the implementation of the safety functions shall be included in the given environmental resistance class in accordance with Sections 3a.2.2.2600 to 3a.2.2.2900.

3a.2.2.2500. Connections shall be established between the classifications of the systems, structures and components according to the various considerations, and the relationships taken into account in them and the methodology applied shall be shown.

3a.2.2.2600. Class 1 shall include systems, structures and components that have active (F1A, F1B and F2) safety functions to protect against a given internal or external hazard factor and manage its potential consequences.

3a.2.2.2700. Class 2 shall include systems, structures and components that takes part in the protection against a given external or internal hazard factor and management of its potential consequences in a passive way.

3a.2.2.2800. Class 3 shall include systems, structures and components that do not have a safety function and is not a physical barrier, but may jeopardise the function of a system, structure or component important to nuclear safety.

3a.2.2.2900. Class 4 shall include all systems, structures and components of the nuclear power plant that are not included in Classes 1, 2 or 3 as specified above. They shall be designed against the effects of external and internal hazard factors in accordance with general industry standards.

3a.2.2.3000. Standards and technical specifications corresponding to the safety class of the system component shall be applied during design.

3a.2.2.3100. Design requirements based on national and international standards and proven engineering practices shall be assigned to the safety classes of systems, structures and components and they shall be applied consistently.

3a.2.2.3200. The process of safety classification applied during design shall be documented in full detail in order to allow the results to be verified by independent reviews.

3a.2.2.3300. Safety classification is an iterative process, which shall be carried out during design and throughout the lifetime of the power plant at specific intervals and shall be repeated if warranted by modifications.

3a.2.2.3400. The classification of systems, structures and components shall be based primarily on deterministic methods, supplemented with probabilistic methods and engineering judgement.

III. The design basis of the nuclear power plant

3a.2.2.3500. For the design, all postulated initiating events that may influence the safety of the nuclear power plant shall be identified. The ones of these events to be incorporated into the design basis shall be selected by a deterministic method or the combination of deterministic and probabilistic methods.

3a.2.2.3600. In the design basis of the nuclear power plant, the performance parameters and functional and reliability characteristics, which are required to fulfil the prescribed criteria even under circumstances caused by external or internal hazard factors, shall be determined for all operating conditions of the nuclear power plant.

3a.2.2.3700. When defining the design basis, reasonably conservative assumptions shall be applied to compensate for uncertainties.

3a.2.2.3800. For each operating condition of the nuclear power plant, design limits shall be specified for the fundamental physical parameters of the systems, structures and components important to nuclear safety. The design limits shall be consistent with the nuclear safety requirements and the applied standards.

3a.2.2.3900. Boundary conditions and design requirements applicable to systems, structures and components important to nuclear safety shall be derived from initiating events resulting in DBC2- 4 and DEC1-2 or from the conditions under which they have to fulfil their functions.

3a.2.2.4000. Among the assumed initiating events, all events listed below shall be considered:

a) those related to the site of the nuclear power plant and its surroundings and are of natural origin,

b) those that are the consequences of intentional human actions not purposefully directed against the nuclear power plant or of inadvertent on- or off-site human actions;

c) technological failures resulting from the operation of the nuclear power plant or the failure of its systems, structures and components, or

d) those resulting from human error.

3a.2.2.4100. All events that may have radiological consequences and cannot be excluded on the basis of Section 3a.2.2.5000 shall form part of the design basis. The assumed initiating events that occur during low power state or when the nuclear reactor is shut down and dismantled shall also belong hereto. Such possible events taking place outside of the nuclear reactor shall also be considered as part of the design basis.

3a.2.2.4200. During the design of the nuclear power plant, all possible external and internal hazard factors shall be determined.

3a.2.2.4300. Of the external hazard factors, at least the following shall be taken into account:

a) extreme wind load,

b) extreme external temperatures,

c) extreme precipitation conditions,

d) lightning,

e) icy and ice-free floods and low water level,

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

g) flying objects moved by wind,

h) extreme cooling water temperatures and icing,

i) geological conditions taken into account for the verification of the geological suitability of the site (in particular, earthquake and soil liquefaction),

j) crash of a military or civilian aircraft,

k) transport, industrial and mining activities near the site,

l) disturbances in the connecting external electric grid, including its lasting and total inoperability,

m) facilities on the site or within its vicinity, which may cause fire, explosion or other hazards to the nuclear power plant,

n) external fire,

o) electromagnetic interference, and

p) biohazards.

3a.2.2.4400. Those of the external hazard factors that belong to the design basis shall be selected on the basis of a site-specific risk assessment.

3a.2.2.4500. Among the various DBC1-4, at least the following internal events shall be taken into account in the design of the nuclear power plant:

a) normal operating conditions belonging to DBC1;

aa) operation at full power,

ab) uploading process,

ac) hot standby condition,

ad) hot shutdown condition,

ae) cold shutdown condition,

af) refuelling condition,

ag) operation with a disconnected loop, if allowed,

ah) test conditions.

b) anticipated operational transients belonging to DBC1 operating condition:

ba) increase or decrease in temperature at a rate allowed by the Operational Limits and Conditions,

bb) abrupt increase or decrease in load to an extent allowed by the Operational Limits and Conditions,

bc) increase or decrease in load at a rate allowed by the Operational Limits and Conditions,

bd) switchover to island operation with house load,

be) overvoltage or losses of consumers caused by the instability of the electric grid, switchovers, oscillations reaching operational limits,

bf) operation under the limiting conditions allowed by the Operational Limits and Conditions,

c) DBC2 operating conditions:

ca) inadvertent movement of the control rod assembly with a subcritical reactor,

cb) inadvertent movement of the control rod assembly with operation at full power,

cc) incorrect positioning of control rod assemblies or rod groups,

cd) inadvertent dilution of boric acid,

ce) partial decrease of the primary flow rate of the coolant,

cf) inadvertent closing of the main steam isolation valves;

cg) total loss of load or turbine failure,

ch) loss of the main feedwater flow of the steam generator,

ci) uncontrolled decrease or increase of the main steam flow rate,

cj) failure of the main feedwater system of the steam generator,

ck) loss of off-site voltage for less than 2 hours,

cl) turbine overload,

cm) temporary pressure decrease in the primary cooling loop,

cn) pressure decrease in the secondary circuit caused by inadvertent opening of the safety valve of the steam generator or another single failure,

co) unjustified startup of the emergency core cooling system,

cp) failure of the primary circuit chemical and volume control system,

cq) slight loss of coolant, in particular, the rupture of a pulse line,

cr) loss of the primary ultimate heat sink,

d) DBC3 plant states:

da) loss of coolant in the primary circuit, in particular, a small pipe break,

db) small pipe break in the secondary circuit,

dc) forced reduction of the coolant flow,

dd) placing a fuel assembly in an incorrect position,

de) pulling out a control rod assembly in operation at full power,

df) unjustified operation of the safety valve of the pressurizer,

dg) rupture of the volume control tank,

dh) rupture of a tank for retaining gaseous wastes,

di) rupture of a liquid waste collection tank,

dj) rupture of one steam generator tube or a pipe connected to the primary cooling circuit of the nuclear reactor that is partially outside of the containment, or damage to a heat exchanger tube, without a preliminary iodine peak,

dk) loss of off-site voltage for 72 hours,

dl) instability of the active core,

dm) delayed intervention by systems fulfilling a reactor shutdown function required during DBC2 plant states,

e) DBC4 plant states:

ea) rupture of the main steam pipeline,

ea) rupture of the main feedwater pipeline,

ec) sticking of the main circulating pump,

ed) ejection of any control rod assembly,

ee) loss of coolant in the primary circuit, including the rupture of the largest diameter pipeline of the primary circuit with a discharge through 200% of the cross-section,

ef) accident related to the handling, moving and storage of nuclear fuel;

eg) rupture of a steam generator tube with a preliminary iodine peak,

eh) rupture of more than one steam generator pipe or lift-off of the primary collector.

3a.2.2.4600. The events listed in Section 3a.2.2.4500 may be transferred to another category if it can be demonstrated by appropriate safety analyses that this is warranted on the basis of their calculated frequencies of occurrence. It shall be ensured by comprehensive design solutions that the frequencies of occurrence of all events remain at the lowest reasonably achievable level. Furthermore, irrespective of the classification based on the frequency of occurrence, efforts shall be made to meet the most stringent acceptance criteria reasonably achievable for all events.

3a.2.2.4700. In addition to the events listed in Section 3a.2.2.4500, the following event groups shall also be examined within the DBC3-4, and the criteria corresponding to the frequencies of the initiating events shall be applied to the consequences of the specific initiating events associated with them:

q) dropping of a heavy load when using hoisting machinery,

b) effects of fire, explosion and internal flooding, and the initiating events triggered by them, and

c) processes potentially triggering secondary consequences, in particular, missiles, including dislodged turbine parts, release of dangerous medium from failed systems, vibration, whipping of a broken pipe and jet impact.

3a.2.2.4800. All realistic combinations of the individual events shall be considered during design, including events of external and internal origin, which may lead to DBC2-4. The event combinations to be taken into account in the design shall be selected by taking into account both engineering judgement and probabilistic analyses.

3a.2.2.4900. During design, the expected extent and duration of the effects of the external and internal events to be taken into account on the concerned systems, structures and components shall be determined.

3a.2.2.5000. The following can be excluded from the scope of assumed initiating events:

a) internal initiating events occurring due to the failure of systems, structures or components or human error or both if their frequencies are less than 10^{-6}/year;

b) a hazard factor resulting from external human activities characteristic to the site, the frequency of which is less than 10^{-7}/year, or if the hazard factor is at a distance that it can be demonstrated that it is not expected to have an effect on the nuclear power plant unit; and

c) all initiating events triggered by an external hazard factor of natural origin with a frequency of less than 10^{-5}/year, or such an external hazard factor of

natural origin that is demonstrated as being not able to physically endanger the power plant.

3a.2.2.5100. All hazard factors of natural origin, which cannot be excluded on the basis of the above screening criteria, shall also be examined by deterministic and, as far as the state of the art allows, probabilistic methods, too. The analysis shall take into account all available, validated data and, as far as possible, shall establish a relationship between the severity of the hazard factors, in particular, their magnitude and duration, and the frequency of their occurrence. As far as possible, the maximum severity of the hazard factors, which still has a well-founded extent, shall be determined.

3a.2.2.5200. During the analysis of external hazard factors:

a) all relevant site and regional data shall be taken into account. Special attention shall be paid to historic data,

b) special attention shall be paid to hazard factors that may vary over time,

c) the acceptability of the methods and assumptions applied shall be demonstrated, and uncertainties affecting the results shall be estimated.

3a.2.2.5300. If the frequency of occurrence of a hazard factor of natural origin cannot be determined with an acceptably low uncertainty, an event for which the same level of safety is demonstrated shall be selected.

3a.2.2.5400. The stability and changes of external hazard factors affecting the nuclear safety of the nuclear power plant units shall be forecast for their whole lifetime, and this forecast value shall also be taken into account in the design basis. In the case of hazard factors changing over time, the least favourable one shall be taken into account.

3a.2.2.5500. In the case of a nuclear power plant with more than one unit, it shall be taken into account in the design of the entire nuclear power plant and the units that some external hazard factors may affect all units of the nuclear power plant simultaneously.

3a.2.2.5600. In the case of a nuclear power plant with more than one unit, the possibility of a common cause failure of safety systems used by the units, which have the same intended purpose, type and operation, shall be examined during design.

3a.2.2.5700. The failure of safety systems jointly applied by more than one unit and their simultaneous effect on nuclear safety of the individual units shall be examined.

3a.2.2.5800. In the case of a site, where several nuclear power plant units operate, or in the vicinity of which another nuclear facility operates, the effect of

the units and facilities on each other in all operating conditions of the facilities as well as under all circumstances resulting from all assumable hazard factors shall be analysed. For the analysis of the interactions, the implementation, commissioning and decommissioning life cycle phases shall also be taken into account.

3a.2.2.5900. It shall be ensured by design solutions that following DBC2-4, the nuclear power plant unit reaches a controlled condition, then a safe shutdown condition as soon as reasonably possible. A controlled condition shall be achieved within 24 hours, at the latest, and a safe shutdown condition shall be achieved within 72 hours, at the latest.

IV. Extension of the design basis

3a.2.2.6000. In harmony with the defence in depth principle, events and event combinations resulting in DEC plant states shall be selected by deterministic analyses supplemented by probabilistic methods and engineering judgement. It shall be demonstrated that all possible events and event combinations have been taken into account. The one out of the methods that corresponds the most to the case reviewed or their most appropriate combination shall be applied for the analysis used for the demonstration of safety.

3a.2.2.6100. During the analysis of DEC1 plant state, in order to compensate for uncertainties, either reasonably conservative assumptions shall be applied or the best estimate method and data shall be used, supplemented with the necessary uncertainty and sensitivity analyses.

3a.2.2.6200. The analysis of DEC2 plant state can be carried out for the median values of effects, stresses and material properties.

3a.2.2.6300. For the extension of the design basis, the following shall at least be taken into account if they are not included in the design basis and if they are applicable for the given power plant type:

a) station blackout,

b) loss of systems performing reactor shutdown functions required under DBC2-4,

c) rupture of a steam pipeline with additional damage to the heat exchange 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 with the total loss of an emergency core cooling system type,

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

h) total loss of one or more auxiliary systems of systems, structures, components providing fundamental safety functions,

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

j) loss of cooling of the spent fuel pool,

k) uncontrolled dilution of boric acid,

l) simultaneous rupture of more than one heat exchanger tube of the steam generator,

m) loss of safety systems required for the long-term management of an assumed initiating event,

n) loss of the containment pressure reduction function in operating conditions when it would be needed,

o) other events resulting in fuel melting,

j) crash of a military or civilian aircraft,

q) events resulting in multiple failures.

3a.2.2.6400. In selecting events leading to DEC1, all events or event combinations about which it cannot be established with high certainty that the probability of their occurrence is extremely low and may lead to conditions that have not been taken into account in the design basis shall be taken into account. The following shall be taken into account in the selection of the events:

a) events occurring during possible operating conditions,

b) events occurring as a result of internal and external hazard factors,

c) common cause failures,

d) the effect of all nuclear facilities on the site, and

e) events that may affect all facilities on the site, together with the interactions that can be assumed between them.

3a.2.2.6500. All DEC2 plant states shall be identified.

3a.2.2.6600. The DEC analyses shall identify all reasonably achievable measures by which severe accidents can be avoided. Irrespective of the success of the identified measures, preparations shall also be made for severe accidents. As part of the analyses, all reasonably achievable solutions by which the consequences of severe accidents can be mitigated shall also be identified.

3a.2.2.6700. For the analyses of DEC events:

a) only well-founded methods and assumptions can be used;

b) the reproducibility of the analysis shall be ensured also in cases where engineering judgement was taken into account during the analysis, and all uncertainties relating to the analysis and their effects shall be taken into account;

c) all preventive or consequence-mitigating actions by which the resistance of the power plant can be increased against conditions unconsidered 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 systems, structures and components, the conditions associated with the event reviewed and the efficiency of the planned accident response measures shall be taken into account;

f) it shall be demonstrated that sufficient margins are available for avoiding the cliff edge effect;

g) the results of probabilistic safety analyses and their appropriate use shall be shown;

h) where relevant, phenomena taking place during the severe accident shall be taken into account;

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

3a.2.2.6800. An alternative power supply optionshall be provided for avoiding a station blackout. The alternative power source shall be independent and physically separated from the safety power supply, its activation time shall be consistent with the mission time of the uninterrupted power supply.

3a.2.2.6900. Following DEC1 considered in the design extension condition, the achievement of a controlled condition shall be ensured within 24 hours, and the achievement of a safe shutdown condition within 72 hours, at the latest.

3a.2.2.7000. For the extension of the design basis, the accident management functions and the capabilities of the systems performing them shall be taken into account to ensure that the consequences of a DEC2 can be mitigated according to the criteria set for large or early releases in Section 3a.2.4.0800.

3a.2.2.7100. The parameters of DEC1 and DEC2 shall be used to derive boundary conditions and requirements for which the systems and components used for management of events resulting in DEC shall be designed.

3a.2.2.7200. At least the following events shall be practically eliminated by design solutions or the implementation of preventive accident management capabilities, i.e. it shall be demonstrated that their occurrence is physically impossible or the frequencies of their occurrence are less than 10^{-7}/year with high certainty:

a) rupture of the reactor vessel,

b) reactivity accidents with prompt criticality, including the cases of heterogeneous boric acid dilution,

c) all loads appearing in the short and long run, which may jeopardise the integrity of the containment, in particular, the dropping of a heavy load, steam and hydrogen explosion, interaction between the molten core and concrete load-bearing structures, and containment overpressurzation,

d) loss of cooling during the storage of irradiated fuel elements, which may lead to damage to the fuel elements, and

e) loss of coolant with open containment, which may cause core dry out.

3a.2.2.7300. In order to minimise uncertainties and ensure robustness of the safety of the nuclear power plant unit, demonstration of physical impossibility shall be preferred to demonstration of low probability when justifying practical elimination.

3a.2.2.7400. During design, the intended severe accident management functions and the pressure reduction and hydrogen removal systems performing such functions during severe accidents shall be determined to such an extent that high-pressure processes in events causing fuel melting and early damage to the containment can be avoided.

3a.2.2.7500. The functions mitigating the consequences of severe accidents and, if necessary, the systems providing these functions shall be specified to such an extent that in severe accidents the molten fuel can be retained in a cooled condition within the containment.

3a.2.2.7600. Reaching a safe condition after a severe accident shall be ensured within the reasonably shortest time , but with regard to Section 146 *a)* to *c)* of Annex 10, not later than within 168 hours, by restoring the damaged systems or by operating the systems, structures and components providing for the management of DEC plant states.

3a.2.2.7700. The required means of accident management shall be designed and accident management guidelines shall be developed for the efficient mitigation of the consequences of beyond design basis conditions analysed in detail, including severe accident processes resulting in a full fuel melting, in such a way that the hazard to the environment and the population remains below a predefined,

manageable level if the processes and means of accident management operate successfully.

3a.2.2.7800. 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 performance of design basis safety functions.

3a.2.2.7900. During the analysis of external hazard factors resulting in DEC plant states, at least the following shall be performed for the identification of reasonably achievable safety enhancement measures:

a) the severity of the given event beyond which the fundamental safety functions cannot be ensured shall be determined,

b) it shall be demonstrated that sufficient margins are available for avoiding the cliff edge effect,

c) the most efficient ways of providing the fundamental safety functions shall be identified and evaluated,

d) events that simultaneously affect more than one unit or a redundant or diverse system, structure or component, furthermore events that have an effect on the on-site and regional infrastructure, off-site services and protective measures shall also be taken into account,

e) it shall be demonstrated that in the case of a nuclear power plant with more than one unit, common use resources are available in sufficient quantities, the compliance with which shall also be confirmed by on-site inspections.

V. Principles of design for safety

3a.2.2.8000. During the design of the nuclear power plant unit, the initiating events resulting in DBC2-4 and DEC1-2 shall be identified. In the case of the design basis a conservative method, while in the case of the design extension conditions a best estimate method shall be used to determine the effects of the events on systems, structures and components important to nuclear safety. The initiating events may be categorised into representative groups. The design requirements, the effects to be considered, and the events and the threshold values can also be determined for each group, on the basis of an enveloping principle.

3a.2.2.8100. During the management of processes following initiating events, a 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 caused by the event increases safety due to the inherent safety characteristics of the systems;

b) as a result of the initiating event, the nuclear power plant remains safe through the operation of passive safety features or systems that continuously operate under the condition of the initiating event;

c) following the initiating event, the nuclear power plant is brought to a safe shutdown condition through the operation of the safety systems that are required for managing the event; and

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

3a.2.2.8200. If an immediate intervention is required after an initiating event, it shall be ensured that the intervention automatically takes place to prevent more severe consequences. Operator intervention may only be applied if it is demonstrated in the safety analyses that the interval between the detection of the event and the necessary action is sufficiently long. In the case of an operator intervention, the availability of appropriate administrative, operational, accident response and accident management procedures required for the management of the initiating event shall be ensured.

3a.2.2.8300. The failures of systems, structures and components designed for normal operation purposes shall not hinder the performance of safety functions.

3a.2.2.8400. A failure following an initiating event resulting in any DBC2-4 and DEC1-2 shall not cause the loss of a safety function required to manage the given initiating event. Other failures arising from the initiating event shall be taken into account as part of the initiating event.

3a.2.2.8500. During design, the failure modes, the possibility and consequences of inadvertent operation of system components shall be taken into account.

3a.2.2.8600. It shall be ensured by the appropriate design that all physical barriers perform their functions in the case of DBC1-2.

3a.2.2.8700. It shall be ensured by the appropriate design that if any event resulting in DBC3-4 or DEC1 occurs, at least one of the items set forth in Section 3a.2.1.1600 *b)-d)* fulfils its function in addition to the fuel matrix.

3a.2.2.8800. During design, autonomy requirements shall be defined in respect of operator interventions, external services necessary for safe operation, external power supply and the ultimate heat sink. The requirements shall be derived from the timeframes relating to Level F1 and F2 safety functions. 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.

3a.2.2.8900. It shall be ensured by the appropriate design that:

a) regarding operator interventions:

aa) in the case of events resulting in DBC2-4 or DEC, there shall be no need for operator interventions for 30 minutes in the control room, and for one hour outside of the control room for complying with the release limits defined in the design,

ab) there shall be no need for on-site mobile light equipment to prevent a fuel melting within six hours in the case of an event resulting in DEC plant states, and to preserve the containment function within 24 hours in the case of an event resulting in DEC plant states and for 72 hours in the case of an event resulting in DBC2-4,

ac) in the case of an event resulting in DBC2-4 and DEC, there shall be no need for on- or off-site mobile heavy equipment for 72 hours, and

ad) in the case of events resulting in DEC plant states, the containment system shall withstand the hazards for at least 12 hours, but possibly for 24 hours, without operator intervention;

b) regarding the heat sink:

ba) an appropriate heat sink shall be available on the long term in the case of events resulting in DBC2-4 and DEC plant states,

bb) the emergency feedwater reserve shall be sufficient for at least 24 hours, and

bc) at the site of the nuclear power plant, water sufficient at least for 72 hours shall be available for the cooling of the steam generators;

c) in electric powersupply:

ca) independence from external supply shall be ensured for at least 72 hours in the case of DBC1-4 and DEC plant states,

cb) in DBC2-4 the batteries fulfilling a F1 safety function shall fulfil the safety function for at least 2 hours without recharging

cc) in station blackout plant states (DEC1) the batteries fulfilling a F1 safety function, independently of the batteries designed to fulfil a F1 safety function in DBC2-4, shall fulfil the safety function for at least 6 hours without recharging, and

cd) the batteries supplying power to systems used for the management of DEC2 plant states shall perform their safety function for at least 24 hours without recharging and shall be independent of the batteries performing the F1 safety function.

3a.2.2.9000. Systems categorized in nuclear safety classes shall be so designed that the nuclear power plant unit need not be shut down due to their scheduled preventive maintenance or testing required during operation.

3a.2.2.9100. During design, simplicity and clarity shall be aimed at. The use of passive protective systems is preferable to active solutions.

3a.2.3. Demonstration of safety

I. Basic requirements

3a.2.3.0100. The design and analysis tools, models and model parts used for the demonstration of the fulfilment of the general safety requirements of the design basis as well as the input data shall be verified and validated. The validation of the analysis tools shall be presented on the basis of appropriate internationally available data, i.e. 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.

3a.2.3.0200. The independent verification of the analyses containing the characteristics of the designs, which are decisive from a safety point of view, shall also be carried out by different calculation methods.

3a.2.3.0300. The suitability of the methods applied and data used for the determination of the design basis and the analysis of the events reviewed shall be demonstrated by using physical data or experiments or other methods. To compensate for the remaining uncertainties, conservative assumptions shall be used to a reasonable extent substantiated in the safety analysis, primarily by selecting conservative initial and boundary conditions.

3a.2.3.0400. Sensitivity analyses shall be performed to evaluate the uncertainty of assumptions, the data used and the calculation methods. Where the results of the analysis prove to be sensitive to the assumptions of the model, further analyses shall be carried out by using methods and procedures independent of the previously used methods and procedures.

3a.2.3.0500. The analyses used for the demonstration of safety shall be documented in a such way and to such a depth that they may be repeated, independently reviewed and modified to an extent necessary for the evaluation of modifications throughout the lifetime of the nuclear power plant; furthermore, the extent of conservatisms applied and the extent of margins available based on the analysis may be reviewed and re-evaluated.

3a.2.3.0600. During the lifetime of the nuclear power plant, the suitability of interventions or modifications affecting systems, structures and components important to nuclear safety and causing a situation deviating from the authorised conditions shall be demonstrated by deterministic safety analysis or a combination of deterministic and probabilistic safety analyses.

3a.2.3.0700. The design basis, the extended design basis and their demonstration shall be reviewed upon the completion of the design and at regular

intervals throughout the lifetime of the nuclear power plant, and when important new domestic or international safety information is received, and modifications shall be carried out, if necessary, on the basis of the results of deterministic and probabilistic calculations or engineering judgement. The identified deficiencies and possible safety improvements shall be evaluated, and the necessary actions shall be taken in time.

3a.2.3.0800. 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 affects safety;

c) a change in any material properties due to ageing or other effects that have not been taken into account;

d) the international development of safety standards; and

e) newly available significant domestic or international safety information.

II. Deterministic safety assessment

3a.2.3.0900. For all initiating events included in the design basis or in the extended design basis, the fulfilment of the relevant acceptance criteria shall be demonstrated by deterministic safety analyses.

3a.2.3.1000. At least thermohydraulic, hydrodynamic, reactor physics, strength, static, fracture mechanical, dynamic, hot channel, radiation protection and dispersion calculations shall be applied for the demonstration of safety.

3a.2.3.1100. During the analysis of events resulting in DBC2-4, only the systems providing safety functions may be considered. The performance of these systems shall be assumed as the least favourable possible from the point of view of the process reviewed. The operation of systems, structures or components that have no safety function and affect the series of events shall be assumed if their operation exacerbates the effect of the initiating event.

3a.2.3.1200. In the analyses of events resulting in DBC2-4, the single failure of systems providing safety functions, which mostly determines the consequences of the given event and results in the most severe consequences, or a human error shall be assumed. However, there is no need to assume the failure of a passive design solution if it can be demonstrated that there is very low probability for the failure of the given design solution or that it is not affected by the occurrence of the assumed initiating event.

3a.2.3.1210. 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.

3a.2.3.1300. Initiating events resulting in DBC2-3 shall also be analysed with the loss of systems performing the required shutdown functions during the operating condition. During the evaluation, in cases combined with DBC2, DBC4 criteria shall be applied, while in cases combined with DBC3 with frequencies of occurrence of $\geq 10^{-3}$/year, DEC1 criteria shall be applied.

3a.2.3.1400. For stresses and pressure tests in DBC1, for initiating events resulting in DBC2-4, as well as for any thermal stresses due to pressure developing during event sequences with frequencies over 10^{-6}/year, the fulfilment of suitability criteria for the integrity of the reactor vessel shall be evaluated.

3a.2.3.1500. In the analyses of events resulting in DBC2-4 and DEC1, the operator interventions may only be considered on the basis of a conservatively defined time requirement. In the case of operator interventions assumed within a 30-minute timeframe, the analysis also determining the uncertainties shall demonstrate that the assumed operator activities can be performed within the available time.

3a.2.3.1600. In the analyses of events resulting in DEC1 and DEC2, the best estimate method shall be used. The inoperability of any system, structure or component shall be presumed if damage to it is likely as a result of the initiating event or the course of the breakdown.

III. Probabilistic safety analysis

3a.2.3.1700. To determine the total risk presented by the nuclear power plant, to demonstrate the achievement of the relevant risk goals and acceptance criteria, to evaluate the balanced nature 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.

3a.2.3.1800. A Level 1 and 2 probabilistic safety analysis shall be devised for the design of the nuclear power plant unit, including the fuel storage and management systems, which shall include all possible operating conditions, system configurations and all assumed initiating events, for which it cannot be demonstrated by any other method that its contribution to the risks is negligible. In the level 1 and 2 probabilistic safety analyses, considering the state-of-the-art results of science and technology, the external hazards and their combinations shall be taken into account to the largest extent possible. 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.

3a.2.3.1900. In the probabilistic safety analysis, important functional, territorial dependencies, dependencies based on the physical locations of system components, dependencies from operation, maintenance and other common cause failures, in particular, missiles, effects of liquid and steam jets, internal fire and flooding, as well as the accidents of nearby industrial facilities and the effects of human activities shall be taken into account and the effects triggered by hazard factors of natural origin shall also be evaluated.

3a.2.3.2000. Within the probabilistic safety analysis, uncertainty and sensitivity analyses shall also be performed, and their results shall be taken into account for all applications.

3a.2.3.2100. The probabilistic safety analysis shall realistically model the behaviour of the nuclear power plant. For this, the relevant design data, operating and emergency operating procedures, severe accident management guidelines or their drafts shall be taken into account, by taking the human interventions and related potential human errors into account. The suitability of the required operating times assumed in the probabilistic safety analyses shall be demonstrated.

3a.2.3.2200. Human reliability analyses shall be performed, considering factors that may affect the activities and performance of the operating personnel in the individual operating conditions of the nuclear power plant unit.

3a.2.3.2300. In analyses regarding the determination 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.

3a.2.3.2400. For the calculations reliable, credible, primarily facility-specific, secondarily facility-type-specific and thirdly type-specific reliability data shall be used. The data source and the sample size shall be documented. If the source data change, the differences between the design data and the operating conditions shall be taken into account and evaluated. Where no useful statistical data are available, substantiated estimates shall be used.

3a.2.3.2500. The probabilistic safety analyses shall be prepared in accordance with the designed, then the actual maintenance, testing and inspection practices of the systems and components. The fulfilment of the requirements for the results of probabilistic safety analyses shall be demonstrated by taking into consideration the effect of maintenance, tests and inspections on system and component reliability.

3a.2.3.2600. 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 management system of the licensee.

IV. Preparation of the Preliminary and Final Safety Analysis Report

3a.2.3.2700. A Safety Analysis Report shall be prepared for the substantiation of the regulatory licensing procedures prior to the construction, commissioning and operation of a nuclear power plant unit. In the Safety Analysis Report, the information regarding the demonstration of the fulfilment of the requirements for the construction, commissioning and operation of the nuclear power plant shall be included in an integrated system.

3a.2.3.2800. The Preliminary and Final Safety Analysis Report shall be compiled on the basis of the following content requirements considering the contents of Section 1.2.3.0280 of Annex 1:

1. laws, regulations and standards to be applied, and demonstration of compliance therewith,

2. general design principles for the nuclear power plant unit(s) and methods applied to achieve the fundamental safety objectives,

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

4. determination of the site boundaries by EOV coordinates, the key characteristics of the site from a safety point of view,

5. description of the safety functions, the systems, structures and components providing such functions, the principles of safety classification, the design basis for systems, structures and components, their technical description and the description of the their operation under every operating condition,

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

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

8. description and safety aspects of the organisation operating the nuclear power plant and the management system and description of the organisational relations associated with nuclear safety of the nuclear power plant,

9. commissioning programme for the nuclear power plant and considerations serving as a basis thereof, and

9.1. demonstrating in the Preliminary Safety Analysis Report that the designed commissioning activity is suitable for demonstrating that the nuclear power plant unit will operate according to the plans and safety regulations,

9.2.. commissioning results that substantiate safe operation in the Final Safety Analysis Report,

10 emergency operating procedures and severe accident management guidelines, inservice inspection instructions, training requirements and training for the operating personnel, procedure for feedback on operating experience and relevant research results, and a comprehensive ageing management programme,

11. maintenance, testing and monitoring programmes, and the considerations on which they are based,

12. Operational Limits and Conditions and their technical substantiation,

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

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

15. on-site management system for radioactive wastes,

16. considerations for final shutdown and decommissioning during design and operation,

17. in the case of a nuclear power plant with more than one unit or in the case of nuclear facilities in the vicinity of each other, possible technical, organisational and administrative interactions between the units,

18. human factors and evaluation of the safety culture, and

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

3a.2.3.2900. In the descriptions, analyses and findings set forth in the Preliminary and Final Safety Analysis Reports, the entire site shall also be examined in order to take into account hazard factors that:

a) may affect all facilities within a short time,

b) may come from harmful interactions between the facilities.

3a.2.3.3000. In the case of a site with a multiunit nuclear power plant or if there is another nuclear facility operating in the vicinity and the facilities share human

or other resources, it shall be demonstrated that the intended safety functions are fulfilled with regard to all units and facilities.

3a.2.3.3100. The licensee shall have all documentation that is not publicly accessible, but referenced or considered in the Preliminary and Final Safety Analysis Reports.

3a.2.4. Acceptance criteria for safety analyses

3a.2.4.0100. For the processes originating from initiating events resulting in DBC2-4, it shall be demonstrated that the dose determined for a person of the reference group of the population does not exceed:

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

b) for processes originating from initiating events resulting in DBC3, 1 mSv/event, and

c) for processes originating from initiating events resulting in DBC4 and DEC1, 5 mSv/event.

3a.2.4.0200. Initiating events resulting in DBC2 shall not cause doses exceeding 1 mSv/event/person outside the controlled area of the nuclear power plant, in the operational areas of the nuclear power plant where people are allowed to be present.

3a.2.4.0300. Initiating events resulting in DBC3-4 shall not cause a radiation exposure exceeding 10 mSv effective dose or 100 mGy dose for the thyroid outside the controlled area of the nuclear power plant and within operational areas of the nuclear power plant where people are allowed to be present.

3a.2.4.0400. Initiating events resulting in DBC2 may cause radioactive contamination in the controlled area of the nuclear power plant could be only of such a rate and type that can be managed and eliminated by operational methods, systems and system components.

3a.2.4.0500. Initiating events resulting in DBC2-4, with the assumption of a single failure and no other independent defects, shall not induce a consequence that violates the safety criteria set for the given operating condition.

3a.2.4.0600. The total frequency of cases resulting in a partial or full core meltdown for an event sequence originating from all assumed initiating events, except for sabotage, shall not exceed 10^{-5}/year.

3a.2.4.0700. For the fulfilment of the criterion of limited environmental impacts, for events resulting in DEC1 and for events resulting in DEC2 with consideration to the specifications of Section 3a.2.2.7000, it shall be demonstrated that

a) no urgent protective measures are required beyond a distance of 800 m from the nuclear reactor;

b) there is no need for any kind of temporary action, i.e. the temporary evacuation of the population, beyond a distance of 3 km from the nuclear reactor;

c) there is no need for any kind of subsequent protective measure, i.e. the final re-settlement of the population, beyond a distance of 800 m from the nuclear reactor;

d) there is no need for any long-term restriction on food consumption.

3a.2.4.0800. Events resulting in large or early releases shall be practically eliminated. The total frequency of event sequences resulting in large or early releases summarized for all initiating operating conditions and effects, excluding sabotage, shall not exceed 10^{-6}/year. The fulfilment of the requirement shall be demonstrated by Level 2 probabilistic safety analysis.

3a.2.4.0900. The design shall confirm by deterministic safety analyses that the initiating events resulting in DBC2 will not lead to the loss of function of any barrier even with the postulation of a single failure.

3a.2.4.1000. The integrity of the reactor vessel against brittle fracture shall be ensured by ensuring that the stress intensity factor of the critical components of the vessel nowhere exceed the fracture toughness corresponding to the resulting temperature, i.e. discontinuities of the structural materials shall not propagate during the events leading to DBC1-4 and DEC1.

3a.2.4.1100. Following initiating events leading to DBC2-4 , the control and safety protection devices, fuel assemblies and the structural components of the nuclear reactor shall not damage or deform to an extent that the movement of control and safety devices aimed at terminating the fission chain reaction becomes impossible.

3a.2.4.1200. Following initiating events resulting in DBC2-4 and DEC1, the fuel assemblies, the primary circuit of the nuclear reactor and the connected systems shall remain in a condition that the short- and long-term cooling and manageability of the irradiated nuclear fuel can be ensured, furthermore, the systems required for heat removal shall be able to perform their functions both in the short- and long-term.

3a.2.4.1300. For events resulting in DBC2, the criteria ensuring the integrity of the fuel rods shall be set during design by setting limits for the temperature of the nuclear fuel, the critical heat flux and the temperature of the cladding. In order to meet the requirement for long-term coolability and manageability, the allowable maximum extent and type of fuel element damage shall be determined for DBC3-4 and DEC1.

3a.2.4.1400. In order for the systems, structures and components confining or retaining radioactive releases , to perform their safety functions, criteria shall be set for the maximum pressure, maximum and minimum temperatures, thermal and pressure transients, degradation and, depending on the temperature range provided, stresses throughout their lifetime.

3a.2.4.1500.

3a.2.4.1600. To fulfil the nuclear safety requirements, criteria shall be provided for temperature, pressure and leakage rate throughout the lifetime of the containment.

3a.2.5. Operational Limits and Conditions

3a.2.5.0100. During the design process, the limits and conditions for the operation of systems, structures and components which, if met, ensure that the nuclear power plant can be operated in accordance with the design objectives documented in the Safety Analysis Report and in conformance to the nuclear safety requirements, shall be defined.

3a.2.5.0200. The operational limits and conditions shall be so defined that, if met, situations leading to DBC3-4 or DEC1 can be prevented and, in the case of possible accidents, the consequences can be mitigated. When setting the safety limits, a conservative approach shall be applied to take into account the uncertainties of the safety analyses.

3a.2.5.0300. Each operational limit and condition shall be defined on the basis of design considerations and safety analyses of the nuclear power plant and the results of commissioning tests.

3a.2.5.0400. When setting the operational limits and conditions, the following successive safety levels shall be taken into account:

a) safety limits,

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

c) limits and conditions for normal operations.

3a.2.5.0500. The operational limits and conditions shall cover all operating conditions, including operation at full power, the shutdown condition and refuelling as well as the transition conditions between the previous conditions, furthermore, temporary situations arising during maintenance, tests and the monitoring of system components.

3a.2.5.0600. To guarantee safety, a margin shall be maintained between the values of the parameters of the systems providing safety functions as specified in the document “Operational Limits and Conditions” and the safety limits, by

appropriate conservative approach or taking into account the uncertainties of the safety analyses.

3a.2.5.0700. The document “Operational Limits and Conditions” shall contain limits for the operational parameters and, regarding systems important to nuclear safety, the minimum required number of operable system components, which need to be in operational or standby condition in the various DBC1-2. It shall also contain the interventions to be carried out by the operating organisation and the time allotted for carrying out interventions for cases when there is a deviation from the operational limits and conditions.

3a.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.

3a.2.5.0900. As part of the document “Operational Limits and Conditions”, the requirements for the necessary and the sufficient personnel for safe operation shall be determined. When determining the necessary and sufficient personnel for safe operation, the requirements for management of incidents and accidents shall also be fulfilled.

3a.2.5.1000. Prior to the commissioning of the nuclear power plant, the preliminary version of the document “Operational Limits and Conditions” shall be developed. Its contents shall ensure that the systems, structures and components of the nuclear power plant operate in accordance with the design assumptions and objectives of the Safety Analysis Report.

3a.2.5.1100. The preliminary version of the document “Operational Limits and Conditions” shall be reviewed on the basis of the experience gained during commissioning and shall be modified and finalised as required, in accordance with the Safety Analysis Report.

3a.2.5.1200. Rules applicable to the modification of the document “Operational Limits and Conditions” or temporary deviations from its contents shall be laid down in internal procedures. The permissibility and compliance of the deviations shall be demonstrated by safety and other analyses in every instance.

3a.3. SPECIAL DESIGN REQUIREMENTS

3a.3.1. Design of safety class systems

3a.3.1.0100. During the design of safety class systems, structures and components, in order to fulfil the required design criteria, primarily redundancy, diversity, physical separation, and separation of electrical power supply, functional

separation and independence, and independent data link and fail-safe design principles shall be applied. Such systems shall be designed by using reliable qualified system components and, as required, by developing independent auxiliary systems.

3a.3.1.0200. It shall be demonstrated for every initiating event that the system, structure and component participating in providing safety functions associated with the level of defence in depth involved in the course of the event are independent of the systems, structures and components associated with other levels of defence in depth.

3a.3.1.0300. In order to ensure a greater independence, it shall be systematically implemented to a reasonable extent that irrespective of the initiating events, a safety system, structure or component can be associated with only one specific level of the defence in depth.

3a.3.1.0400. During the design of systems, structures and components, passive, inherently safe solutions shall be applied to the extent reasonably achievable, which ensure that the failure of the systems, structures and components, even without external interventions, leads to a safe condition.

3a.3.1.0500. Regarding safety class systems, structures and components efforts shall be made for their fail-safe design. If the individual safety class systems, structures and components provide safety functions in several different positions or conditions, it shall be determined that the failure of which safety function will lead to a more severe consequence. The so determined fail-safe provision of the safety function shall be preferred during design.

3a.3.1.0600. The failure of a system, structure or component important to nuclear safety shall not cause the failure of a system, structure or component included in a higher safety class.

3a.3.1.0700. Simple safety systems shall be applied to the extent reasonably achievable in order to minimise:

a) the number of operator interventions,

b) the number of interventions to fulfill a given function,

c) the necessity of protective interlocks,

d) the number of system components necessary for operation and related to safety and reliability,

e) the need for maintenance and inspections, and

f) the number of service systems.

3a.3.1.0800. The safety class systems, structures and components shall be sized for external effects of natural origin to a minimum frequency of recurrence of 10^{-5}/year if the component may have a safety function in the given situation.

3a.3.1.0850. In the design of systems, structures and components the loads and load combinations shall be determined based on the analysis of those circumstances and effects, under which the safety function of the systems, structures and components is fulfilled considering normal operation, anticipated operational occurrences, design basis accidents and the test conditions, as well as the safety and seismic safety class of the component. The particular combinations shall be determined in the design specification based on the concurrence and importance of the loads. In those cases, when the safety function of the system, structure and component is required for management of DEC plant states, the loads and environmental conditions characteristic within them shall be considered.

3a.3.1.0900. It shall be ensured that the safety systems, structures and components and their auxiliary systems are protected as much as possible from the effects of internal and external hazard factors and from interactions between failed systems, structures and components.

3a.3.1.0910. The possibility of potential adverse interactions of the concurrently operating systems shall be assessed, and the adverse interactions shall be prevented if necessary. During the assessment attention shall be paid to physical connections and the impact of intentional and inadvertent operation on environmental conditions and the impact of the caused environmental condition on the other component.3a.3.1.1000. The possibility of common cause failure shall be taken into account when it is determined where and how the principles of redundancy, diversity, physical separation and functional separation shall be applied to provide the required function and reliability.

3a.3.1.1100. During design, the requirement of single failure tolerance shall be applied. The possibility of the inadvertent operation of system components shall be handled as a possible mode of failure. The failure of a passive design solution shall be taken into account, unless it can be demonstrated that the failure of the passive design solution is highly unlikely or does not influence the given function.

3a.3.1.1200. F1 systems and systems providing Level F2 safety functions, which are not accessible for recovery, shall have an individual safety power supply for each redundant branch. Furthermore, their designed redundancy and independence shall at least:

a) prevent the loss of a protective function in the case of a single failure occurring in the system, and

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

3a.3.1.1300. It shall be ensured that the operability of systems providing Level F1 safety functions can be inspected during operation.

3a.3.1.1400. The activation and operation of systems providing Level F1A safety functions shall be ensured with either automated systems or passive systems in such a way that no operator intervention is needed within 30 minutes following an initiating event resulting in DBC2-4. 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, and it shall also be demonstrated that the planned intervention can be performed by an operator.

3a.3.1.1500. If the achievement of probabilistic safety objectives could only be ensured by using systems of extreme high reliability, such safety functions shall be provided diversely.

3a.3.1.1600. The appropriate design of the system performing the automatic shutdown of the nuclear reactor and controlling the systems providing active safety functions shall ensure that in the case of events resulting in either DBC1 or DBC2-4, the operating personnel cannot prevent automatic safety actuation from their established operating control positions, while being able to perform the necessary interventions.

3a.3.1.1700. In addition to the general requirements for programmed systems, programmed systems performing safety functions shall fulfil the following requirements:

a) hardware devices and software tools that have references fulfilling the most stringent quality assurance requirements shall be used,

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

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

d) if the necessary reliability level of a system cannot be demonstrated, the performance of the protection functions assigned to it shall also be ensured by diverse means.

3a.3.1.1800. Appropriate margins shall be provided between the safety limits and the set values of the systems providing safety functions.

3a.3.1.1900. During the design, installation and maintenance of safety class systems, structures and components, it shall be ensured that their quality and the reliability of the safety functions provided by them correspond to their safety class.

3a.3.1.2000. For each safety class, the following shall be specified:

a) the appropriate requirements and standards to be applied during design, manufacture, assembly and inspection,

b) the need for power supply from a backup energy source,

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

d) quality requirements, and

e) requirements for environmental qualification.

3a.3.1.2100. The harmony between safety classification and the design and manufacturing specifications assigned to it shall be shown and demonstrated, including the codes and standards applied.

3a.3.1.2200. 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.

3a.3.2. Design for lifetime

I. Design lifetime

3a.3.2.0100. The design lifetime of the nuclear power plant shall be specified and that the lifetime of which system component performing a safety or physical barrier function defines or limits this design lifetime.

3a.3.2.0200. By analysing the degradation processes that limit the design lifetime, it shall be demonstrated that the lifetime of non-replaceable system components and non-replaceable system components that perform passive safety and physical barrier functions is at least as long as the design lifetime of the whole nuclear power plant, also considering the stresses and ageing processes expected throughout the lifetime with the required margins.

3a.3.2.0300. It shall be specified under what conditions the nuclear safety requirements can be fulfilled during the design lifetime.

3a.3.2.0400. If the lifetime of a system, structure or system is shorter than the design lifetime of the nuclear power plant, their possible refurbishment or replacement shall be ensured.

3a.3.2.0500. The period required for decommissioning shall also be taken into account in the design lifetime of systems, structures and components that provide functions until the commencement of or during decommissioning.

II. Requirements regarding structural materials

3a.3.2.0600. During the design of systems, structures and components important to nuclear safety, the following types of structural materials shall be used:

a) that have been tested, environmentally qualified, and fulfil the design and environmental conditions,

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

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

c) the materials of which are the least susceptible to activation and once becoming activated, the activated parts remain in place as a result of their structures,

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

d) in the case of system components exposed to neutron radiation and included in Safety Class ABOS 1, the change in material properties of which is minimal and verifiable throughout the lifetime,

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

f) for which such a surface can be manufactured that can be the decontaminated to the greatest possible extent during operation and decommissioning, and

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

3a.3.2.0700. System components coming into contact with radioactive media shall be made of such structural materials that have high corrosion resistance in order to reduce the deposition of corrosion products.

3a.3.2.0800. In the case of system components exposed to fatigue stress, the use of castings shall be avoided.

3a.3.2.0900. In the main circulation loop and in the system components of the connected systems, the rate of materials producing Co^{60} final product shall be minimised (the use of cobalt-containing surface-hardening materials is not allowed and the limitation of the production of Co^{58} shall be taken into account when nickel-containing materials are used).

3a.3.2.1000. During the use of austenitic materials, the risk of intercrystalline corrosion shall be avoided through the use of titan-stabilised alloys, the regulation of the rate of their carbon and titan content, and the requirement of testing the raw materials for intercrystalline corrosion. In the case of austenitic welding materials, the delta ferrite content of the welds shall be limited.

3a.3.2.1100. In the case of non-metal structural materials, it is especially important to evaluate compliance with all environmental conditions expected throughout the lifetime of the unit.

3a.3.2.1200. When pressure retaining equipment and pipelines are designed, special care shall be taken for the design specifications of welding applied during manufacturing and assembly as a special process, which can be corrected to a limited extent and, in particular, for the following:

a) applicable welding methods,

b) weld design,

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

d) specification of the scope of the 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,

ec) requirements set for the qualification documentation of welding.

3a.3.2.1300. During design, it shall be demonstrated through the analysis of degradation processes limiting the lifetime that

a) despite the effect of ageing, the strength properties of structural materials correspond to the maximum loads calculated for DBC1-4 and DEC1 and DEC2 by taking into account the safety margins specified for the operating condition, of the system component concerned performs a safety function in the given operating condition; and

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

3a.3.2.1400. During design, the criteria for catastrophic failure shall be fulfilled when materials are selected. All typical fracture mechanisms shall be analysed for the concerned system components.

3a.3.2.1500. During design, when structural materials are selected, inspections, material testing and the documentation requirements shall be determined in a graded manner, in accordance with their classification on the basis of the material

or product standards as well as the manufacturing and operating experiences of nuclear reactors.

3a.3.2.1600. In the case of new materials and manufacturing methods, an environmental and seismic qualification procedure shall be carried out, on the basis of which the fulfilment of the goal and requirements of use can be demonstrated.

3a.3.2.1700. It shall be ensured that the physicochemical properties of the materials used in the containment do not contribute to hydrogen production during events resulting in DBC2-4 and DEC1.

3a.3.2.1800. During design, the following requirements shall be fulfilled with regard to structural materials:

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

b) if austenitic casts are used, the resistance against thermal ageing and stress corrosion shall be analysed and demonstrated,

c) the use of copper, aluminium and their alloys is prohibited in safety class system components,

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

e) in the case of carbon-steel system components coming in contact with water, a wall thickness allowance determined in strength analyses shall be designed for general corrosion processes,

f) use of plastics shall be allowed exclusively in safety class three only after evaluation of the operating pressure, temperature and environmental conditions, and

g) selection of structural materials shall be performed to keep the number of dissimilar welds at the lowest.

3a.3.2.1900. During design, when the materials to be used are selected, the following aspects of the planned decommissioning of the nuclear power plant shall be taken into account:

a) long-term storability at the nuclear power plant as defined in the decommissioning strategy,

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

c) material of the decontaminable surfaces, and the system of decontamination chemicals and technologies shall be so selected that the desired cleanliness and

radiation conditions needed for the treatment can be preserved until the end of the service life of the system, and

d) in the case of materials activated during operation, in accordance with the planned schedule of decommissioning, the shortest possible half-life.

III. Chemistry

3a.3.2.2000. The water control of the primary and secondary circuit systems of the nuclear power plant unit as well as its auxiliary and service systems shall be so designed that

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

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

c) the quantities 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 dissolved gases in the primary circuit in DBC1.

3a.3.2.2100. The suitability of the cooling and working media shall be demonstrated with calculations and analyses, taking into consideration the design lifetime of the nuclear power plant.

3a.3.2.2200. A sampling system shall be designed to allow the monitoring of changes in water parameters important to safety, and to allow undesirable water chemistry and corrosion processes, the accumulation of corrosion products and changes in their activity, and the loss of leaktightness of fuel cladding to be detectable in due time. The design shall ensure that samples from the sampling system are representative and free of countercheck regarding safety.

3a.3.2.2300. For each system, a process for the removal of corrosion products, radioactive contamination and other contaminants shall be designed, and appropriate methods shall be devised and appropriate tools shall be designed for it.

3a.3.2.2400. 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 be determined in such a way that they have an adverse effect at the reasonably lowest achievable level on the structural materials used in all planned operating conditions of the nuclear power plant unit under given temperature, pressure and flow conditions.

3a.3.2.2500. During the design of water systems, the effects of parameters affecting corrosion and corrosion products on structural materials and physical processes, e.g. heat transfer, shall be analysed. Concentration limits shall be set

for corrosion products and the acceptable amounts of deposits that do not jeopardise safe operation shall be determined in systems and system components important to nuclear safety. The required measures, means and procedures shall be designed to prevent the exceedance of the limits and to retrieve the normal values if the limits are exceeded.

3a.3.2.2600. When the concentrations of chemicals correcting the pH effect resulting in concentration changes of parameters influencing corrosion and the neutron-absorbing, reactivity control material are regulated, the effects of radiolytic reactions shall be taken into account.

3a.3.2.2700. Water purification systems shall be designed to facilitate that the amount and concentration of radioactive materials released into the environment remain below the limits and at the lowest reasonably achievable level in every planned operating condition. It shall be ensured that the amount and activity of the radioactive waste produced during cleaning processes remain at the lowest reasonably achievable level.

3a.3.2.2800. The capacity of water purification systems shall guarantee that the amounts of corrosion products in the systems are continuously at an appropriately low level allowed in the design.

3a.3.2.2900. Cleaning technologies that ensure that a passive protective layer remains or regenerates on the surface of the affected structural materials shall be applied.

IV. Environmental qualification of system components

3a.3.2.3000. During design, the environmental conditions and the impacts arising as a result of external and internal hazard factors shall be determined for DBC1-4 and DEC1, under which the systems and system components shall perform their safety and physical barrier functions. To the extent defined in the design, the environmental conditions for extended design basis conditions shall also be specified.

3a.3.2.3100. Qualification procedures shall be used for demonstrating that the systems and system components important to nuclear safety are able to perform their functions throughout the lifetime of the nuclear power plant under environmental conditions occurring during events resulting in DBC1-4 and DEC1 if their operation is required under these conditions.

3a.3.2.3200. The environmental resistance of passive metallic and concrete system components shall be ensured by design. If required, the environmental resistance shall be demonstrated by analyses.

3a.3.2.3300. The suitability of non-metallic, non-concrete system components and active system components shall be demonstrated by individual or type qualification.

3a.3.2.3400. During the design and initial qualification of a system component, the ageing mechanisms during operation shall be considered, and it shall be demonstrated that despite the ageing effects, the system components are able to perform their functions with the required reliability even at the end of their designed lifetime.

3a.3.2.3500. In the designs of the system components, the method and conditions of maintaining a qualified state shall be specified.

3a.3.2.3600. Qualification for flooding and fire is required if they may occur at the location of installation of the system component, and such events cannot be ruled out if the single failure criterion is applied to demonstrate the performance of safety functions.

3a.3.2.3700. It shall be examined whether electromagnetic effects jeopardise the performance of any safety function. It shall be ensured that the performance of the safety functions cannot be influenced by such effects.

3a.3.2.3800. If a system component has a function in DBC3-4 or DEC , then it shall be qualified for tolerating the loads caused by the operating conditions.

3a.3.2.3900. During the qualification procedure of systems and system components participating in severe accident management and the mitigation of the consequences of accidents, their operability for the required time shall be demonstrated for the most likely conditions and loads that can be assumed in DEC2.

V. Maintenance, review and inspection

3a.3.2.4000. The designer shall provide installation, operating and maintenance instructions for all systems, structures and components. The installation and maintenance instructions shall have a level of detail as to include the dimensions and fitting values required for the full disassembly, inspection and assembly of the system, structure or component.

3a.3.2.4100. In the case of all systems, structures and components important to nuclear safety, the programme of in-service or regular inservice inspections, reviews and material testing programmes; the mode and frequency of the testing of structural integrity, leaktightness and functions, and the designer specifications for planned preventive maintenance and other maintenance strategies shall be determined.

3a.3.2.4200. Parameters characterising operability and suitability shall be specified. For these parameters, suitability criteria shall be provided, compliance with which shall be measured and confirmed during tests and inspections. For the case of deviations from the acceptable values, the required actions shall be planned, including the modification of maintenance programmes.

3a.3.2.4300. If the performance of tests and inspections cannot be ensured due to a covered structure or limited access during design, then either design solutions are required to compensate for the limited access, or it shall be demonstrated that operation can be maintained for the design lifetime without inspections or monitoring.

3a.3.2.4400. During design, the cycle time of functional tests, the revision frequency, the requirements for conducting reviews and maintenance methods and conditions for systems, structures and components important to nuclear safety shall be defined and substantiated in such a way that

a) they are consistent with the design principles and design of the system, structure or component,

b) they ensure that the given safety function is reliably performed during the test, revision and maintenance of the system or system component, and

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

3a.3.2.4500. During design, specifications, acceptance criteria shall be defined for the acceptance testing of system components at the manufacturers, and for the on-scene assembly and pre-commissioning inspections. The in-manufacturing and the subsequent inspection methods shall conform to the in-service inspection methods planned during operation and defect detection sensitivity in the interest of subsequent comparability. Special specifications shall be set for the tests to be performed during manufacturing of the system components, for which the in-service inspection cannot be performed due to the lack of access or the activation of system components.

3a.3.2.4600. The substantiation of the solutions used during design and the manufacturing drawings relating to spare parts shall be attached to the documentation accompanying the products, in particular, in the case of non-long-lived fe equipment.

VI. Ageing management

3a.3.2.4700. The ageing processes and characteristics shall be identified in the case of all safety class system components, and data and methods required for

developing an ageing management programme and system to be carried out during operation shall be provided. The ageing management system specified by the design shall conform to the maintenance programmes, the rating of tests and the environmental qualification of system components, as well as the programmes for maintaining the qualified state.

3a.3.2.4800. During the design of systems, structures and components important to nuclear safety, the expected ageing processes and their effects shall be examined: it shall be demonstrated, by taking into account the possible uncertainties of the "0" condition and the ageing processes, that the ageing processes of the used structural materials do not hinder the systems, structures and components in performing safety functions during the design lifetime.

3a.3.2.4900. When systems, structures and components important to nuclear safety are designed, changes in the properties of the selected structural materials occurring as a result of ageing processes shall be evaluated. The allowed lifetime and integrated operating time of the systems, structures and components as well as the number of cycles of operational, accident, maintenance and testing stresses shall be determined.

3a.3.2.5000. During design, clear operating indicators and criteria shall be specified for the systems, structures and components important to nuclear safety for determining their ageing processes, operability conditions and remaining lifetime.

3a.3.2.5100. Ageing management specifications shall be devised for the systems, structures and components important to nuclear safety. The specifications shall include the identification of measures for:

a) the identification of the locations of ageing of systems, structures and components important to nuclear safety and the ageing processes expected on them,

b) an estimate of the expected progress of ageing processes,

c) maintenance, supervision, testing and monitoring activities required for the management of ageing processes, and

d) determination of measures for slowing down ageing and condition deterioration processes and the mitigation of their adverse effects.

3a.3.2.5200. A monitoring programme shall be devised and implemented for parts of the pressure retaining equipment and pipelines of the primary circuit that are exposed to high neutron radiation or other ageing processes in order to monitor the ageing processes in the materials used.

3a.3.3. Design of pressure retaining equipment and pipelines

3a.3.3.0100. During design, operating conditions and mechanical loads and load cycles, including effects triggered by external and internal hazard factors, under which the given pressure retaining equipment and pipeline can operate, shall be determined.

3a.3.3.0200. The calculations substantiating sizing and supporting the suitability of the system components shall be carried out in accordance with a uniform set of specifications or standards accepted in the nuclear industry, in accordance with the safety class of the systems, structures and components. The calculations substantiating sizing, the control analyses performed for the individual loading cases and the circumstances and considerations assumed during design shall be described.

3a.3.3.0300. The application of pressure retaining equipment and pipelines designed according to various standards and sets of specifications shall be avoided. If it happens, the possibility of adjusting and assembling pressure retaining equipment and pipelines designed on the basis of different sets of standards shall be substantiated by a separate analysis.

3a.3.3.0400. The containment shall be sized as a piece of pressure retaining equipment and the possibility of the regular verification of its pressure-retaining capability shall be ensured.

3a.3.3.0500. It shall be demonstrated that the material of system components performing physical barrier functions according to Levels B1 and B2 and included in Safety Classes ABOS 1 and 2 has the toughness corresponding to the load. No new cracks shall occur in the material in DBC1-4 and DEC1. It shall be demonstrated that the cracks already existing in the material have appropriate resistance against unstable crack propagation, thereby it is ensured that the designed inservice tests will detects the defects in time.

3a.3.3.0600. During the design of pressure retaining equipment and pipelines, the change of the physical and mechanical properties of materials as a result of neutron flux shall be taken into account.

3a.3.3.0700. During the design of pressure retaining equipment and pipelines, within the framework of the standards applied, it shall be ensured that

a) the number of joints is minimised in the pressure retaining components and main circulation loop pipelines, and

b) use of welded joints should receive priority, taking into account the opportunity to perform non-destructive examinations and maintenance .

c) use of detachable joints shall be justified by risk analysis of the system.

3a.3.3.0800. It is allowed to use seams only in a specific, warranted case, if a separate analysis is carried out, at places where they are exposed to bending stress and where the tension is concentrated. For the welding of pressure retaining equipment and pipelines, full penetration welds shall be used. Analysis shall justify the use of partially penetrating welded joints.

3a.3.3.0900. During the design of systems and components important to nuclear safety, vibration generated by mechanical sources and flows and the deterioration processes caused by them shall be taken into account. The systems and components shall be designed in such a way as to minimise vibration. During commissioning, it shall be demonstrated that the vibration level does not exceed the extent taken into account during design as allowable.

3a.3.3.1000. Pressure retaining equipment and pipelines shall be provided with monitoring and measuring instruments to the extent determined by the safety function performed by them in order to monitor pressure, temperature, and the flow-rate, level and chemical composition of the working medium as well as displacement and leaktightness.

3a.3.3.1100. The quantity, location and type of the fittings to be installed in the individual systems shall be so determined that the following are possible:

a) setting normal operation paths and parameters,

b) performance of safety functions,

c) performance of inservice function tests and inservice monitoring programmes, and

d) close off of system components for maintenance and repair.

3a.3.3.1200. If a higher than allowable pressure can develop in them, the pressure retaining equipment and pipelines shall be equipped with an appropriate pressure limiting device. The pressure limiting devices shall be so designed that if they operate, the quantity of radioactive materials released into the environment has the lowest reasonably achievable level.

3a.3.3.1300. If a system or component important to nuclear safety is in contact with a system or component the operating pressure of which is higher than that of the former one, the system or component shall be designed for the pressure values of the latter system or component, or it shall be ensured by design solutions that even in the case of a single failure, the pressure in the system or component designed for the lower pressure does not exceed the design value.

3a.3.3.1400. The results of strength analyses shall demonstrate that:

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

b) the structural materials comply with the maximum loads calculated in DBC1-4 and DEC1 by taking into account the criteria set for ageing and the specific operating condition; and

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

3a.3.3.1500. The requirements and standards applicable to the design of pressure retaining equipment and pipelines shall be applied in accordance with the safety class of the given system or component.

3a.3.3.1600. A strength analysis shall be performed to demonstrate the compliance of all load-bearing components, pressure retaining systems and components. Strength calculations may be carried out only within one set of standards.

3a.3.3.1700. The data used in strength analyses shall come from a conservative approach, and they shall be collected in accordance with the selected standard. Effects leading to the degradation of structural materials shall be taken into account.

3a.3.3.1800. Protection against brittle fracture shall be examined in the case of system components where this is necessary.

3a.3.3.1900. It shall be demonstrated by means of strength analyses that the load on the examined system components remains below the acceptable load value in DBC1-4 and DEC1.

3a.3.4. Design of buildings and building structures

3a.3.4.0100. During the design of the nuclear buildings of the nuclear power plant, the general rules applicable to architectural and technical design shall be applied by taking into account the specific requirements for nuclear systems and components.

3a.3.4.0200. The nuclear building design programme of the nuclear power plant shall contain in the form of a textual document the determination of essential specific requirements comprehensible for the building and building structure, specified in the Govt. Decree on the National Community Planning and Construction Requirements and to be set for the building and building structure as a result of its specific features, on the basis of the intended purpose or purposes of the nuclear building.

3a.3.4.0300. All specific requirements set in the design programme shall be determined considering the provisions of the Nuclear Safety Code and the relevant legislation applicable to nuclear systems and components. In line with the principle determined in Subsection 4 (2) of the Atomic Act, the determined specific requirement shall receive priority over the determined basic requirement.

3a.3.4.0400. It shall be ensured that the buildings and building structures of the nuclear power plant tolerate the loads and environmental impacts arising in DBC1-4 and under DEC1 and DEC2 representing the design extension condition in accordance with the acceptance criteria provided for the given plant state.

3a.3.4.0500. Where necessary, appropriate sampling and monitoring facilities shall be established in order to allow the continuous monitoring of the suitability of the building structures throughout their lifetimes.

3a.3.4.0600. The safety class buildings shall be designed for stresses caused by the safety earthquake, including the appropriate design of the foundation and the effects of the triggered geotechnical hazards. The additional stress on buildings arising during earthquakes shall be minimised by the appropriate structural design of safety class buildings. Interaction with adjacent buildings shall be excluded in the case of a safety earthquake.

3a.3.4.0700. Sizing for earthquakes shall be carried out on the basis of methodological and standard specifications adopted for safety class buildings and building structures.

3a.3.4.0800. The implementation of the design input required for the earthquake resistance of buildings and building structures shall be based on the design input response spectra derived from the free ground response spectra of safety earthquakes. Soil movements in the foundation plane of the building shall be calculated back from this.

3a.3.4.0900. The appropriate load-bearing capacity of the supporting structures of the buildings relative to loads caused by soil movements corresponding to safety earthquake shall be demonstrated by dynamic analyses. The methodology of the dynamic analysis and the complexity of modelling shall be in harmony with the risk caused by the nuclear power plant and, within that, the safety class of the building structure, the function of the building structure and the purpose for which the expected calculation results are used.

3a.3.4.1000. In the modelling of the interaction between the soil and buildings, the underground structures of the building, the properties of the building and the foundation structures used, the layers and soil environment, the soil physical parameters and dynamic properties of soils, and the uncertainties in them shall be taken into account.

3a.3.4.1100. In the case of soil liquefaction developing as a result of an earthquake, after the application of the technical solution, the probability of local soil liquefaction shall be less than 10^{-6}/year with regard to the cliff edge effect.

3a.3.4.1200. The load-bearing capacity shall be verified in accordance with standards adopted in the nuclear industry. The fulfilment of limits relating to displacement and deformation that may be derived from the design of building structures shall be evaluated.

3a.3.4.1300. The design of geotechnical structures shall be carried out in accordance with the relevant Hungarian standards, taking into account effects from design basis earthquakes associated with the nuclear power plant.

3a.3.4.1400. In the design of all building structure, including the building structures being in interaction with the soil, it shall be demonstrated that the relevant load bearing limiting states are not exceeded in any building state.

3a.3.4.1500. If the location of the planned building structure is in the vicinity of an operating nuclear facility, the building structures in interaction with the soil shall be designed that the soil and layer conditions of the environment are not changed in such an extent that the building of the nuclear facility in the vicinity would be endangered.

3a.3.4.1600. During the licensing and construction design phases, design reviews shall be conducted to review the soil examination report, the geotechnical plans and part plans. The design review shall be conducted by a geotechnical designer, geotechnical expert authorized according to the decree on the detailed rules of justification of applicability and registration and data content of the registration of professionals to pursue civil engineering-technical expert, civil engineering designer, technical building inspector and responsible construction supervisor activity in relation to structures applied for the use of atomic energy.

3a.3.5. Layout

3a.3.5.0100. In the layout of system components, in order to avoid common cause failures, the requirements for redundancy, diversity and independence shall be taken into account.

3a.3.5.0200. The layout shall ensure that interactions between design basis events and the individual buildings and systems cannot cause damage to an unacceptable extent to the nuclear power plant.

3a.3.5.0300. Redundant systems important to nuclear safety shall be designed with appropriate physical separation.

3a.3.5.0400. Cables important to safety shall be laid in stand-alone cable tunnels. Electrical and IT cables shall not be laid in shared ducts.

3a.3.5.0500. Pipelines shall be separated according to their radioactive and inactive contents. Pipelines conveying radioactive materials shall be laid where no human presence is needed.

3a.3.5.0600. The pipes and ducts of heating, ventilation and air conditioning shall be separated from pipes and ducts important to safety.

3a.3.5.0700. Handling paths used by means of transport within the nuclear power plant shall be so designed that the possible dropping of lifted loads shall not jeopardise the performance of the safety function of any other system, structure or component, or devices shall be designed with which it can be ensured that the acceptance criteria relating to DBC4 are met if the load is dropped.

3a.3.5.0800. The location of systems, structures and components shall be so designed that it should provide a possibility for carrying out inspections, maintenance, repair, the replacement spare parts and decommissioning along with the minimisation of doses arising during these activities. Opportunities shall be provided for monitoring through visual inspection and non-destructive testing, and cleaning, washing and repair of the raw material and welded joints.

3a.3.5.0900. Workplace access or escape routes shall be designed in such a way that the operating personnel can easily move around even in their protective equipment. Unobstructed routes of appropriate size and load-bearing capacity shall be provided for the mechanical transport of activated or contaminated objects. The rooms used for the storage of tools and equipment 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.

3a.3.5.0910. The rooms housing safety class systems, structures and components, and the openings at the boundary of the controlled area shall be equipped with monitoring and alarm systems that provide information on their state in the control room.

3a.3.5.1000. The logistics background, services and equipment required for the operation of the nuclear power plant unit, including traffic roads, water supply, fire water network and on-site communication equipment shall be so designed and installed that they can fulfil their functions in DBC1-4 and DEC1-2, to the extent required for the management of the plant states.

3a.3.5.1100. The nuclear power plant unit shall be so designed that, if necessary, there should be a possibility for the operating personnel to enter certain rooms of the containment while the leaktightness of the containment is continuously ensured.

3a.3.5.1200. The buildings of the nuclear power plant shall be so designed that in the case of an emergency, the escape and rescue of the personnel present on the site of the nuclear power plant can be carried out quickly and safely.

3a.3.5.1300. Redundant systems included in safety classes, which play a role in the management of the effects of external and internal hazard factors, shall be placed so that the effect cannot prevent the fulfilment of the safety function of all redundant components at the same time.

3a.3.5.1400. In accordance with the fire protection plans, working areas and corridors shall be provided with emergency lighting. Escape routes shall be clearly marked. The hazard-signalling systems shall reach all members of the personnel, and the noise level and the design of the protective equipment shall be taken into account during design.

3a.3.5.1410. At least one escape route shall be available from the workplace and other locations used by the personnel in the case of events or event combinations considered in the design.

3a.3.5.1500. In the case of a nuclear power plant with more than one unit, every unit shall have its own safety systems, structures and components for management of DBC1-4 and DEC1 and DEC2 to the extent reasonably achievable. The safety systems may be shared between the units only if warranted from a safety point of view.

3a.3.5.1600. In DEC1-2, it is allowed to apply connected support systems between the individual units if it can be demonstrated that they help the restoration of a given safety function during accident management. No interconnection is allowed between the units that would increase the probability or severity of consequences in the case of any unit.

3a.3.5.1700. All such components, which manual operation may be necessary to respond to a given event or during recovery, shall be so placed that the intervention can be performed under the anticipated environmental conditions.

3a.3.6. Specific hazard factors

I. Earthquake

3a.3.6.0100. The site-specific safety earthquake shall be characterised according to the mean hazard curve, with the free ground response spectra and the corresponding acceleration-time function, taking into account non-linear transmission through surface layers. Based on this, the response spectra that forms the standard design input during design, verification and qualification for safety earthquakes shall be determined.

3a.3.6.0200. Irrespective of the seismicity of the site, the maximum horizontal acceleration value of the safety earthquakes shall not be less than 0.25 g on the free ground.

3a.3.6.0300. The nuclear power plant shall be so designed that the fundamental safety functions are provided even in the case of a safety earthquake, and the nuclear power plant is brought in a controlled, safe shutdown condition after the earthquake even in the case of a single failure of the systems, structures and components.

3a.3.6.0400. Systems, structures and components performing F1 safety functions and performing F2 functions participating in the implementation of earthquake protection shall be so designed and qualified that they maintain their required operability and function in the case of a safety earthquake. The design and qualification shall be carried out in accordance with the safety class and the nuclear standards and testing procedures.

3a.3.6.0500. Systems, structures and components providing B1 and B2 functions and included in Safety Classes ABOS 1 and 2 as well as ones performing B3 functions participating in the implementation of earthquake protection shall be so designed, qualified that they preserve their structural integrity, stability and leaktightness in the case of a safety earthquake. The design shall be carried out in accordance with the safety class and the nuclear standards.

3a.3.6.0600. The protection of systems, structures and components with F1, B1 and B2 functions and ones providing F2 or B3 functions participating in the implementation of earthquake protection shall be ensured against damage to, and interaction between, system components that have no safety or physical barrier functions occurring as a result of a safety earthquake.

3a.3.6.0700. It shall be ensured that even if the spectral and maximum acceleration values of a safety earthquake are exceeded to a small extent, the immediate loss of function of the systems, structures and components is prevented.

3a.3.6.0800. During the design of systems, structures and components and the development of nodes and anchorages, it shall be ensured that the structure has an energy-dissipating capability while operating in the elasto-plastic range.

3a.3.6.0900. Brittle damage shall be excluded by the appropriate selection of materials and design solutions. Interaction and collision between adjacent systems, structures and components and surrounding supporting structures shall be prevented.

3a.3.6.1000. The loads combined with the loads generated by a safety earthquake shall be determined by taking into account the functions of the systems, structures and components. During design for earthquakes, loads arising during the operation, shutdown, maintenance, refuelling or DBC2 of the nuclear power plant shall be combined with the loads generated by the safety earthquake.

The compliance criteria can relate to stresses, deformation, displacement and operability as well as to their combinations in accordance with the nuclear standards applicable to the given safety class. The concurrence of events resulting in DBC3-4 and a safety earthquake as independent events need not be assumed. The secondary effects of the safety earthquake shall also be taken into account during design.

3a.3.6.1100. During the design of systems and components, the response spectra characteristic to the location of installation and the acceleration time function shall be regarded as prevailing, which shall be performed in accordance with the standard by taking into account the design input specified for a site-specific safety earthquake, the dynamic response of the building and the interaction between the soil and the building.

3a.3.6.1200. The management of the effect of the earthquake shall not be dependent on the availability of external services (electrical network connection, firefighting or logistic services).

3a.3.6.1300. The nuclear power plant unit shall be designed and equipped with a seismic alarm system included in Safety Class ABOS 2, on the basis of the signal of which either automatic protective operations are launched or the operator takes the necessary actions. The characteristics of the earthquake associated with the operation and actions shall be determined in both cases. If a system is established that triggers automatic protective operation in the case of an earthquake, then its structure, redundancy, diversity, physical separation and reliability shall be fit into the requirements for the protective system.

3a.3.6.1400. The nuclear power plant unit shall be designed and equipped with an earthquake-registration system included in Safety Class ABOS 3. The processing of its signals shall allow the effects of the earthquake and the safety of continued operation to be evaluated. The characteristics of the earthquake and the characteristics that are necessary for the evaluation of the condition of the nuclear power plant, which form a basis for the evaluation of continued safe operation, shall be specified in the design.

3a.3.6.1500. Special emergency operating and accident management procedures and actions shall be devised for the case of earthquakes. The organisation of the operation and service of the nuclear power plant, the evaluation of the post-earthquake condition, the scope and method of post-earthquake inspections and the conditions of restart shall be regulated in the procedures and action plans.

3a.3.6.1600. It shall be ensured that in the event of an operation-base earthquake with the same frequency as the operational events, the operation shall continue either undisturbed or if the nuclear power plant shuts down in the case of an

operation-base earthquake, it shall remain in a condition that can be restarted following the quake.

3a.3.6.1700. The systems, structures and components of the nuclear power plant with functions F1 and F2 as well as B1, B2 and B3, included in Safety Classes ABOS 1 to 3, shall also be designed and qualified for operation-base earthquakes if the peak ground acceleration value of the operation-base earthquake exceeds one-third of the peak ground acceleration value of the safety earthquake. The design, verification and qualification shall be performed in accordance with the rules and compliance criteria specified for DBC2.

II. Special internal hazard factors

3a.3.6.1800. As part of the examination of initiating events, special internal hazard factors, such as flooding, fire, explosion, high energy line break, shall be identified, the occurrence of which may influence the performance of the safety or isolation barrier function.

3a.3.6.1900. The rooms exposed to internal hazard and the systems, structures and components with safety functions potentially affected within such rooms shall be identified. The effect of the examined events shall not hinder the performance of the safety functions.

3a.3.6.2000. In the event of flooding, it shall be ensured that the spilled medium can be appropriately collected and safely released.

III. Natural hazard factors

3a.3.6.2100. In the case of events of natural origin existing for a long time, preparations shall be made for the exchange of the personnel and supplement of the equipment required for the protection measures.

3a.3.6.2200. The design parameter for design input shall be determined for all types of hazard factors associated with the design basis natural phenomena and processes characteristic to the site on the basis of the hazard curve, taking into account the screening criteria relating to the given hazard factor. The design basis parameters and characteristics shall be so determined that they ensure the avoidance of cliff edge effects by means of the design input.

3a.3.6.2300. The safe operation of the nuclear power plant shall also be ensured under circumstances of caused by external natural hazard factors. Reasonably assumable combinations of natural hazard factors shall be taken into account. The effect on the safety functions arising from the failure of systems, structures and components without a safety function due to natural hazard factors shall be taken into account.

3a.3.6.2400. For protection against design basis natural hazard factors, a comprehensive protection plan shall be developed, which ensures that the requirements of Section 3a.2.1.1000 are met.

3a.3.6.2500. The comprehensive protection plan shall be developed by taking into account the considerations in Sections 3a.2.1.2200, 3a.2.2.9100 and 3a.3.2.3800 and the following:

a) The predictability and development over time of the expected events shall be taken into account.

b) Appropriate equipment and procedures shall be provided in order to allow the confirmation of the condition of the power plant during and after the events taken into account in the design basis.

c) Preparations shall be made for events affecting more than one unit and more than one system, structure or component at the same time (in the case of a redundant system, all branches at the same time) and have an effect on the regional infrastructure, off-site services and protective measures.

d) In the case of a nuclear power plant with more than one unit, the required resources shall also be provided in the case of events where shared equipment and services need to be used in order to avoid that they adversely affect the protection established against design basis events.

3a.3.6.2600. The condition-monitoring equipment and warning signals shall be continuously operable in order to provide support to the comprehensive protection plan through the prediction of possible hazards. Where it is justified, alarm thresholds shall be determined in order to timely perform the appropriate actions. Furthermore, such intervention thresholds shall be determined, at which the pre-planned post-event interventions shall be performed.

3a.3.6.2700. In the case of systems and organisational solutions planned for averting the effects of external hazard factors, the situation where access to the site and the service and operation of the systems encounter difficulties on a permanent basis shall be taken into account.

IV. External hazard factors associated with human activities

3a.3.6.2800. If there is a radio frequency or microwave electromagnetic radiation source with a significant energy density on or in the vicinity of the site, its effect on the systems and components important to nuclear safety shall be assessed. If there is a possibility for such an effect, appropriate protective measures shall be provided.

3a.3.6.2900. The hazard factors associated with human activities and their effects on systems, structures and components with safety functions shall be considered.

Should these effects influence the performance of the safety function, protection against such effects shall be provided. The protection may also be provided through administrative tools, i.e. restricting human activities posing a hazard, but technical solutions for protection shall be preferred against these effects if such solutions can reasonably be accomplished.

3a.3.6.3000. Standard design input parameters characterising the effects of hazard factors arising from external activities shall be determined on the hazard curve in accordance with the screening criteria. The postulated hazards shall be provided deterministically, with the parameters characterising the given event.

3a.3.6.3100. The fulfilment of requirements for DEC1 shall be ensured for the case of the crash of a military or civil aircraft.

3a.3.6.3200. The consequences of a crash of a military or civil aircraft flying across the Hungarian airspace shall be analysed.

3a.3.6.3300. It shall be demonstrated that the nuclear power plant unit has built-in design parameters and functional capabilities that ensure that even after a crash of a military or civil aircraft:

a) the cooling of the active core of the nuclear reactor is not compromised or the containment is not damaged, and

b) the cooling or integrity of the spent fuel pool is maintained.

3a.3.6.3400. The analysis under Section 3a.3.6.3200 shall include:

a) specification of the affected buildings,

b) mechanical effects due to the event: the stability of the buildings, rupture of structures and vibration of, and impact to, buildings and the affected system components,

c) the effects of fire and explosion, and

d) the ability of the operating personnel to carry out the necessary activities.

3a.3.6.3500. The potential effects of transport activities in the vicinity of the nuclear power plant and the risks arising therefrom shall be analysed, with special regard to the transport of hazardous materials.

3a.3.6.3600. On and in the vicinity of the site of the nuclear power plant, the parameters of all permanent or temporary facilities, which may become a source of fire or explosion, shall be identified and determined, and it shall be evaluated to what extent it causes a hazard to the nuclear power plant. If necessary, appropriate protective measures shall be taken.

3a.3.7. Fire protection

3a.3.7.0100. Systems, structures and components important to nuclear safety shall be so designed and located that the frequency and effects of fire are minimised. It shall be ensured that the nuclear power plant can be shut down both during and after a fire, the residual heat can be removed, the release of radioactive materials into the environment can be prevented, and the operating conditions of the nuclear power plant can be monitored. In the buildings encompassing systems, structures and components important to nuclear safety, the rooms comprising redundant or diverse systems and components shall be established as separate fire sections. If this is not accomplishable, fire cells equipped with active and passive fire protection equipment shall be applied in accordance with the fire hazard analysis.

3a.3.7.0200. The buildings containing systems, structures and components important to safety shall be designed to be fireproof, taking into account the results of the fire hazard analysis.

3a.3.7.0300. Every fire section shall be equipped with a fire alarm. In the unit main control room, an informative signal shall be provided about the exact location of any fire. These systems shall be provided with uninterruptible safety power supply and appropriate fireproof cabling.

3a.3.7.0400. Built-in or mobile, automatic or manual fire extinguishing systems shall be installed, which shall be so designed and placed that their failure or unjustified operation does not significantly affect the ability to perform the safety functions of the systems, structures and components important to nuclear safety.

3a.3.7.0500. The fire extinguisher system shall ensure that the areas of the nuclear power plant important to safety are covered. Coverage shall be demonstrated by fire hazard analysis.

3a.3.7.0600. The ventilation systems shall be so arranged that in the event of a fire, each fire section can perform its separation function.

3a.3.7.0700. The parts of the ventilation systems that are situated outside of fire sections shall have the same fire resistance category as the fire section or their isolation shall be provided with fire dampers of the appropriate category.

3a.3.7.0800. The areas where a fire may cause any radioactive release shall be equipped with fire alarms and, where necessary, built-in fire extinguishing systems. The arrangement, the fire protective separations, the ventilation systems and the built-in fire extinguishing systems in such areas 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 materials are used during radioactive waste management, built-in fire extinguishing systems shall be applied and the extinguishing agent shall be effective for the combustible material.

3a.3.7.0900. The possibility and potential effects of self-ignition of radioactive wastes shall be analysed.

3a.3.7.1000. During the use and storage of an explosive medium, it shall be ensured that the protection of the affected system components corresponds to the hazard level of the medium.

3a.3.8. Decommissioning

3a.3.8.0100. The requirements for final shutdown and decommissioning of the nuclear power plant unit shall also be taken into account during design.

3a.3.8.0200 It shall be ensured that the radiation exposure of the persons present on the site of the nuclear power plant and the population as well as the radioactive releases are kept at the lowest reasonably achievable level, and the radioactive contamination of the environment is avoided during decommissioning, too. To this end, design solutions that allow the optimisation of radiation exposures expected to arise during decommissioning and keep the quantity and activity of the radioactive wastes generated at a reasonably low level shall be applied.

3a.3.8.0300. As early as in the design phase, measures shall be planned in order to mitigate radioactive leakages and releases. To this end:

a) the quantity of covered pipelines, ducts and system components embedded into concrete or laid in the ground shall be limited in the walls and floor structures, and the possibility of monitoring shall be provided in the case of covered system components,

b) the quantity of tanks, shafts and wastewater pipelines potentially containing radioactive media shall be limited, and

c) the pipelines, tanks and shafts embedded into concrete shall be made of stainless steel.

3a.3.9. Human factors

3a.3.9.0100. The working areas and working environment of the operating personnel and the human-machine relations shall be analysed from the ergonomic aspect and from the point of view of potential wrong interventions. The plans shall be prepared taking into account the results of the analyses.

3a.3.9.0200. The human-machine relations and ergonomic features of systems, structures and components shall be so designed that, taking into account 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.

3a.3.9.0300. An appropriate simulation environment shall be designed to facilitate the preparation of the operating personnel for management of DBC1-4 and DEC1 and DEC2.

3a.3.9.0400. During design, the analysis of tasks falling under the responsibility of the operating personnel and associated with the performance of safety functions shall be performed. The scheduled operator interventions and their ability to be executed with appropriate reliability shall be validated, with special regard to the management of DBC3-4 and DEC1 and DEC2. For the case of DBC3-4, the most important means of validation is the full-scope simulator. The results of such tests shall be taken into account during the elaboration of procedures and plans for the introductory training and refreshing training of personnel.

3a.3.9.0500. Ergonomic design requirements shall be specified for the design, manufacture and qualification of the operator interfaces in the conceptual design period.

3a.3.9.0600. Operating, instrumentation and control, information technology and process specialists shall be involved to support the design and monitoring of human-machine interfaces, such as control panels and screens.

3a.3.9.0700. In order for the members of the operating personnel to have such complete information, to the extent corresponding to their positions, which can be efficiently processed, in each operating mode of the nuclear power plant unit, appropriately qualified measuring instruments and traditional or computerised displays shall be placed in the relevant working areas. It shall be ensured that the instrumentation allows the measurement of all significant parameters 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 to safety.

3a.3.9.0800. An appropriate communication system shall be designed for the purpose of information flow and transfer of instructions between the different locations. The communication system shall also provide the appropriate mobility necessary for the performance of mobile activities. Communication connections shall also be provided with external organisations, the activities of which may be necessary under DBC1-4, DEC1 and DEC2.

3a.4. DESIGN OF SYSTEMS, STRUCTURES AND COMPONENTS OF KEY IMPORTANCE

3a.4.1. Design of the nuclear reactor and the active core

I. Integrity of the nuclear reactor and the active core

3a.4.1.0100. All potential influencing effects shall be taken into account during the design of the structure of the active core and the internal components of the nuclear reactor. The safe operability shall be demonstrated by taking into account especially the deformation and stresses caused by irradiation, chemical and physical processes, static and dynamic mechanical loads and temperature as well as manufacturing tolerances and changes occurring during the lifetime.

3a.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 displacement and vibrations leading to damage of the entire core structure and components within the structure.

3a.4.1.0300. The nuclear reactor and its structural components shall be so designed that they can be assembled only in one way, and the reinstallation in the wrong order or the placement of an inappropriate system component can be excluded.

3a.4.1.0400. The design or the manufacturing process shall provide an 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.

3a.4.1.0500. The nuclear reactor and the active core shall be so designed that in the case of events resulting in DBC1-4 and DEC1, the mechanical failures of the systems, structures and components of the nuclear power plant unit and the physical behaviour of the coolant of the nuclear reactor shall not hinder the shutdown, the maintenance of the subcritical condition and the cooling of the nuclear reactor.

3a.4.1.0600. The measuring systems installed in the active core shall ensure the sufficiently accurate and continuous determination of the parameters necessary for monitoring the fulfilment of the Operational Limits and Conditions. The necessary parameters shall be provided on the basis of regularly obtained measurement information or by the combination of measurements and calculations.

3a.4.1.0700. The nuclear characteristics of the active core shall be such that changes in temperature, loss of the coolant, boron dilution or geometric changes in the active core in DBC1-4 and DEC1 shall not cause a reactivity increase of an uncontrollable extent.

3a.4.1.0800. In the shutdown state and during the refuelling of the nuclear reactor, it shall be ensured that the subcriticality continuously remains at the prescribed level even during the placement of fission materials or absorbents in the active core or their removal from there.

3a.4.1.0900. During the design of the active core and its components, it shall be ensured that slight changes in some core parameters do not cause significant unfavourable changes in DBC1-4 and DEC1.

3a.4.1.1000. The design of the active core shall ensure that following an event resulting in DBC1-4 and DEC1, the fuel assemblies can be removed with operational tools from the nuclear reactor.

3a.4.1.1100. It shall be prevented by appropriate design that the unplanned removal of any part of the active core from the core or its displacement within the core as well as the entry of any foreign body into the core can cause an unplanned increase in reactivity or a blockage of the coolant flow.

3a.4.1.1110. Components that measure the neutron flux distribution in the reactor core and its changes shall be arranged in such a manner that provide the controllability of the parameters of the conditions and limits related to the neutron flux distribution of the core and its changes.

3a.4.1.1120. The due accuracy implementation of the first and post-refuelling reactor-physical startup measurements shall be ensured during the design of the measurements system with the reasonably achievable lowest number of correction factors.

II. Control of reactivity

3a.4.1.1200. The shutdown of the nuclear reactor and the control of its reactivity shall be ensured by at least two systems that operate according to different principles and provide an F1A safety function, of which at least one shall be able by itself to shut down the nuclear reactor from DBC1-4. At least one of the shutdown systems shall be automatic and quick-actuation, which, if the pre-determined conditions are met, shuts down the nuclear reactor with high reliability in an uninterrupted manner regardless of the activities of the operating personnel. The reactor protection system generating the protection signal giving an instruction for a quick shutdown of the reactor shall also perform its task even if one of the branches of the system fails and, simultaneously, another branch is also inoperable due to maintenance or testing. In addition, both shutdown and control systems shall be single failure tolerant, even in the case of failure of any electric power supply or the inoperability of the control rod assembly of the highest worth.

3a.4.1.1210. The shutdown and control equipment shall be suitable to avoid each such foreseen reactivity increase that could lead to inadvertent criticality during the shutdown, in shutdown state or during refuelling.

3a.4.1.1220. Regular inspection of ageing of the neutron detectors installed for monitoring the state of the active reactor core with protection, control or diagnostic functions shall be provided.

3a.4.1.1300. The reactivity control of the active core shall be achieved with a combination of fuel enrichment, control and safety rods, dissolved and burnable reactor poisons, which ensure the avoidance of re-criticality or sudden reactivity changes in and following DBC1-4 and DEC1.

3a.4.1.1400. In the case of some of the assumed initiating events where it is necessary to shut down the reactor quickly, the protection signals shutting down the nuclear reactor shall be so developed that the protective operation occurs when the limit value of either one of two different, independent physical parameters, which are individually measured with appropriate redundancy, is exceeded. The outcome of the event sequences in the case of such transients shall not be significantly dependent on which physical parameter triggers the reactor protection.

3a.4.1.1410. The reactor protection shall be fail safe and shall be capable of overwriting the non-safe intervention of the control system.

3a.4.1.1500. It shall be ensured by the appropriate design of the systems controlling reactivity and shutting down the nuclear reactor that in DBC1-4, it is excluded that the safety limits applicable to the temperature of the nuclear fuel and coolant and to other physical parameters are exceeded.

3a.4.1.1600. The power coefficient of reactivity of the active core shall remain negative in DBC1-4 and DEC1.

3a.4.1.1700. The systems controlling reactivity and shutting down the nuclear reactor shall be so designed that the extent and rate of reactivity increase cannot exceed the design limit even in the case of operation outside design limits.

3a.4.1.1800. Subcriticality shall be ensured and maintained during any phase of the storage and transport of fuel elements.

III. Design of fuel assemblies

3a.4.1.1900. The entire life cycle of fuel assemblies shall be planned, and the fulfilment of the nuclear safety requirements shall be demonstrated in each phase, taking into account all the expected effects, from the arrival of fresh fuel assemblies to the interim storage of spent fuel assemblies, including management and transport processes.

3a.4.1.2000. The nuclear fuel shall be so designed that it shall not exclude the possibility of recycling or safe final disposal.

3a.4.1.2100. Under the conditions of normal operation, the leakage of fission products from irradiated fuel rods shall be kept at the lowest practicable level. Operating limits shall be set for the extent of allowable leakage.

3a.4.1.2200. During design, methods shall be provided for the identification and special treatment of failed fuel assemblies in order for the radiation protection, nuclear safety and safeguards requirements for DBC1 to be fulfilled.

3a.4.1.2300. The fuel assemblies shall tolerate all effects arising from deterioration processes without a failure exceeding the extent allowable under the Operational Limits and Conditions, taking into account the maximum allowable burn-up.

3a.4.1.2400. It shall be ensured by appropriate design that flow-induced vibrations and displacement cannot damage the fuel rods.

3a.4.1.2500. During the operation of the nuclear power plant unit, new types of fuel assemblies can be introduced only following the demonstration of the fulfilment of the original design requirements. In the absence of relevant reference, i.e. problem-free application at a similar nuclear power plant, under the same usage conditions, the application of introductory fuel assemblies shall be required.

3a.4.1.2600. In the case of different fuel assembly, the specification of, and compliance with, the design requirements of the fuel assemblies and the models describing the behaviour of the nuclear fuel shall be validated by experimental results.

3a.4.1.2700. In the case of different fuel assembly, in addition to the specifications in Sections 3a.4.1.1900 to 3a.4.1.2500, the following shall be presented to demonstrate the safety of fuel elements:

a) the results of experiments based on which the limits of the individual design requirements can be fulfilled with a sufficient margin,

b) the results of inspections examining the post-operation condition of the fuel,

c) the results of test-bench measurements verifying the ability to comply with the strength requirements of the structural elements of the fuel assembly, and

d) the validation of the codes describing the behaviour of the nuclear fuel also based on the experimental results above.

3a.4.1.2800.

3a.4.1.2900. The assemblies shall maintain their vertical situation in every position of the active core, even without lateral support.

3a.4.1.3000. The cladding of the fuel assemblies shall be designed to be resistant to the wearing effect of foreign objects that may get into the primary circuit.

3a.4.1.3100. The fuel assemblies shall be so designed that possible deposits and foreign objects should not prevent access by the coolant.

3a.4.1.3200. The swelling of fuel due to radiation shall be taken into account in the designs of the fuel elements and fuel assemblies.

3a.4.1.3300. During the design of the fuel, the extent of maximum burn-up, the requirement for manoeuvring, the maximum time to be spent in the core, expected manufacturing defects, considerations of handling and storage outside the core, in particular, subcriticality and radiation protection, shall be taken into account.

3a.4.1.3400. Fundamental functional requirements:

a) maintaining the axial and horizontal position,

b) appropriate compactness,

c) compliance of the operation of the control rod assembly (speed, stopping),

d) design and selection of materials corresponding to the conditions within the core (flow, chemical medium, vibration and irradiation), and

e) unloadability.

3a.4.1.3500. The requirements shall be developed to a level of detail that ensures that the fuel assemblies are compatible with the design basis, each other, the other components of the core, the fuel handling methods and the spent fuel management facilities even in the case of several different manufacturers.

3a.4.2. Design of the main circulation loop

3a.4.2.0100. The system components in the main circulation loop shall bear all static and dynamic loads, which affect these system components in DBC1-4 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 condition.

3a.4.2.0200. During design, the effects expected during operation on the system components during their lifetime, including effects from the erosion, elongation, fatigue, radioactive and chemical environment and all uncertainties in the determination of the initial condition of the properties of the system components and their possible deterioration due to ageing shall be taken into account. Accordingly, the system components of the main circulation loop shall be designed with sufficient margins, while it shall also be demonstrated that the robust design does not lead to disadvantages in DBC3-4 and DEC.

3a.4.2.0300. The selection of the material and the designs of the main circulation loop shall allow the application of the concept of leak before break.

3a.4.2.0400. The main circulation loop, as a pressurised system, which contains the primary circuit coolant and provides a B1 function, shall be so designed that:

a) the possibility of high energy line break shall be excluded to the possible maximum extent;

b) the conditions for detection of leak before break and the respective action shall be met, and in the event of possible leakages, it shall be ensured that their growth is slow in order to allow sufficient time for detection and intervention;

c) in the event of the rupture of connecting pipelines, the closure of the main circulation loop shall be ensured by installing two gate valves in each pipeline, which are positioned near the main circulation loop; and

d) the continuous monitoring of the integrity of the main circulation loop shall be ensured.

3a.4.2.0500. During the selection of materials for the main circulation loop, the minimisation of the activation of structural materials during operation shall be ensured, with special regard to the decommissioning considerations of the nuclear power plant.

3a.4.2.0600. In the case of the internal structural components of the main circulation loop, the possibility of failures that may result in damage to other main circulation loop components due to loose objects, shall be decreased to a minimum.

3a.4.2.0700. 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 in the design, and equipment shall be provided to monitor and localise the leakages.

3a.4.2.0800. The heat exchanger tubes of the steam generators shall be welded into the tube wall 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 wall.

3a.4.2.0900. The heat exchanger tubes of the steam generators shall be fixed in order to decrease the deterioration caused by vibrations. The tube supports shall be so designed as to allow the least wear and deposits from the operational medium between the heat exchanger tubes and the support. The heat exchanger tubes shall be made of a wear-resistant material.

3a.4.2.1000. The heat exchanger tube bundles of the steam generators shall be so sized as to allow for sufficient margins to be available to compensate for plugged and clogged heat exchanger tubes even at the end of the design lifetime.

3a.4.2.1100. During the design, the place of the welds shall be so determined to ensure the accessibility for in-service inspection purposes, and the construction of the welds and the environment shall be such that the material testing activities on the weld can be performed easily and with high reliability.3a.4.2.1200. It shall be ensured that the internal design of the secondary side of the steam generators allows the efficient removal of deposits, the prevention of the entry of foreign objects from secondary circuit pipelines and the efficient removal of water droplets from the steam.

3a.4.2.1300. The sizes of the water and steam spaces of the steam generators shall be specified with sufficient margins to allow compliance with the operating limits specified for the primary and secondary circuits in all DBC1.

3a.4.2.1400. The sizes of the water and steam spaces of the pressurizer shall be specified with sufficient margins in order to ensure the compliance with the operating limits specified for the primary circuit in all DBC1.

3a.4.2.1500. The primary circuit shall be provided with appropriate overpressure protection. Pressure control systems shall be designed to handle the effect of changes in volume due to temperature changes in the primary coolant circuit, while also considering the following requirements:

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

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

c) pressure reduction shall be ensured in accident situations,

a) replaceable operational heating elements in the pressurizer and such independent operational injection pipes shall be applied, the nozzles of which can be easily inspected and replaced;

e) an emergency injection system that is entirely independent of the operational injection system shall be designed;

f) for the arrangement of the pipes connecting the pressurizer to the main circulation pipeline, attention shall be paid to thermal stratification and the possibility of external and internal inspection;

g) a leakage detection system that is capable of detecting leakages with appropriate accuracy and within the shortest possible time and determining their extent and that can provide assistance in the determination of the location of a

leakage shall be designed for the main circulation loop. The leakage detection system shall be single failure tolerant.

3a.4.3. Heat removal

3a.4.3.0100. All 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 medium shall be ensured by the application of heat transfer systems and components.

3a.4.3.0200. The cooling of the active core shall be ensured, and to this end:

a) forced circulation shall be provided for the removal of the generated heat or residual heat from the rated capacity of the nuclear reactor to its cooled down condition; and

b) natural circulation cooling of sufficient efficiency shall be ensured in the main circulation loop, which ensures the removal of residual heat from the active core when forced circulation is shut down.

3a.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 if the connection of smaller pipes below this level is unavoidable, it shall be demonstrated that the reactor vessel cannot be emptied below the top of active part of nuclear fuel in shutdown conditions,

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

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

d) it shall be ensured by the removal of non-condensable gases that they cannot hinder natural circulation, and

e) the possibility of removing corrosion products and depositions shall be ensured to avoid the blockage of the flow routes and thereby endanger the coolability of the active core.

3a.4.3.0400. The steam generators shall be so designed that they provide appropriate cooling for the nuclear reactor in DBC1-4 and DEC1.

3a.4.3.0500. Under DBC2-4, the removal of the residual heat from the reactor, the spent fuel pool and the containment shall be ensured by means of one or

more redundant heat removal systems in such a way that jointly they are capable of performing heat removal even if one of the systems or a redundant branch of a system is lost due to a failure and, simultaneously, another system or redundant branch is inoperable due to maintenance or testing. If the heat removal system or its service system contains passive design solutions, for which an extremely low probability of failure can be demonstrated for the given operating condition, it is sufficient to design the passive system components to be single failure tolerant.

3a.4.3.0600. Sufficient and diverse heat removal solutions, which are also independent in respect of power supply, shall be provided for the removal of the residual heat from the reactor and the spent fuel pool. At least one design solution shall perform its function also during DEC events caused by external hazard factors.

3a.4.3.0700. It shall be ensured that under DBC2-4, the limits set for a given operating condition with respect to either the fuel elements, fuel assemblies or the pressure retaining equipment and pipelines of the primary circuit are not exceeded.

3a.4.3.0800. It shall be demonstrated that if the cooling capability of the fuel elements designed for DBC1-4 and DEC1 is lost, sufficient time is available to start the alternative cooling of the fuel elements.

3a.4.3.0900. In addition to the heat removal systems described in Sections 3a.4.3.0500 and 3a.4.3.0600, an additional independent heat removal solution shall be provided for DEC2. Systems used for managing other operating conditions can also be used for heat removal if they remain operational and suitable for operation under DEC2.

3a.4.3.1000. In the case of systems containing irradiated fuel assemblies, such as the shutdown nuclear reactor or spent fuel pool, capabilities shall be provided for passive heat removal.

3a.4.3.1100. If the capability of transferring the residual heat to the ultimate heat sink cannot be demonstrated for every operating condition with high reliability, a secondary ultimate heat sink and systems required for its operation shall be provided, which ensure through their location and design solutions that the heat removal safety function is not lost as a result of external hazard factors.

3a.4.3.1200. The nuclear power plant shall have an emergency core cooling system, which is capable of handling processes resulting in the loss of coolant, which may arise in the primary circuit and the systems connected to it and which is taken into account during design, and is capable of providing appropriate cooling for the fuel.

3a.4.3.1300. The operability and efficiency of the emergency core cooling system shall be ensured by an appropriate primary circuit configuration and the appropriate placement of the connection points of the emergency core cooling system.

3a.4.3.1400. The emergency core cooling system shall be so designed that it is capable of removing the residual heat for the necessary time. To achieve this, among others, the recirculation of the coolant discharged from the primary circuit to the reactor shall be ensured. During the design of the recirculation system, special attention shall be paid to the adverse effects of the solid and chemical contamination that gets into the discharged coolant. In order to avoid that such contamination damages the recirculation system and the reactor, appropriately sized filtering equipment (sump filters) shall be installed. The suitability of the filtering equipment shall be demonstrated by experiment. During the design of the filters, the following shall be taken into account:

a) the ratio of contamination passing through or bypassing the filter should be sufficiently low as not to jeopardise the operation of the recirculation system and the efficiency of the cooling of the reactor;

b) the drop in pressure caused by contamination and caught by the filtering equipment shall not prevent the operation of the recirculation system or significantly reduce its efficiency;

c) it shall be ensured that the filtering equipment can be cleaned by reverse flow or gas injection in order to avoid its clogging.

3a.4.4. Unit main and backup control rooms and technical support centre

3a.4.4.0100. A unit main control room shall be established within the nuclear power plant unit, from where activities aimed at the operation of the nuclear power plant unit, its maintenance in a safe condition or its return to such condition, can be performed in DBC1-4, DEC1 and DEC2. The most up-to-date ergonomic considerations and principles shall be taken into account during the design of the unit main control room.

3a.4.4.0200. Sufficient display and archiving and actuating devices shall be available for the operating personnel in the unit main control room for DBC1-4, DEC1 and DEC2 plant states for the following purposes:

a) appropriate monitoring of the condition of the nuclear power plant unit and its systems, structures and 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 actuated, their subsequent actuation, and

d) development of an overall picture of the processes of the nuclear power plant unit.

3a.4.4.0300. A backup control room shall be established at the nuclear power plant unit at a location functionally independent of the unit main control room, which is also separated from it both physically and with regard to its electrical system, where sufficient instrumentation and control instruments shall be installed for condition monitoring and interventions, to ensure that if the normal use of the unit main control room became impossible for any reason:

a) the reactor can be shut down, cooled down and maintained in a safe shutdown condition for unlimited time; and

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

3a.4.4.0400. The functionality of the backup control room shall be provided by regular inspection.

3a.4.4.0500. There shall not be computers, in particular, personal computers and servers, in the unit main and backup control rooms; they shall be placed in rooms other than the control rooms. Entry in such rooms shall be detected, and it shall be signalled and archived in the unit main and backup control rooms.

3a.4.4.0600. Stand-alone accident management panels with identical functionality shall be installed in the unit main control room and the backup control room. Information required for the implementation of the recommendations of the accident management guidelines in DBC4 and DEC1 and DEC2 plant states and the intervention options required for accident management shall be provided at these locations.

3a.4.4.0700. It shall be ensured that during the internal or external events in DBC1-4, DEC1 and DEC2, the unit main control room and the backup control room shall not become unsuitable for use simultaneously, and that the unit main control room and the backup control room are suitable (habitable) for ensuring the long-term presence of the operating personnel in them.

3a.4.4.0800. Receiving and display of the necessary information shall be provided in the unit main and backup control rooms, allowing the timely evaluation of the condition of the nuclear power plant unit and the critical safety functions in DBC2-4 and DEC1 and DEC2, too.

3a.4.4.0900. A continuous and uninterruptible power supply shall be provided for the systems and components of the unit main and backup control rooms, which perform safety functions.

3a.4.4.1000. Technical solutions that exclude the possibility of the simultaneous operation of systems and components from the unit main control room and the backup control room shall be applied. 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. A signal shall be provided in the other control room about any attempt to use a control room.

3a.4.4.1100. The identification of potential events within or outside the unit main and backup control rooms, which may directly endanger the personnel working there or the continuous use of the control room, shall be managed as a priority. During design, reasonably achievable measures, which minimise the effects of such events, shall be defined.

3a.4.4.1200. The unit main and backup control rooms shall be located in separate fire sections, which allows the safe shutdown of the nuclear reactor and the maintenance of safety functions necessary in a shutdown condition also in the case of fire occurring in the surrounding rooms.

3a.4.4.1300. An appropriate passageway shall be provided between the unit main and backup control rooms.

3a.4.4.1400. The following requirements shall be taken into account during the design of the unit main and backup control rooms:

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

b) the logical functional classification of the displayed information and the actuating devices shall be provided, with special regard to ensuring that the classification of information and interventions is not contradictory, and

c) it shall be ensured that no unnecessary or insignificant information is displayed.

3a.4.4.1500. The following requirements shall be taken into account during the design of the unit main control room in accordance with Section 3a.4.4.0100:

a) option for the screen-based monitoring of systems and processes and high-capacity computer technology devices 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 main control room personnel, and

c) the following shall be provided in the safely accessible and manageable proximity of the unit main control room personnel:

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

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

cc) information from fire alarm systems and the operation of certain fire extinguishing systems of special importance,

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

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

cf) equipment for controlling and restricting access to the unit main control room.

3a.4.4.1600. The following requirements shall be taken into account 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 account the expected instances of use of the backup control room,

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

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

ca) appropriate placement of the personnel required for operation,

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

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

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

3a.4.4.1700. An accident technical support centre shall be established in a space separated from, but appropriately close to, the unit main control room in such a way that its location allows oral communication between operators and specialists assembling for supporting the work of operators, but their work shall not disturb the personnel of the unit main control room.

3a.4.4.1800. An emergency technical support centre, which is independent of the unit main control room, the backup control room and the accident technical support centre shall be established in the Emergency Command Centres determined in Sections 3a.7.1.0300.-3a.7.1.0500., from where technical support can be provided to the operating personnel in the DBC1-4 and DEC1 and DEC2 of the units. The centre shall remain operable and available for safe use by the personnel in the DEC1 and DEC2 of the units.

3a.4.4.1900. At both the accident and emergency technical support centres, access shall be provided to the operating parameters of the nuclear power plant

and the radiation data of the nuclear power plant and its immediate vicinity. The centres shall be provided with equipment suitable for communication with the unit main control room, the backup control room and all locations of the power plant that are important from the point of view of accident management and emergency response. Sufficient space shall be provided at the centres for the work of the specialists assembling to support the operating personnel. The following shall be available at the centres:

a) a complete data archive on a unit process computer, starting at least one day prior to the situation requiring accident management and with continuous updates;

b) complete technical documentation of the facility;

c) data on the personnel present on site, required for accident management, and

d) on-line and archive data of an external environmental monitoring system.

3a.4.5. Electrical systems, instrumentation and control

I. Electrical systems and equipment

3a.4.5.0100. It shall be ensured that the power supply system of the nuclear power plant unit is able to supply the safety systems and components with electricity necessary for operation, assuming single failure and the loss of off-site voltage.

3a.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.

3a.4.5.0300. The power supply to systems and components important to nuclear safety shall be designed in accordance with their safety classes and graded requirements.

3a.4.5.0400. In DBC1-4 and DEC1, the planned electrical load on the electrical systems and components shall not exceed their maximum allowable load capacity. The limitations with regard to the electric load of systems and components shall be provided in the design specification. On the basis of these, the quantity, quality and power of the electricity sources required for the operation of safety systems shall be determined, taking into account the possible common cause failures and the required operating period.

3a.4.5.0500. An appropriate power supply shall be provided for the cases of DEC plant states in accordance with the required interventions and timeframe established by DEC analyses, taking into account external and internal hazard factors.

3a.4.5.0600. The design basis shall contain appropriate actions for the management of events occurring in the normal power supply system of the nuclear power plant unit, in such a way that the safety of the nuclear power plant unit can also be guaranteed in such situations.

3a.4.5.0700. In addition to safety classification, the power supply systems and components shall also be grouped with respect to allowable electric power failure. The electricity supply network of the nuclear power plant unit shall be designed on the basis of these.

3a.4.5.0800. The characteristics of uninterruptible power supply and the duration of allowable loss of essential energy supply shall be determined by safety substantiation. Batteries performing a function under DEC1 and DEC2 plant states shall have an appropriate capacity until they can be recharged or until another power supply solution can be provided.

3a.4.5.0900. When operational power supply is lost or its parameters exceed the acceptable range, the safety power supply systems shall automatically switch to backup supplies within an appropriate time.

3a.4.5.1000. Fixed redundant equipment providing safety power supply independent of the external electricity grid shall have a design that is independent of the service systems of the nuclear power plant to the possible extent.

3a.4.5.1100. For the power supply of systems and components important to nuclear safety, interlinked electrical connections may only be established in such a way that incorrect operational or maintenance actions shall not result in an inadvertent loss of function.

3a.4.5.1200. In the case of a nuclear power plant with more than one unit, direct electrical connection between the units shall be provided to the extent reasonably achievable in such a way that the propagation of possible failures from one unit to another can be practically eliminated.

3a.4.5.1300. An electricity source shall be designed for DEC1 plant state, which:

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

b) is able to provide an appropriate power supply to prevent a DEC2 plant state and to mitigate its consequences in the case of a station blackout.

II. Instrumentation and control

3a.4.5.1400. Instrumentation suitable for the measurement of parameters necessary for monitoring fundamental safety functions shall be provided, 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 DBC2-4 and DEC1 and DEC2.

3a.4.5.1500. Started F1A and F1B functions shall not be stopped, they shall finish.

3a.4.5.1600. The operation of software running in programmable ABOS 2 systems and components shall be deterministic, and the cycle time of its running shall not depend on the combination or rate of change of input signals. No real time or timing between redundancies and diversities or synchronisation mechanism shall be used in an ABOS 2 system.

3a.4.5.1700. Monitoring and measurement instrumentation shall be provided for the observation of the locations where radioactive materials are present and for the measurement of their quantities in all locations where they may be released into the environment.

3a.4.5.1800. The results of scientific and technological development shall be applied during the design of instrumentation and control. Modern equipment, but about which appropriate operating experience is available shall be used. The use of technologies the production of which is ceased shall be avoided. During the design of systems, the relatively short life cycle of instrumentation and control systems and the possibility of subsequent safety enhancement shall also be taken into account. Accordingly, sufficient reserve capacities shall be designed according to the following considerations: there shall be

a) sufficient free space in the electronic rooms and cabinets,

b) free standard connection facilities for subsequent development,

c) free memory and processing capacities in the computers, and

d) sufficient backup data transmission capacities.

3a.4.5.1900. Instrumentation and control systems shall be so designed that they can be simply refurbished even several times during the operating time of the unit. The refurbishment strategy to be applied for instrumentation and control systems during the operating time of the unit shall be described in the construction licence application.

3a.4.5.2000. In the case of ABOS 2 and ABOS 3 systems, it shall be demonstrated with a certificate that the instrumentation and control platform used has been examined by a specialised, independent and accredited certification body, and it has been qualified to be fault free and suitable for being used in the safety systems of the nuclear power plants. In the case of programmable instrumentation and control, the certificate shall also demonstrate the compliance of the software and hardware platforms as well as the development tools and code generators.

3a.4.5.2100. In the case of systems included in Safety Classes ABOS 2 and ABOS 3, the following verification analyses shall be carried out:

a) deterministic analysis for the demonstration of protection against single failure,

b) analysis of hardware and software failure modes and effects,

c) function and task analyses for establishing human-machine relations and the level of automation,

d) analysis of common cause failure possibilities, in particular, the ones relating to specification, design, fabrication, software and hardware, environmental impacts, maintenance problems, the use of an identical system or component in different levels of defence in depth, architecture, separations and sufficient diversity,

e) probabilistic reliability analysis,

f) test coverage analysis.

3a.4.5.2200. Facilities subject to strict administrative monitoring shall be provided for changing systems or system components important to nuclear safety, their instrumentation and control configuration, operating logic or the data associated with them.

3a.4.5.2300. Appropriate hazard signals that allow intervention by the operating personnel before the given parameters would reach the set values triggering the operation of the safety protection systems shall be applied. The signals associated with protection operations or important parameter deviations shall be supplied with sound alarms both in the unit main and backup control rooms. The signals associated with protective operation shall be acknowledgeable only by the intervention of the operating personnel even after the limit is no longer exceeded.

3a.4.5.2400. Instrumentation associated with safety parameters shall ensure the recognition of the faulty condition of both the measurement and the processing system.

3a.4.5.2500. Appropriate monitoring and control equipment shall be used to prevent the violation of the Operational Limits and Conditions.

3a.4.5.2600. Such instrumentation, data processing, display and archiving system shall be established that is independent to the extent reasonably achievable, is suitable to provide information regarding the condition of the nuclear power plant unit even under the environmental circumstances of DEC2 plant states, to the extent of the guidelines developed for such situations and internal instructions.

3a.4.5.2700. The instrumentation and control systems shall ensure:

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

b) comprehensive and accurate information, which is available within the required time, about the condition of the nuclear power plant for the operating personnel,

c) actuating and monitoring devices,

ca) for the supplementation of failed automatic operations,

cb) for manually or automatically bringing the nuclear reactor in a safe shutdown condition and for maintaining it in such a condition under the circumstances of DBC1-4 and DEC1,

cc) for the safety interventions that do not belong to the scope of automatic safety operations,

cd) for manual interventions necessary for accident management, and

d) an appropriate data storage and recording system to allow the later investigation of the details of a transient and accident.

3a.4.5.2800. The requirements for the accuracy, response time, event sequence determination, processing capacity reserve and communication capacity reserve of instrumentation and control systems shall be specified consistently with the design basis of the nuclear power plant.

3a.4.5.2900. It shall be ensured that the safety instrumentation and control system detects DBC1-4 and DEC1 and shall ensure, in accordance with the condition:

a) the shutdown of the nuclear reactor,

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

c) the activation of supporting functions.

3a.4.5.3000. In the case of commands leading to an executive device and associated with various safety levels, priority shall be provided for the higher safety level command. Any deviation therefrom shall be demonstrated by analysis. The safety class of the system component ensuring priorities shall be established from the safety level of the command belonging to the highest level safety function handled by it.

3a.4.5.3100. All data important to safety shall be archived. A time stamp shall also attached to the data. The time stamp shall be generated the closest to its generation in the data stream, as early as possible. The archive shall be retained until the end of the operating time of the units.

3a.4.5.3200. The process functional specification of the instrumentation and control systems shall comply with the following requirements:

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 classify the management tasks in functional safety levels on the basis of the importance of the given task to safety and shall assign them to the appropriate level of defence in depth,

d) it shall determine the independence criteria associated with the functions, including diversity requirements,

e) it shall determine the response times associated with the functions,

f) for each output, it shall determine a safety condition or position that the output should assume in the case of its detected error,

g) it shall determine the tasks that require operator intervention in the DBC1-4 and DEC1 of the nuclear power plant in such a way that the operating personnel are able to perform them,

h) in addition to a description in a human language, it shall use an appropriately structured, formal language description method,

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

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

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

l) it shall determine the expected reliability requirements, and

m) in the case of programmable instrumentation and control systems included in the Safety Class ABOS 2, it shall determine simulation methods for their functional monitoring and validation.

3a.4.5.3300. The design and implementation of programmable instrumentation and control systems and components shall be carried out according to the standards selected for systems and components of the relevant safety class and to the graded requirements.

3a.4.5.3400. Data exchange between the digital design tools and databases used during the design of instrumentation and control shall be carried out in an automated way. An effort shall be made that one piece of data is stored in one

place in a consistent data structure. Modern development tools that have the following functions shall be used for the design of programmable systems and components:

a) programming,

b) code generation,

c) documentation,

d) code analysis, and

e) simulation and testing.

3a.4.5.3500. In the case of digital systems included in Classes ABOS 2 and ABOS 3, it shall be documented that the generated user software code has been read back, then the analysis of the code read back has demonstrated that the code generation process did not enter any error. All operations in the development, design, manufacturing and implementation stages shall be documented in detail. Any document can be subjected to inspection by the authorities or evaluation by experts throughout the lifetime of the facility.

3a.4.5.3600. 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.

3a.4.5.3700. The ABOS 2 systems and components shall not communicate with a system outside the given unit, and shall provide data to a system or component of the same unit in a lower safety class only via a physically one-way communication channel.

3a.4.5.3800. An instrumentation and control system connected to the technology shall provide data to the instrumentation and control system of another unit or to external systems only via a physically one-way data connection.

3a.4.5.3900. An ABOS 2 system shall be connected to instrumentation and control systems in a lower class for the purpose of exporting data only via a physically one-way communication channel. In the case of diagnostic tools and equipment used for repair service purposes, it shall be demonstrated that the entry of inadvertent or malevolent commands in the safety system is excluded from the direction of the connected diagnostic tools and equipment used for repair service purposes. In the case of ABOS 3 systems, it shall be demonstrated that the entry of inadvertent or malevolent commands is excluded from the direction of the connected systems and components included in lower classes.

3a.4.5.4000. The subsystems of the instrumentation and control systems in Safety Class ABOS 2 shall be redundant to an extent sufficient for the fulfilment of

the required failure tolerance. The functionality of redundant stocks shall be as identical as possible while applying the intended diversity.

3a.4.5.4100. The architecture of the instrumentation and control systems shall fit into the levels of defence in depth. The levels fitting into defence in depth shall be separated from each other to the extent reasonably achievable.

3a.4.5.4200. Non-safety functions or functions assigned to lower functional safety levels shall not be integrated into a subsystem included in a safety class or in a safety class that is higher than necessary. If this is not possible, it shall be demonstrated by safety analysis that the subsystem performing a function in a lower safety class does not, in any way, hinder the performance of any function in a higher safety class.

3a.4.5.4300. In the case of connections between instrumentation and control systems included in different safety classes, it shall be demonstrated 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 instrumentation and control systems in the same safety class, it shall be demonstrated that the failure of one of the systems does not hinder the performance of the autonomic safety functions of the other.

3a.4.5.4400. The continuous maintenance of single failure tolerance shall be ensured in respect of the F1A, F1B and F2 functions. Loss of an F1A, F1B or F2 function is impermissible even in the case of maintenance or manually started testing. In the case of F1A and F1B functions, a single failure shall not cause false operation either. It shall be demonstrated that the applied architecture complies with the reliability requirements.

3a.4.5.4500. All components of the instrumentation and control systems included in Safety Classes ABOS 2 and ABOS 3 shall have an automatic self-check capability. If a failure is detected during self-check, a signal shall be generated for the operator and, if necessary, the outputs of the subsystem shall be directed in a pre-determined condition leading to safety in accordance with the specifications of Section 3a.4.5.3200.

3a.4.5.4600. A manually initiated automated testing opportunity shall be provided for the detection of failures of the instrumentation and control systems included in Safety Classes ABOS 2 and ABOS 3, which cannot be detected by self-check, and for the demonstration of the operability of the safety functions. Built-in tools shall be used for carrying out automated testing, which can be initiated manually. The suitability of the testing cycle time shall be demonstrated by the application of safety analysis.

3a.4.5.4700. In the case of instrumentation and control systems included in Safety Class ABOS 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 requirements. It shall be verified by analysis that the probability of common cause failures is sufficiently low with the selected solution.

3a.4.5.4800. Requirements shall be specified in accordance with the design basis of the nuclear power plant for the probability of an operation failure when actuation is requested and, in the case of instrumentation and control systems included in Safety Class ABOS 2, relating to the frequency of false operation.

3a.4.5.4900. The instrumentation and control systems and components included in safety classes shall be fully tested in the given environment, with the preliminary determination of the testing and acceptance criteria, as follows:

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 these 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 of 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.

3a.4.5.5000. It shall be ensured by appropriate design solutions and measures that the instrumentation and control systems may only be accessed, both physically and logically, only by persons required and allowed to do so and only at a level and with the options that allow the performance of the tasks assigned to them.

3a.4.5.5100. When a commercial product is applied, it shall have specific and type identification and an appropriate qualification from an appropriate, accredited testing organisation to demonstrate that the product meets the requirements derived from the design basis.

3a.4.5.5200. The instrumentation shall provide information on the condition of safety functions and the process systems required for the management of the operating condition even under the circumstances of DBC1-4, DEC1 and DEC2.

3a.4.5.5300. During the design of programmable instrumentation and control, the relevant parts of the Basic Design Threat and the provisions of the Govt. Decree on the physical protection of use of atomic energy shall also be taken into account.

3a.4.5.5400. The protection considerations of programmable systems shall also be taken into account in the design. If, during design, the protection considerations of nuclear safety and the programmable systems are in conflict, the consideration of nuclear safety shall take priority.

III. Requirements for the safety design of information technology and instrumentation and control

3a.4.5.5500. In the Preliminary Safety Analysis Report and the Final Safety Analysis Report, in connection with the instrumentation and control of the nuclear power plant unit, the physical possibilities of modification in functions, programs and data, as well as of access posing a risk to information technology and instrumentation safety shall be defined, with a distinction of rigid wiring, including the logic manufactured with semiconductor-based circuits, and programmed instruments. These options shall be ranked by feasibility and the level of expertise necessary to achieve the modification and the interventions shall be designed accordingly.

3a.4.5.5600. The irregularities of programmable equipment shall be detected. It shall be ensured that the program and the constant data files can be checked

according to reliable data generated during installation and read from non-rewritable data carriers. Where it is reasonably achievable, the credibility of the data read from the technology shall be examined.

3a.4.5.5700. The systems and equipment that operate executive devices belonging to protection and safety systems and that provide functions collecting and displaying data important to nuclear safety, which influence the decisions of operating personnel, shall be protected against external influences, which allow the alteration of a safety function.

3a.4.5.5800. The possibilities of physical access and the placement of the data transmission equipment and data cables shall be designed in accordance with the physical protection zones.

3a.4.5.5900. The necessary administrative system and the safety protocol of the associated internal procedure and access shall be developed for:

a) the performance of maintenance necessary in the systems,

b) the necessary modification of the digital systems,

c) the detected program and data errors, and

d) monitoring of the inward and outward transport of data carriers.

3a.4.5.6000. Configuration management of instrumentation and control shall also cover the following areas:

a) documentation of the system and components, also in the case of commercial products,

b) hardware documentation,

c) all forms of software documentation and codes, among others, specifications, design documents, source codes, executable codes, computer codes and directories,

d) development systems, including core generators, translator programs, test environments and test tools,

e) test cases and results,

f) modifications and related analyses, and

g) training materials.

3a.4.6. Containment and its systems

I. Design and structural integrity of the containment

3a.4.6.0100. During the design of the containment, the following shall be realised:

a) physical barrier function restricting or retaining the radioactive releases and the function ensuring the monitored release of radioactive materials;

b) shielding function protecting against ionising radiation in DBC1-4 and DEC1 and DEC2; and

c) protection function against external events.

3a.4.6.0200. For the performance of the radioactive release restriction or retention and monitored release function of the containment:

a) the leakage of the containment shall be limited at a value where the releases can be maintained at the lowest reasonably achievable level in DBC2-4 and where compliance with the specifications of Sections 3a.2.4.0100 to 3a.2.4.0500 can be ensured,

b) the reduction of the concentration of radioactive aerosols and radioiodine shall be ensured in the containment atmosphere,

c) isolation valves shall be installed to ensure the isolation of pipelines penetrating the wall of the containment,

d) in order to maintain the physical integrity of the containment, it shall be ensured that the climate of the containment in normal operation is appropriate and the normal operational ventilation system of the containment is suitable for providing the pressure within the containment in accordance with the design,

e) the inservice monitoring of leakage from the containment shall be ensured,

f) heat removal from the containment, protection of the structure against overpressure and the management of combustible gases generated shall be ensured in all operating conditions,

g) the cleaning of the atmosphere of the containment or the filtering of a gaseous medium released from the containment shall be ensured,

h) the containment elements shall keep the effect of direct radiation originating from the contained systems and components on personnel working within the containment and those outside the containment at the lowest reasonably achievable level, and

i) the destructive effect of the fuel melt on the structural integrity of the containment shall be prevented or shall be limited to the extent reasonably achievable.

3a.4.6.0300. During the implementation of the protective function against external events, it shall be ensured that:

a) the building structure and internal structural components of the containment as well as the process systems of the containment are so designed and are so

resistant against the effects of external hazard factors that they ensure the integrity and operability of the main circulation loop systems and components of Safety Class ABOS 1 with a B1 physical barrier function, i.e. containing the primary circuit coolant, and of the systems designed to prevent fuel damage when external events occur, while maintaining the allowable leakage value of the containment and the global integrity of the structure, and

b) in addition to maintaining the allowed leakage rate, the containment shall maintain its structural integrity even in DEC1 and DEC2 plant states.

3a.4.6.0400. The functions of the containment may be provided by either one or two separate containment structures.

3a.4.6.0500. If the containment function is provided by two separate containment structures, the closed space between the two structures shall be provided with a ventilation system that ensures a pressure that is lower than the atmospheric pressure, is provided with appropriate filters to remove radioactive materials that may leak from the containment, has single failure tolerance and is independent of the other ventilation systems of the nuclear power plant to the extent reasonably achievable.

3a.4.6.0600. Processes resulting in DBC2-4 and events resulting in DEC1 and DEC2 shall be taken into account 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 to the strength design of the containment, taking into account the characteristics of the material and design of the load-bearing structure.

3a.4.6.0700. The containment shall be so designed that it allows

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

b) leakage monitoring at working pressure,

c) the performance of pressure (leak) tests,

d) monitoring the condition of the containment and its capability of performing its function, and

e) inservice and local testing of penetrations, manholes and airlocks with flexible sealing and expansion fittings for leakage.

3a.4.6.0800. The method and frequency of containment monitoring shall be specified.

3a.4.6.0900. Containment penetrations of appropriate size shall be provided between internal rooms or spaces in order to prevent a pressure difference and the high flow rate of the medium in the containment from causing damage to the structure or any other system component.

3a.4.6.0910. The number of penetrations through the containment wall shall be kept to a practical minimum and all penetrations shall meet the design requirements for the containment leaktightness and integrity. The penetrations shall be protected against reaction forces caused by pipe movement or accidental loads, especially against external or internal events, against missiles, jets and pipe whip.

3a.4.6.1000. The entry of the operating personnel into the containment shall be accomplished by interlocked airlocks that can ensure that at least one door of the airlock is in a closed position in DBC1-4 and DEC1.

3a.4.6.1100. The functionality criteria for the containment airlocks valid for DEC1 and DEC2 plant states shall be determined.

3a.4.6.1110. Safety provisions shall be determined for the personnel entering the containment. Safety of the personnel entering the containment or using the equipment airlocks shall be ensured.

3a.4.6.1120. Containment openings for the movement of equipment or material through the containment wall shall be designed to provide quick and reliable closure in the event that isolation of the containment is required.

3a.4.6.1200. The design margin for the pressurised part of the containment shall ensure that the ferrite materials do not become brittle due to the stresses assumed during operation, maintenance, inspection and during DBC1-4 and DEC1, and the probability of unstable crack propagation will be minimum.

3a.4.6.1300. The materials of claddings and coatings shall be selected and their application shall be specified in accordance with the function of the containment. Their application, wear and tear, and failure shall not influence the performance of the safety functions.

3a.4.6.1400. 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.

II. Process systems of the containment

3a.4.6.1500. The containment as a system shall comprise:

a) all important parts of the primary circuit,

b) execution organs of the 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.

3a.4.6.1600. 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, then it shall ensure their maintenance at a reasonably achievable low level, assuming single failure.

3a.4.6.1700. The containment heat removal system shall be so designed that the inservice inspection of the components necessary for the provision of the integrity and performance of the system can be implemented.

3a.4.6.1800. Technical solutions shall be applied for DEC1-2 , for the monitoring and control of pressure and temperature in the containment, for the management of combustible gases and for avoiding a significant deterioration of the leaktightness of the containment during a reasonable period following such events.

3a.4.6.1810. The cross-sections of openings between containment compartments shall be of such dimensions as to ensure that the pressure differential occurring during pressure equalization in accident conditions does not result in unacceptable damage to the pressure retaining structure or to systems that are important in mitigating the effects of the accident conditions.

3a.4.6.1900. The pipelines penetrating the containment wall, directly connecting to the pressure boundary of the main circulation loop or the containment atmosphere shall be supplied with at least two fast activation isolation valves, operated reliably and independently by external energy, in serial arrangement, one placed within the containment and the other outside of it.

3a.4.6.1910. In the design of isolation valves and the connected penetrations the following shall be ensured:

a) in the case of double wall containment, its properties shall be considered,

b) the isolation valves shall be placed as close as possible to the containment wall penetration,

c) considering the consequences of a failed isolation function, leakage monitoring of the pipe section between the isolation valves shall be provided,

d) functionality of the isolation valves and the penetrations shall be regularly inspected and tested,

e) the operation of the isolation valves shall be sufficiently fast to effectively limit the flow via the given pipeline.

3a.4.6.1920. Solutions different from 3a.4.6.1900. can be designed supported by deterministic analysis supplemented with probabilistic analysis.

3a.4.6.1930. The isolation valves operated by external energy shall be remotely activated. Status signals about their position shall be displayed in the unit main control room and in the backup control room.

3a.4.6.1940. If an isolation valve different from 3a.4.6.1900. is applied, it shall be provided that the valve can be automatically operated remotely or lockable.

3a.4.6.1950. Within the containment a check valve can also be accepted, if the status of the valve is continuously monitored.

3a.4.6.1960. In the pipe section that are not directly connected either to the pressure boundary of the main circulation loop or the containment atmosphere, the isolation valve can be omitted if justified and if the integrity of the pipe section is ensured via a technical solution.

3a.4.6.1970. In the case of isolation valves operated by external energy, efforts shall be made for fulfilling the function in a fail-safe design if the external energy or the operating medium is lost.

3a.4.6.2000. The isolation of the containment shall be possible even in the case of DEC1-2 plant state. In those shutdown states, when timely isolation cannot be performed, the fuel damage shall be avoided with high certainty. If an event leads to bypassing the containment, design solutions that practically eliminate the damage to the fuel elements shall be provided.

3a.4.6.2100. The ventilation systems of the containment shall be so designed that

a) they provide an environment suitable for work for the operating personnel in the rooms which can be served in DBC1;

b) they maintain conditions in line with the environmental qualification of the systems and components located in the rooms of the containment;

c) they limit the spread of materials harmful to human health and ensure the reduction of the concentration of harmful materials in the air to a level below the health limit values; and

d) they ensure appropriate ventilation and separation, as needed, of the different rooms and the exclusion of ventilation routes in order to eliminate or the risk posed by hazard sources to a level below the acceptable value.

3a.4.6.2200. The cleaning of the containment atmosphere shall be so performed that the systems used for the management and monitoring of fission products, hydrogen, oxygen and other materials potentially released into the containment atmosphere ensure the reduction of the quantity and concentration of the fission products released into the environment, assuming a single failure, as well as the

control of concentration of hydrogen or oxygen in the containment atmosphere in order to ensure the integrity of the containment.

3a.4.6.2300. The cleaning system of the containment atmosphere shall be so designed that it allows the appropriate inservice inspection of important components in order to ensure system integrity and performance.

3a.4.6.2400. Appropriate protection shall be provided against fire in the containment. However, the installation of fire barriers shall not hinder the functions and operation of the containment.

3a.4.7. Auxiliary and service systems

I. Essential service water system

3a.4.7.0010. The reliability of the auxiliary and support systems shall satisfy all requirements from the safety systems supplied by them and their capability for their functions shall be testable.

3a.4.7.0100. Heat removal from systems and components important to nuclear safety and the maintenance of their temperature at the designed level under normal operating and accident conditions shall be provided by the essential service water system. Single failure shall be assumed for the design of the system.

II. Ventilation and air conditioning systems

3a.4.7.0200. The ventilation systems of the nuclear power plant shall ensure the prevention or reduction of the spread of radioactive materials within the facility or their release into the external environment, and the climate conditions necessary for the operating personnel or systems, structures and components, which provide for maintaining the qualified state.

3a.4.7.0300. In the case of rooms containing system components important to nuclear safety, it shall be examined what effect the loss of the ventilation and air conditioning systems has on their operation. If warranted, the ventilation and air conditioning system shall be included in a safety class and shall be installed with appropriate redundancy.

3a.4.7.0400. The rooms shall be provided with independent ventilation systems according to their category. An exception to this shall be the unit main and backup control rooms and the rooms of the containment, to which Sections 3a.4.7.0700 and 3a.4.6.0900 shall apply.

3a.4.7.0500. The following shall be ensured by the ventilation and air conditioning systems, which are meant to limit the dispersion of radioactive materials:

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

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

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

3a.4.7.0600. Efforts shall be made to use a single exhaust stack to ensure the possible monitoring of the integrated quantity of gaseous radiation releases.

3a.4.7.0700. During the design of the ventilation systems, the following shall be ensured as general requirements:

a) 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 and the risk of entry of chemicals shall be taken into account,

b) fire protection and fire restriction functions shall be performed,

c) the ventilation systems, if necessary, shall be suitable for removing the smoke generated by fire, restoring normal air conditions, while the propagation of fire through the ventilation systems shall be prevented,

d) the suction side of the ventilation and air conditioning system shall be provided with appropriate filters in order to avoid that the explosive, toxic and other hazardous materials and contamination, the appearance of which can be expected, cannot get into the safety class rooms. The ventilation system shall be provided with appropriate measuring instruments that are suitable for detecting hazardous materials,

e) the discharge side of the ventilation and air conditioning system shall be provided with filters suitable for removing radioactive materials getting into the ventilation system and, if necessary, capabilities shall be provided for cooling the air removed from the room and for limiting the flow in order to limit releases,

f) in accordance with Section 3a.5.2.0200, the geometric design of the ventilation and air conditioning systems and the materials used shall be so selected that they can be easily decontaminated,

g) the unit main and backup control rooms, the technical support centre and the emergency management centre shall be provided with isolation and filtration systems that allow that in the case of DBC2-4 and DEC1 and DEC2, the personnel can work in them without personal protective equipment, even in the long run. The ventilation and air conditioning systems serving the rooms of the unit main and backup control rooms, the technical support centre and the emergency

response centre shall be independent to the extent reasonably achievable and shall have single failure tolerance.

3a.4.7.0800. The system components of air conditioning systems shall be standardised to the extent possible. The design shall take into account testability and, if necessary, leaktightness and noise level requirements.

3a.4.7.0900. The design of ventilation ducts shall be carried out by taking into account the available standard profiles, radiation protection requirements, earthquake resistance, installability and expected external and internal pressure conditions.

3a.4.7.1000. During the design of fans, the system-compatible characteristic curves of single and parallel operation, protection from rotary components, easy accessibility and installability (in particular, in the case of belt-driven fans) and the prevention of the spread of vibrations shall be taken into account.

3a.4.7.1100. During the application of heating equipment, both electric and water heaters can be applied. It is advisable to install electric heaters for places to be designed for earthquake resistance. In the case of cooler heat exchangers, the use of corrugated fins is advisable in such a way that their distance limits the deposition of materials.

3a.4.7.1200. The flap-valves shall be provided with mechanical position indicators, and in the case of the ones used for adjustment, the possibility of fixing them in the appropriate position shall be provided.

III. Hoisting equipment

3a.4.7.1300. The design of the hoisting equipment shall comply with the earthquake resistance, lifting, anti-dropping, design and testing requirements and criteria.

3a.4.7.1400. Depending on their function, the hoisting equipment shall have manual and remote control facilities, which can ensure the safe lowering of the load to the ground in the case of the loss of voltage.

3a.4.7.1500. The hoisting machinery affecting safety or physical barrier functions shall be designed by applying a special nuclear design standard.

IV. Elevators

3a.4.7.1600. The design of elevators shall comply with the earthquake resistance, lifting, anti-dropping, design and testing requirements and criteria.

3a.4.7.1700. Depending on their functions, the elevators shall have a facility for manual handling, which can ensure the safe lowering of the elevator in the case of the loss of voltage.

3a.4.7.1800. Elevators affecting safety or physical barrier functions shall be designed by applying a special nuclear design standard.

3a.4.8. Special design requirements for system components

I. Valves

3a.4.8.0100. The systems shall be so designed that the possible lowest number of valves are needed, taking into account, at the same time, the considerations of safety, functionality, reliability and availability.

3a.4.8.0200. Requirements compliance with which ensure the operability of the valves and their drives under all design conditions shall be specified for each valve. The most important considerations shall be the safety function, the flow-rate, pressure drops, reliability requirements, redundancy requirements and exclusion requirements.

3a.4.8.0300.

3a.4.8.0400. In the interest of subsequent replaceability and modifications, in addition to operational and maintenance information as well as drawings and diagrams, the technical information delivered together with the valves shall contain the justification for selection, in particular, hydraulic resistance, special features of cavitation and two-phase medium, drive load as a function of medium flow and pressure difference, and travel time.

3a.4.8.0500. The minimisation of the probability of any leakage from the valves shall be ensured by design solutions.

3a.4.8.0600. The valve housing components that come into contact with a boric acid medium when any gasket leaks shall be made of a material resistant to boric acid corrosion.

3a.4.8.0700. The open or closed position of the valves shall be visible from outside.

3a.4.8.0800. It shall be possible to test the safety function of valves. The conditions of testing shall be close to the design conditions to the extent possible.

3a.4.8.0900. The parts of valves belonging to the same type shall be interchangeable.

II. Valves drives

3a.4.8.1000. The design requirements for valve drives shall ensure their operation under any planned condition, selecting the worst conditions for sizing, including fluctuations in the parameters of the supply voltage or the driving medium.

3a.4.8.1100. The drives shall provide the torque required for the operation of the valve as well as the closing and opening (travel) times designed in the safety analysis without damaging the driven valve.

3a.4.8.1200. The type of the drive shall be selected by taking into account its function.

3a.4.8.1300. Motor drives shall be preferred in the containment, in particular, in the case of control valves. If, however, the motor drives cannot meet the prescribed performance or safety requirements, own-medium or pneumatic drives may also be used.

3a.4.8.1400. The driven valves shall be provided with a manual operation and chaining facility, if necessary.

3a.4.8.1500. The gaskets of the pneumatic drives shall be rated.

3a.4.8.1600.Torque and overload protection shall be provided for the valves.

3a.4.8.1700. The indication of the overloading of valve drives included in Safety Class 1 shall be ensured in the unit main control room.

3a.4.8.1800. Overload protection shall not prevent the performance of the safety functions.

III. Pumps

3a.4.8.1900. The use of pumps requiring service systems shall be avoided as far as possible.

3a.4.8.2000. The maintenance of the pumps shall be so planned that the loss of the availability of the pumps arising from normal wear and tear between two scheduled maintenance cycles can be excluded.

3a.4.8.2100. Instead of throttling elements, the use of control valves shall be preferred for the adjustment of the hydraulic parameters in the interest of replaceability.

3a.4.8.2200. The internal parts of pumps shall be easy to remove for maintenance and the pumps themselves shall be easy to replace.

3a.4.8.2300. Where possible, long-life gaskets and continuous lubrication shall be applied at places that have high dose rates.

3a.4.8.2400. The gaskets shall allow the pumps to be started with a closed discharge line.

3a.4.8.2500. Cavitation wear shall be prevented by providing appropriate suction line conditions. The use of booster pumps shall be avoided or if they are still necessary, they shall provide the suction pressure and flow rate required for

avoiding cavitation, in particular, in startup and shutdown operating modes, and their reliability shall be at least identical with that of the main pump.

3a.4.8.2600. Axially divided pump casings shall not be used in systems conveying materials with a high medium temperature or ones characterised by high heat stress and ones conveying radioactive materials under high pressure.

3a.4.8.2700. Axially divided pump casings shall not be used in safety systems.

3a.4.8.2800. An effort shall be made to use hermetic pumps on the basis of very low leakage, an increased maintenance cycle time and the resulting lower maintenance dose exposure.

3a.4.8.2900. The design shall ensure that the pumps can be tested during operation at flow rates that demonstrate reliable operation during normal operation and that do not lead to the deterioration of the pumps.

3a.4.8.3000. In the case of main circulation pumps, the sufficiency of the long running time of the pumps shall be ensured in accordance with the targets stated in the analyses of the Preliminary and Final Safety Analysis Reports. The existence of the target running time shall be demonstrated during the commissioning tests.

3a.4.8.3100. Leakage near the shaft of the main circulation pumps shall be limited even if the sealing water supply is lost for a short time.

IV. Heat exchangers

3a.4.8.3200. Heat exchanger types that can be placed into service at any time, without any preparation and conditioning, shall be used, if possible.

3a.4.8.3300. In the case of tube bundle heat exchangers, the source of the working medium shall be eliminated in the roll-in zone of the tube sheet and the heat exchanger tubes.

3a.4.8.3400. The radioactive medium shall flow in the heat exchanger tubes and, wherever possible, its pressure shall be less than the pressure in the shell space.

3a.4.8.3500. The heat exchanger tubes shall be protected from vibrations generated by the flow of medium even under the least favourable flow and temperature conditions.

3a.4.8.3600. The heat exchangers shall be sized with appropriate margins, taking into account the required pipe plugs and clogging and deposits.

3a.4.8.3700. Appropriate corrosion allowances shall be taken into account in the case of the heat exchanger tubes, however, the margins shall not lead to over-sizing.

3a.4.8.3800. The heat exchangers shall be fully drainable and cleanable.

3a.4.8.3900. The possibility of removing and reinstalling the tube bundles of the heat exchangers shall be ensured.

V. Filters and ion exchangers

3a.4.8.4000. In the case of filters treating radioactive liquids, easy handling and installation shall be ensured even by applying remote actuation methods.

3a.4.8.4100. Solutions where the materials removed from the filters do not cause a major radiation exposure shall be applied.

3a.4.8.4200. Cartridge filters shall be such that their replacement at maximum two-year intervals can be easily carried out, and the removed cartridges can be treated by normal waste management procedures.

3a.4.8.4300. For the design of reflux filters, the grain size/quantity in the liquid to be filtered, the gravity reflux solution and the sufficiently large interval of the reflux frequency shall be taken into account.

3a.4.8.4400. In the case of ion exchanger filters, the maintenance of the temperature, loosenability, regeneration and replaceability of the resin as well as the suitability of the vessel for the medium and pressure conditions shall be ensured. The appropriate service life of the resin shall be ensured.

3a.4.8.4500. In the case of air filters, ones that may become radioactive shall be separated from the inactive spaces. A space required for the replacement of cartridges shall be provided.

VI. Storage tanks

3a.4.8.4600. The general design requirements for atmospheric storage tanks shall be as follows:

a) provision of anti-deposition measures and solutions,

b) a design of the external and internal bracing of the tank that does not prevent full drainage/venting and decontamination,

c) appropriate internal lining of concrete tanks,

d) durability or reparability of internal linings,

e) in the case of storage tanks located outdoors, ensuring frost resistance,

f) separate decontamination, emptying, washing, sampling and anti-leak requirements shall be set for tanks used for the storage of radioactive liquids,

g) the storage tanks shall be accessible for maintenance; for this purpose, a space of at least 500 mm shall be provided around them and the vertical clearance of walkable paths shall be at least 2 m.

VII. Pipelines and pipeline components

3a.4.8.4700. In the design of pipelines, the possible inspection of welds, the minimisation of high and low points, possibility to perform deaeration, pressure tests and leakage tests, and, in the case of systems containing radioactive materials, the easy installation of insulation shall be ensured.

3a.4.8.4800. Wherever possible, bent pipe sections shall be used instead of straight pipes and elbows.

3a.4.8.4900. Damper discs shall be installed in straight sections of appropriate lengths, in a manner identifiable from outside.

VIII. Bolted joints and threaded fasteners

3a.4.8.5000. Bolted joints and threaded fasteners shall only be used where a frequent need for disassembly justifies it.

3a.4.8.5100. At the pressure boundary and, within that, primarily in the case of joints bordering hazardous materials, the use of resistant, inspectable fastenings are especially important. If there is a risk of loosening, a releasable closing mechanism shall be used around the joint.

IX. Diesel generators

3a.4.8.5200. The handling, start-up, loading, stable operation and shutdown characteristics of diesel generators shall be such that they ensure automatically or, if necessary, with a manual switching, the staged connection of the required consumers in due time, shall tolerate the switching off and on of the maximum individual load in every operating condition, shall be suitable for quickly providing and continuously maintaining the expected parameters within the set limits, and shall be switched off from operation in an accident condition only by their minimum required protection functions.

3a.4.8.5300. Every diesel generator shall be provided with a stand-alone fuel, exhaust, lubrication, cooling water, combustion air, start-up air and electrical systems, which are protected from external and internal hazards. The diesel generator and its auxiliary systems shall be testable.

3a.4.8.5400. The diesel generators shall be provided with a firefighting system.

3a.5. RADIATION PROTECTION

3a.5.1. General requirements

3a.5.1.0100. During design, the three principles of radiation protection, i.e. justification, optimisation and limitation shall be applied.

3a.5.1.0200. When planning for radiation protection, controlled and supervised zones shall be designated. In the controlled area, the monitoring of the atmosphere and surface contamination of the rooms and the radiation sources

shall be provided for. Appropriate equipment shall be designed and measures shall be taken to control the dispersion of radioactive contamination in the supervised zone.

3a.5.1.0300. A work environment that conforms to the principle that the radiation exposure of the personnel shall be kept as low as reasonably achievable shall be provided in DBC1-4 and DEC1 in every area of the nuclear power plant unit where operating personnel is or can be present according to their intended purpose.

3a.5.1.0400. When designing the circumstances of activities in a potentially radioactive environment, the radiation exposure of individuals shall be so limited that the potential combinations of radiation exposures shall not exceed either the effective dose or the equivalent dose limits of the organs and tissues.

3a.5.1.0500. Protection measures shall be optimised in order to keep the individual doses, the number of exposed people and the probability of radiation exposure as low as reasonably achievable within the individual dose limits, taking into account the dose constraints applicable to the nuclear power plant.

3a.5.1.0600. Normal and potential radiation exposure shall be analysed throughout the site of the nuclear power plant, taking into account DBC1-4 and DEC1 and DEC2 in order to estimate the radiation exposure regularly or potentially affecting the population as well as people present at the site of the nuclear power plant.

3a.5.1.0700. Each dose estimate shall be appropriately conservative in order to take into account the uncertainties of internal and external radiation dose calculations. The available measurement data shall also be used for calculations.

3a.5.1.0800. The highest annual personal dose value and the average collective dose value shall be described.

3a.5.1.0900. The radiation exposure of workers employed in radiation-free jobs at the site shall be determined by estimating the maximum dose value expected from the radiation parameters of the site.

3a.5.1.1000. The radiation exposure of the population living around the site shall be determined on the basis of calculated dose values, which apply to the critical group and also take into account external and internal radiation exposures from artificial sources, except for radiation from medical exposure.

3a.5.1.1100. Design objectives shall be set to determine a collective dose for the operating personnel based on health physics requirements, in possession of available experience.

3a.5.1.1200. During the design process, it shall be estimated by calculations to what extent the operation of a given system contributes to the collective radiation

exposure of the personnel. When the radiation exposure is estimated, contributions from radioactive nuclides in adjacent systems and present in the air shall also be taken into account.

3a.5.1.1300. Radiation exposures occurring during the scheduled inspections and maintenance of the system as well as the repair and replacement of its components shall also be evaluated. The systems that significantly contribute to the collective radiation exposure of the operating personnel while observing the design dose value set shall be identified.

3a.5.1.1400. Systems and components shall be so designed that it becomes possible to operate the nuclear power plant even without the presence or work of personnel in areas with high dose rates.

3a.5.1.1500. Remotely controlled equipment shall be designed and manufactured to handle high activity objects.

3a.5.1.1600. From a dosimetry point of view the proper operation of system components emitting radioactive radiation shall be monitored by continuous and intermittent radiation protection control measurements. The scope of radiation protection monitoring and the number of continuous and intermittent measurements by instruments shall be determined by taking into account normal and potential radiation exposure.

3a.5.1.1700. The drain and air venting valves of systems and components that transport and store a radioactive medium shall be so designed that the separate handling of the radioactive medium becomes possible.

3a.5.1.1800. A dose evaluation system that

a) ensures the measurement and evaluation of the personnel's radiation exposure at regular intervals along with the dose evaluation system of the authority,

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

c) provides appropriate data for the optimisation of radiation protection, and

d) ensures the prompt detection if the dose limits are exceeded

shall be designed for the operation of the nuclear power plant.

3a.5.2. Decontamination

3a.5.2.0100. The possibility for decontamination shall be provided wherever the radiation exposure of the operating personnel can be reasonably reduced. The need for decontamination shall be minimised by preventing any leakage of

radioactive media and by installing closed-circuit drainage, air vent and overflow pipes.

3a.5.2.0200. It shall be ensured that the material and design of system components that come functionally in contact with radioactive media or are exposed to radioactive contamination allow for decontamination and the complete removal of the decontaminating solution. The decontamination process shall be so designed as to ensure that the surface quality of the affected system components meets the requirements even after decontamination.

3a.5.2.0300. The inspection and, if required, decontamination of controlled areas, the persons entering and exiting the controlled areas, the reusable protective clothing as well as objects exiting and entering the controlled areas shall be ensured.

3a.5.2.0400. The licensee shall prepare for the decontamination of potentially contaminated transport containers and other packaging materials.

3a.5.2.0500. Where necessary, decontamination made by remotely operated devices shall be designed.

3a.5.2.0600. The place and resource needs of decontamination shall not decrease the level of nuclear safety.

3a.5.2.0700. New decontamination technology or in the case of a chemical decontamination technology 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 deteriorating the safety functions of the facility;

c) justification that the activity 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 the use;

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

3a.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.

3a.5.2.0900. Regarding decontamination of rooms and equipment of nuclear facilities, as minimum, the planned direction of dispersion of contamination between the rooms and equipment shall be taken into account together with the limitations on use of chemicals and technologies in the given room.

3a.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.

3a.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 medium.

3a.5.2.1200. A design solution shall be provided for the Management of the potentially drying out contaminated surfaces.

3a.5.3. Radiological monitoring equipment

3a.5.3.0100. Appropriate equipment shall be designed for the measurement of radiation conditions. This equipment shall be capable of taking accurate measurements under DBC1-4 and also shall be suitable for providing information in designated areas even under DEC1 and DEC2 plant states. The measuring devices 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 the areas regularly serviced by the operating personnel with instruments if the presence of personnel in these areas may be restricted in certain design operating conditions,

c) to indicate dose rates arising under DBC3-4 and DEC1 and DEC2,

d) to measure the isotope concentration of gaseous and liquid samples taken from process systems and the environment under DBC1-4 and DEC1 and DEC2,

e) to regularly monitor environmental releases with instruments under DBC1-4 and DEC1 and DEC2,

f) to measure radioactive surface contamination, and

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

3a.5.4. Biological protection

3a.5.4.0100. Biological protection shall be designed in every area of the nuclear power plant unit where direct radioactive radiation and the accumulation of radioactive materials may be expected due to a chain reaction.

3a.5.4.0200. When materials are selected for shielding, the following shall be taken into account:

a) the characteristics of radiation,

b) the shielding and mechanical properties of materials, and

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

3a.5.5. Radioactive releases

3a.5.5.0100. Appropriate systems shall be developed in the nuclear power plant unit for management of gaseous and liquid radioactive materials in order to keep the quantity of releases and concentration of radioactive materials below the required limits and as low as reasonably achievable. The number of release locations shall be designed to be as low as reasonably achievable. The integrated monitoring of releases shall be ensured.

3a.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.

3a.5.5.0200. The terrain conditions in the vicinity, weather conditions and distances between buildings and stacks shall be taken into account when the positions and constructions of release locations are designed, taking into account the aerodynamic properties of releases and their compatibility with ongoing operations in nearby buildings.

3a.5.5.0210. The licensee shall make assessments with regard to the releases already in the design of the facility:

a) possible activity of the releases;

b) analysis of effects of most probable releases expected along the possible release routes, including the environmental effects from the releases and the doses of the critical population groups.

3a.5.5.0300. A meteorological station shall be designed in the proximity of the site to ensure the availability of meteorological data whenever required, to the extent and at the frequency specified in the designs. Meteorological information shall be available wherever it is required for designed processes and procedures.

3a.5.5.0400. To monitor the environment outside of the site, the measurement of dose rates as well as the activity concentration of radioactive aerosols and iodine isotopes shall be ensured by a telemetry and sample collection network.

3a.6. MANAGEMENT AND STORAGE OF NUCLEAR FUEL AND RADIOACTIVE WASTE

3a.6.1. General requirements

3a.6.1.0100. The appropriate management, transport and storage of nuclear fuels and radioactive wastes shall be ensured within the site of the nuclear power plant. During design, the storage, transport, packaging and lifting requirements to be met shall be defined.

3a.6.1.0200. The requirements for the on-site management and storage of nuclear fuels and radioactive wastes as well as the storage capacity required on the site shall be defined in accordance with the national strategy for the management and final disposal of spent fuel and radioactive wastes 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..

3a.6.1.0300. Passive safety solutions shall be applied to the extent reasonably achievable when on-site storage is designed.

3a.6.1.0400. During the planned on-site management and storage of nuclear fuel and radioactive wastes, equipment that provides appropriate treatment for the possible conditions of nuclear fuel assemblies and radioactive wastes shall be available.

3a.6.1.0500. Appropriate equipment and packaging shall be available for the management of spent fuel and radioactive waste packages that may show signs of deterioration.

3a.6.1.0600. The systems potentially containing nuclear 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.

3a.6.2. Management and storage of nuclear fuel

3a.6.2.0100. For fresh fuel assemblies, such transport, management and storage systems, structures and components shall be designed and such technical measures shall be developed that:

a) prevent the development of criticality with sufficient safety margins,

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

c) prevent the possibility of dropping the fuel assemblies or damaging them in other ways,

d) ensure the control inspections of the fuel assemblies,

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

f) ensure the identification of the fuel assemblies at every storage site, and

g) the logistic system excludes the potential loss of a fuel assembly.

3a.6.2.0150. Unintended penetration of any liquid to the fresh fuel storage shall be prevented.

3a.6.2.0200. In the case of systems, structures and components used for the management, transport and storage of irradiated nuclear fuel, the following requirements shall also be fulfilled in addition to the requirements for systems, structures and components planned for the transport, management and storage of fresh fuel assemblies:

a) they shall ensure the removal of residual heat in all operational conditions,

b) they shall prevent the fall of heavy objects onto fuel assemblies,

c) they shall ensure the visual inspection of irradiated fuel assemblies as well as the inspection and qualification of the leaktightness of fuel elements,

d) they shall provide storage appropriate to the condition of fuel elements or fuel assemblies with assumed or detectable defects.

e) the possibility of the loss of coolant due to the loss of integrity of the lines and pipes connected to the spent fuel pool shall be excluded by technical measures,

f) it shall be prevented that the irradiated fuel assemblies become uncovered even in the case of the leakage of the underwater storage system, and the make up of the water required for heat removal shall be ensured,

g) the spent fuel pool shall be placed in the containment or, if it is not possible, in an environment that provides sufficient protection against possible consequences arising from any damage to the fuel elements,

i) they shall ensure the efficiency of the applied neutron absorbers,

j) maintenance and dismantling of the fuel assembly moving and storage devices shall be ensured, and

j) decontaminability of the fuel management and storage areas shall be ensured.

3a.6.2.0300. Equipment and technology used for supplying an external water source required for the alternative cooling of the spent fuel pool and setting the appropriate boric acid concentration shall be provided.

3a.6.2.0400. When the storage capacity required for irradiated fuel assemblies is determined, it shall be ensured that the necessary quantity of fuel assemblies can be unloaded from the nuclear reactor on every occasion in accordance with the procedure of planned management of fuel assemblies in the nuclear reactor.

3a.6.2.0500. The designer shall demonstrate the mechanical and chemical compatibility of the applied nuclear fuel and the systems, structures and components of the nuclear power plant designed for their handling.

3a.6.2.0600. The following shall be provided for the spent fuel pool:

a) inspection and testing of the irradiated fuel assemblies, as required,

b) equipment for the water chemistry and radiological monitoring of the storage medium,

c) water purification, leak collector and leak monitoring systems.

3a.6.2.0700. Systems regulating the level and temperature of the spent fuel pool shall be provided in DBC1-4 and monitoring systems shall be provided in DBC1-4 and DEC1 and DEC2.

3a.6.3. Management and storage of radioactive wastes

3a.6.3.0100. Systems, structures and components and procedures shall be designed for the management and on-site storage of radioactive wastes.

3a.6.3.0200. Complex waste management documentation shall be developed to regulate and monitor the path of radioactive materials.

3a.6.3.0300. Systems managing radioactive wastes and the applied processes shall be designed to ensure that the waste as an end product fulfils the requirements for transport, interim storage and, if known, the acceptance criteria for final disposal.

3a.6.3.0400. For efficient waste management, the radioactive wastes produced shall be classified and separated according to 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.

3a.6.3.0500. The representative isotope composition and activity of the radioactive wastes shall be determined by nuclide-specific measurements; in the case of radionuclides that are difficult to measure, it shall be determined indirectly, theoretically. The radioactive wastes generated shall be qualified.

3a.6.3.0600. Liquid radioactive wastes shall be classified according to their activity concentration. Their physical and chemical properties shall be considered during processing. It shall be ensured that storage tanks and containers have suitable ventilation, pressure relief facilities and equipment suitable for collecting leakage.

3a.6.3.0700. Storage shall be designed at the nuclear power plant site in such a way that all waste packages can be inspected and recovered, if necessary.

3a.6.3.0800. It shall be ensured by an appropriate technical solution that the liquid radioactive wastes collected in the accessory buildings containing systems, structures and components coming into contact with radioactive media or, if the nuclear power plant has it, in the secondary containment can be returned to the containment also in DBC and DEC if their quantity exceeds the capacity of the liquid waste processing system.

3a.6.3.0900. It shall be estimated with appropriate margins that what type and what quantities of radioactive wastes are expected to be produced during DBC3-4 and DEC1 and DEC2 events as well as their management and response to them. In their knowledge, solutions suitable for the interim storage and management of wastes shall be designed and their location shall be designated on-site.

3a.6.3.1000. In the determination of storage capacity it shall be considered to provide appropriate reserves that can ensure additional capacity for unanticipated events.

3a.6.3.1100. 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 determined storage duration.

3a.6.3.1200. Management of radioactive wastes requiring special treatment, especially radioactive waste containing considerable amount of alpha emitters, furthermore flammable, explosive, corrosive, toxic and other dangerous materials, shall be designed.

3a.6.3./A. Management of airborne radioactive wastes

3a.6.3.1300. Systems, structures and components suitable for treating airborne radioactive waste shall be designed to comply with the respective limits and keep the releases at a minimum.

3a.6.3.1400. Volatile radioactive wastes shall be removed from the gaseous radioactive wastes to the extent reasonably achievable.

3a.6.3.1500. Measures shall be designed to avoid generation of or remove flammable or explosive compounds.

3a.6.3./B. Management of liquid radioactive wastes

3a.6.3.1600. In the design of liquid radioactive waste processing systems the composition and properties of the liquid shall be taken into account.

3a.6.3.1700. The different type of waste shall be appropriately separated and the most effective method of processing shall be selected to achieve the principal of justification.

3a.6.3.1800. Matrix materials suitable for waste conditioning and appropriate barrels and containers shall be designed.

3a.6.3.1900. Appropriate tank capacity shall be available for the storage of radioactive media to keep the environmental release at a minimum.

3a.6.3./C. Management of solid radioactive wastes

3a.6.3.2000. Suitable waste management procedures shall be designed in line with the principal of keep the wastes at a minimum.

3a.6.3.2100. In the case of mobile conditioning equipment measures shall be designed to avoid spread of contamination.

3a.7. PLANNING OF ON-SITE NUCLEAR EMERGENCY PREPAREDNESS AND RESPONSE

I. General requirements

3a.7.1.0100. The nuclear emergency preparedness and response procedures shall be planned on the basis of the analysis results of DBC3-4 and DEC1-2 and analysis of very severe accidents, taking into account that the above operating conditions may occur at the same time in all reactors and the nuclear facility on the given site. The scope of the analyses shall provide sufficient information to define nuclear emergency preparedness and response activities including the number and composition of the necessary on-site response personnel.

3a.7.1.0200. The hazard factors identified during planning shall be categorised into threat categories based on their potential severity. Of the hazard sources, risk factors not directly related to the nuclear reactor shall also be taken into account, in particular, accident situations relating to the handling of spent fuel, the spent fuel pools, the management of radioactive wastes and the radioactive sources used on the site, as well as off-site risk factors, in particular, the situations of

potential accidents and severe accidents at a nuclear facility in the vicinity to the site. During preparation, the ability to eliminate the most severe emergency situation defined by analyses shall be achieved. It shall be shown that the preparation ensures in the case of every assumed initiating event and possible emergency situation the timely execution of appropriate actions, i.e. classification, notification, activation and nuclear emergency preparedness and response measures.

3a.7.1.0300. An emergency response centre shall be established for the personnel performing emergency response. It shall be ensured that sufficient instrumentation and tools are available at the emergency response centre for the management of actions required during an emergency situation and for communication with the organisational units responsible for nuclear emergency preparedness and response, with locations and with off-site organisations responsible for nuclear emergency preparedness and response.

3a.7.1.0400. The emergency response centre shall be equipped with a redundant and diverse communication system, which is suitable to alert the on- and off-site organisational units responsible for nuclear emergency preparedness and response as well as to communicate with the unit main and backup control rooms, other important locations of the nuclear power plant and the off-site nuclear emergency preparedness and response organisations.

3a.7.1.0500. Personnel at the emergency response centre shall be protected against the circumstances arising from the emergency situation. The regular inspection of the functionality of the emergency response centre shall be allowed. The emergency response centre shall be so located that its accessibility is ensured in the assumed emergency situations. Should the use of the emergency response centre become impossible, a backup emergency response centre shall be established at a sufficient distance from the nuclear power plant, which fulfils the requirements set for an emergency response centre.

3a.7.1.0600. An on-site alarm system shall be installed, which is suitable to alert all people present on the site. In order to execute emergency measures, safe escape routes, which are simply, understandably and durably signalled and reliably lit, and all conditions required for their safe use shall be provided at the nuclear power plant. The escape routes shall be designed to fulfil the industrial safety, radiation protection, fire protection and physical protection requirements.

3a.7.1.0700. Appropriate shelters complying with the civil protection regulations and corresponding to the number of persons involved in nuclear emergency preparedness and response activities shall be installed for the personnel participating in nuclear emergency preparedness and response activities.

3a.7.1.0800. During the design of equipment required for nuclear emergency preparedness and response, attention shall be paid to the need for performing work in high-radiation spaces and for the indispensible, related on-site transporting.

3a.7.1.0900. Systems, structures and components required for the management of emergencies shall be so designed that they are operable and perform their functions even in the long term in all operating conditions, including DEC1 and DEC2 plant states and the conditions according to the results of very severe accident analysis.

3a.7.1.1000. If the use of mobile equipment forms part of accident response, such fixed connection points shall be established for it that can also be used in DEC1 and DEC2 plant states from a physical and radiological point of view.

II. Accessibility during accidents

3a.7.1.1100. The accessibility of the systems, structures and components after accidents shall be ensured in accordance with the monitoring and restoration operations. The areas to which access may be necessary shall be designated in the preliminary plan.

3a.7.1.1200. Routes that need to be used by the personnel during accidents shall be specified. Security measures shall not prevent the necessary movement of operators in accident situations.

3a.7.1.1300. The inspection measures shall be in line with the requirements of having quick access to or quickly leaving certain areas important to safety during accidents.