BESEP

Deliverable 2.2
Requirement Baseline for BESEP

June 2021 version 1.2

Public

Suvi Rein
Fortum Power and Heat Oy
PL100, 00048 FORTUM
Finland
suvi.rein@fortum.com

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 945138.

Project acronym	Project title	Grant agreement No.
BESEP	Benchmark Exercise on Safety Engineering Practices	945138

Deliverable No.	Deliverable title	Version
D2.2	Requirement Baseline for BESEP	1.2
Type	**Dissemination level**	**Due date**
Report	Public	M10
Lead beneficiary		**WP No.**
Fortum Power and Heat Oy		2

Main author	Reviewed by	Accepted by
Suvi Rein	Frans Davelaar	Essi Immonen
Contributing author(s)		**Pages**
		119

Abstract

WP2 provides the common starting point for the benchmark exercise in the BESEP project. It defines the external hazards, safety analysis methods, systems, structures and components and a set of requirements to be involved in the comparison and evaluation of safety engineering processes used by the project partners.

This task 2.2 defines the requirement baseline for the coming work in the BESEP project.

In the beginning the national legal frameworks and the regulatory environment of the BESEP partner countries are described. Then some subjects in the national requirements are listed to provide a holistic view on the regulatory environment. These subjects are event classifications and the target values for core damage frequency and large early release frequency.

At first safety requirement topics are defined for three analysis types including deterministic safety analysis, probabilistic safety analysis, human factors engineering and for safety engineering practices. Safety requirement topics are an extract on the whole safety analysis entity seen relevant for the upcoming project work.

The national original requirements have been collected, selected and partly translated by BESEP partners. The selection has been made based on the current understanding on the project scope. Then these requirements and relevant high-level IAEA safety requirements identified in the preceding BESEP Task 2.1 are classified to the safety requirement topics. Finally, based on the input requirements the BESEP requirements for each safety requirement topic are elaborated. These requirements form the BESEP requirement baseline to be used in the coming work of the BESEP project.

Coordinator contact

Atte Helminen
VTT Technical Research Centre of Finland Ltd
P.O. Box 1000, 02044 VTT, Finland
E-mail: atte.helminen@vtt.fi
Tel: +358 20 722 6447

Acknowledgement

This project has received funding from the Euratom research and training programme 2019-2020 under grant agreement No. 945138.

HISTORY OF CHANGES

Date	Version	Author	Comments
31.5.2021	1.0	Suvi Rein	Final version for review
14.6.2021	1.1	Frans Davelaar	Reviewed version
21.6.2021	1.2	Suvi Rein	Finalized version

LIST OF ABBREVIATIONS

ASN	Nuclear Safety Authority- the French administrative authority
BESEP	Benchmarking Exercise on Safety Engineering Practices
CDF	Core Damage Frequency
DiD	Defence-in-Depth
DSA	Deterministic Safety Analysis
ENSREG	The European Nuclear Safety Regulators Group
EOP	Emergency Operating Procedure
HAEA	Hungarian Atomic Energy Authority
HF	Human Factors
HFE	Human Factors Engineering
IAEA	International Atomic Energy Agency
IRSN	French Radioprotection and Nuclear Safety Institute
LERF	Large Early Release Frequency
LRF	Large Release Frequency
NEA (OECD NEA)	Nuclear Energy Agency
NPP	Nuclear Power Plant
NUREG	United States Nuclear Regulatory Commission
OECD	The Organisation for Economic Co-operation and Development
PRA	Probabilistic Risk Assessment
PSA	Probabilistic Safety Assessment
SAMG	Severe Accident Guideline
SSM	Swedish Radiation Safety Authority
STUK	Säteilyturvakeskus, the Finnish Radiation and Nuclear Safety Authority
TSO	Technical Safety Organization
UJD SR	Nuclear Regulatory Authority of the Slovak Republic
V&V	Verification and Validation
WP	Work Package
YVL	Finnish Regulatory Guide on Nuclear Safety

Note: List of abbreviations used only at Chapter 4 are listed at the beginning of the Chapter 4.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1 Introduction

BESEP (Benchmarking Exercise on Safety Engineering Practices) is an Euratom 2019 project which focuses on benchmarking, cross comparison and evaluation of the project partners on their Safety Engineering processes regarding safety margin determination and safety requirements verification against external hazards. The benchmark exercise is based on example external hazard case studies, which each focuses on a selected set of Safety Engineering topics, requirements, safety analyses etc., for which the needed information and data will be gathered from the project partners and shared between each other. [1]

The objective of BESEP is to demonstrate compliance of safety requirements with sufficient safety margins against external hazards with impact on nuclear power plants using efficient and integrated set of safety engineering practices involved in deterministic and probabilistic safety analyses. In addition, the human factors engineering is considered because the personnel and the safety systems work together to ensure safety of nuclear power plants.

The BESEP partner countries have different nuclear safety requirements which leads to different safety engineering practices. Nevertheless, there are differences in the practices, the goal is the same: showing the fulfilment of the safety requirement in the nuclear power plant design and operation.

To accelerate the implementation of best safety engineering practices a benchmark exercise is conducted between the BESEP partner countries. This will help find the most efficient safety engineering processes to support the operation and licensing of nuclear power plants within EU.

The overall objective of BESEP is to support safety margins determination by developing best practices for safety requirements verification against external hazards, using efficient and integrated set of Safety Engineering practices and probabilistic safety assessment.

The benchmark baseline of BESEP is defined within the Work Package 2 (WP2 - Benchmark baseline). WP2 contains the following main tasks:

- T2.1 Assignment of safety requirement topics for selected external hazards
- T2.2 Creation of benchmark baseline by definition of detailed safety requirements (deliverable: this report)
- T2.3 Specification of key features of efficient and integrated Safety Engineering Process
- T2.4 Identification of general risk significance thresholds of external hazards.

Task 2.1 defines the external hazards, safety analysis methods, systems, structures and components and a set of requirements involved in the comparison and evaluation of safety engineering processes used by the BESEP project partners.

This report is the deliverable of Task 2.2. Main tasks of Task 2.2 are to identify and assign important safety requirement topics and to create the benchmark baseline. Each safety requirement topic, identified partly based on Task 2.1, is elaborated to a set of more detailed safety requirements suitable for the cross case and cross-group comparisons.

Specification of key features of efficient and integrated safety engineering process is involved in Task 2.3. Task 2.4 focuses on identification of general risk-significance thresholds of external hazards.

The requirement baseline of Task 2.2 will be later used in the work packages 3 and 4 for Cross-case comparison within case study groups in Task 3.4 and Comparison between generalized case studies representing the different case study groups in Task 4.2. Also, the requirement topics are used in the set of attributes used for grouping case studies in Task 3.2. In formulating the case studies for further work within BESEP the requirements elaborated in this Task 2.2 are used as a basis, i.e. the fulfilment of one or more safety requirement(s) in relation to external hazards identified in Task 2.2 should be verified within a case study.

Due to the stepwise implementation in BESEP there may occur a need later to define some additional requirements or even additional requirement topics to better proceed with the case study creation or comparison. In this case the new requirements or requirement topics will be defined and described in the corresponding deliverables of the tasks in question.

Chapter 2 of this report presents the national legal framework and the regulatory environment in the BESEP partner countries. It provides background for the requirement base used in defining the BESEP requirement baseline. Additionally, Chapter 2 provides comparison of some common subjects, i.e. initiating event classification and core damage and large early release frequency.

Chapter 3 defines the safety requirement topics for BESEP project. The requirement topics are defined for deterministic safety analysis, probabilistic safety analysis and human factors engineering as well as for safety engineering practices. The topics are defined based on knowledge on the preliminary case studies (collected in the proposal stage of the project [1]), based on the coming work in the project and engineering decisions. The requirement topics cover just parts of the analysis or process relevant for the coming work in the project.

Chapter 4 defines the requirement baseline based on the requirement topics. Input for the requirement baseline requirements are the high-level IAEA requirements identified in Task 2.1 and the national requirements collected by the BESEP partners. The national requirements have been collected during the beginning of the work in Task 2.2 and the selection has been based on the partners' judgement on the relevance for the project. Not all national requirements are included in the requirement base. All input requirements are first classified into the topics, and based on this selection the actual BESEP requirements to be used in the project are elaborated.

Conclusions are presented in the Chapter 5. The BESEP requirement baseline as a whole is shown in the Appendix A of the report. The input requirements for each safety requirement topic are shown in Appendix B.

2 National Legal Framework and the Regulatory Environment

In each BESEP participant country there are different national legislation, regulation, guides/ guidelines and requirements for nuclear installations with respect to protection against external hazards, analysis methods etc.

Based on participants' evaluation the relevant national requirements have been selected and collected to be used in the definition of the requirement baseline.

The national regulatory environment and the national sources for the BESEP requirement baseline are described in the following sections.

2.1 Czech Republic

The State Office for Nuclear Safety is the central authority of state administration responsible for exercise of regulatory activities in the peaceful utilisation of nuclear energy and ionizing radiation and in the field of non-proliferation of weapons of mass destruction. The State Office for Nuclear Safety (hereinafter referred to as "the Office") is headed by a Chairperson appointed and recalled by the Government of the Czech Republic. The Office has an autonomous budget and reports directly to the Government of the Czech Republic.

Based on the Act No. 263/2016 Coll., the Atomic Act, the Act No. 19/1997 Coll., and the Act No. 281/2002 Coll., the Office carries out the competence of the state. Following activities among others fall within its scope:

- authorization of activities performed in accordance with the Atomic Act, e.g. siting and operation of nuclear facilities, ionizing radiation sources and radioactive waste management;
- approval of documentation relating to ensuring nuclear safety, monitoring of the radiation situation, radiation extraordinary event management, limits and conditions of nuclear facilities operation, on-site emergency plans of nuclear facilities.

Part of the Office are eight Regional Centers, and two Site Inspectors Division at Temelín NPP and Dukovany NPP.

The Office is the founder of two public research institutions - National Radiation Protection Institute, and National Institute for Nuclear, Chemical and Biological Protection.

System of the new nuclear law of the Czech Republic has entered into force on 1st January 2017. Some selected regulations related to nuclear safety:

- Act No. 263/2016 Coll., atomic act;
- Decree No. 358/2016 Coll., on requirements for assurance of quality and technical safety and assessment and verification of conformity of selected equipment;
- Decree No. 359/2016 Coll., on details of ensuring radiation extraordinary event management;
- Decree No. 360/2016 Coll., on radiation situation monitoring;
- Decree No. 361/2016 Coll., on security of nuclear installation and nuclear material;
- Decree No. 374/2016 Coll., on the accountancy and control of nuclear materials and reporting of information on them;
- Decree No. 375/2016 Coll., on selected items in the nuclear area;
- Decree No. 377/2016 Coll., on the requirements for the safe management of radioactive waste and on the decommissioning of nuclear installations or category III or IV workplaces;
- Decree No. 378/2016 Coll., on siting of a nuclear installation;
- Decree No. 408/2016 Coll., on management system requirements;
- Decree No. 409/2016 Coll., on activities especially important from nuclear safety and radiation protection viewpoint, special professional qualification and training of persons ensuring radiation protection of the registrant;
- Decree No. 422/2016 Coll., on radiation protection and security of a radioactive source.

All decrees are available at https://www.sujb.cz/en/legal-framework/nuclear-law.

2.2 Finland

Legal basis of the use of nuclear energy consist of the Nuclear Energy Act (990/1987) [2] and the Nuclear Energy Decree (161/1988) [3]. Detailed provisions, the regulations and guidelines published by the Radiation and Nuclear Safety Authority's (STUK) and supervision ensure that the objectives of legislation for the safe use of nuclear energy are achieved.

The use of nuclear energy always requires a licence. The legislation lays down various obligations for operators carrying out activities requiring a licence, such as ensuring the safety of nuclear energy use and managing the nuclear waste. The fulfilment of these obligations is supervised by the Ministry of Economic Affairs and Employment and STUK.

The use and supervision of nuclear energy are regulated by several international agreements. Finland's national nuclear energy legislation fulfils the country's international commitments. The European Union regulates the nuclear energy sector through the Euratom Treaty and the directives under it. The Finnish regulations are visualized in the Figure 2.1.

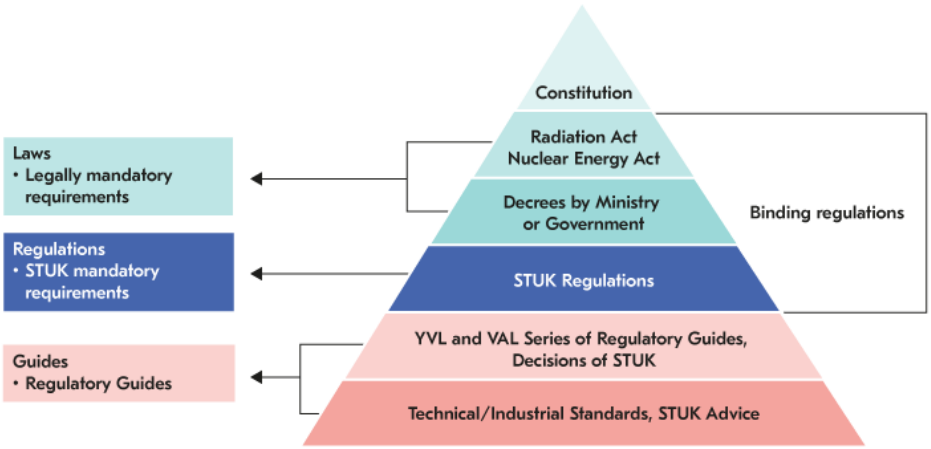


Figure 2.1 Finnish regulations [https://www.stuk.fi/web/en/regulations]

The safety requirements of STUK are binding on the licensee, while preserving the licensee's right to propose an alternative procedure or solution to that provided for in the regulations. If the licensee can convincingly demonstrate that the proposed procedure or solution will implement safety standards in accordance with this Act, STUK may approve a procedure or solution by which the safety level set forth is achieved.

Of the STUK regulations and guidelines relevant for BESEP project are seen the regulation STUK Y/1/2018 [4] and the regulatory guides on nuclear safety (YVL guides) A.3 [5], A.4 [6], A.6 [7], A.7 [8], B.1 [9], B.3 [10], and B.7 [11] of which selected requirements have been identified to be used in the requirement base.

2.3 France

ASN (Nuclear Safety Authority) is the French administrative and independent authority (law 2006-686 of 13 June 2006) on nuclear safety. ASN as the regulatory body ensures the oversight of nuclear safety and radiation protection in order to protect people and the environment. ASN is responsible for protecting and informing the public (transparency on nuclear matters) in order to protect workers, medical patients, the public and the environment from the risks involved by nuclear activities. (http://www.french-nuclear-safety.fr/)

The nuclear regulation in France is prescriptive. The independent regulator is proposing the regulation rules that are then discussed and adopted by the Parliament through Legislative orders and applied through additional decrees relating to nuclear installations (INB – Basic Nuclear Installation) such as:

- Decree 2007-1557 of 2 November 2007 concerning basic nuclear installations and the supervision of the transport of radioactive materials with respect to nuclear safety [12]
- Law – France– JORF No. 0033 of 8 February 2012, page 2231 Text No. 12 – consolidated version 09th September 2014 – French Order of 7 February 2012 setting the general rules relative to basic nuclear installations (environmental code) [13].

In addition the Regulator is providing guides such as the guide nb 22 for the design of Nuclear power plants giving practical guidance and interpretation of the regulation:

- Guide – ASN – Nb°22 18/07/2017 – Design of Pressurised Water reactor (Translated from ASN Conception des réacteurs à eau sous pression – Guide n°22) edited with support from IRSN [14].

IRSN (Radioprotection and Nuclear Safety Institute, https://www.irsn.fr/) is a Technical Support Organization (TSO). It is the French public service expert in nuclear and radiation risks and supports ASN by providing technical advice on nuclear installation. IRSN has research missions in: (nuclear safety, safety of transport of

radioactive and fissile materials, protection of man and the environment against ionizing radiation, protection and control of nuclear materials, protection of nuclear facilities and transport of radioactive and fissile materials against malicious acts.

Figure 2.2 visualises the regulatory pyramid of France [15].

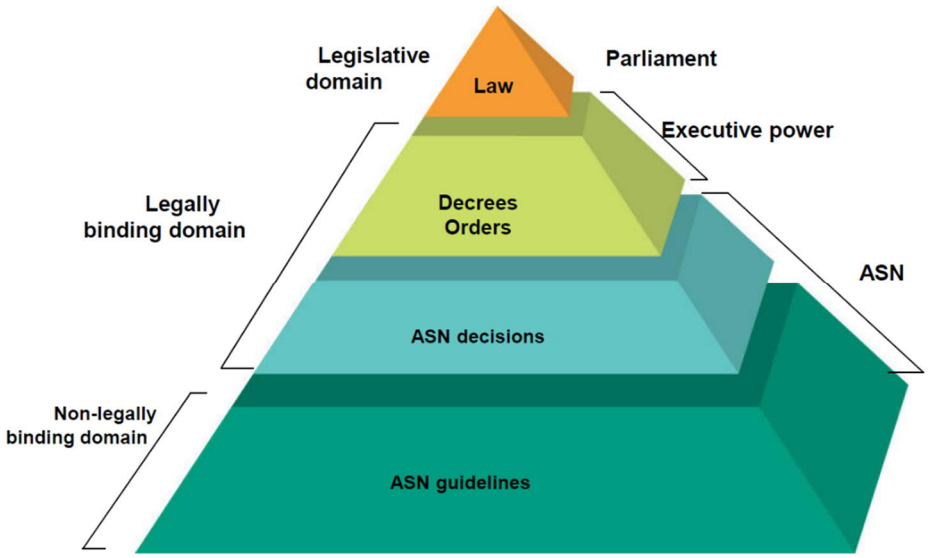


Figure 2.2 French regulatory pyramid [15]

2.4 Hungary

In Hungary, the Act CXVI of 1996 on Atomic Energy [16] is on force on the peaceful use of nuclear energy. Based on the authorization provided, among others, in the Act on Atomic Energy, Govt. Decree 118/2011 (VII. 11.) [17][18][19] describes the nuclear safety requirements of nuclear facilities and related regulatory activities. Annexes 1 to 10 of this decree contain the Nuclear Safety Code, which include the nuclear safety requirements related to regulatory procedures regarding nuclear safety of nuclear facilities, management systems of nuclear facilities, and the execution and supervision of activities according to the life cycle of nuclear facilities.

The Nuclear Safety Code represents high level nuclear safety requirements that shall be fulfilled in relation to nuclear facilities in Hungary. In particular, Volume 3 [19], Volume 3a [18] and Volume 7 [17] of the Nuclear Safety Code are of particular interest in the BESEP Project. Volume 3 includes design requirements for operating nuclear power plants, Volume 3a lists design requirements for new nuclear power plants, while Volume 7 contains requirements for site investigation and evaluation of nuclear facilities.

Besides the nuclear safety requirements and provisions, those individual authority requirements, conditions and obligations shall be met that are determined by the nuclear safety authority in its resolutions regarding nuclear safety. Several regulatory guides have been issued by the Hungarian Atomic Energy Authority (HAEA) in order to facilitate the compliance with the requirements of the Nuclear Safety Code. If methods different from those laid down in the regulatory guides are applied, then the authority shall conduct an in-depth examination to determine if the applied method is correct, adequate and full scope, which may entail a longer regulatory procedure, involvement of external experts and extra costs. During its activities the HAEA also considers the standards, guidelines and recommendations of international organizations (e.g. IAEA, ENSREG and OECD NEA) and other countries having advanced nuclear industry.

Requirements described in the Nuclear Safety Code have been looked at for the purposes of this Task 2.2 of the project. In particular, the requirements given in Volume 3 and Volume 7 of the Nuclear Safety Code were considered because the case studies that have been proposed by NUBIKI for evaluation in the project are related to the Paks NPP as an operating nuclear power plant in Hungary.

2.5 Slovak Republic

The Nuclear Regulatory Authority of the Slovak Republic (UJD SR) is a central government authority of the Slovak Republic for nuclear regulation. The authority exercises state supervision over nuclear safety of nuclear installations, including radioactive waste management, spent fuel management and other stages of the fuel cycle, over nuclear materials, including their inspection and registration, as well as over physical protection of nuclear installations and nuclear materials provided for by the relevant license holder.

The Authority performs assessment of plans for use of nuclear energy and the quality of classified equipment and nuclear technology devices and the commitments of the Slovak Republic arising from international treaties on nuclear safety of nuclear installations and nuclear materials management. UJD SR is a legal entity; rules for managing funds of a state budgetary organization apply, it has a separate chapter in the state budget, it has no subordinated bodies on a regional or district levels, and it is not a founder of any state budgetary or state contributory organization or any other legal entities.

The most important Act in the area of peaceful use of nuclear power in the Slovak Republic is Act no. 541/2004 Coll. on the Peaceful use of nuclear energy (Atomic Act) [20] and on amendment and alterations of several acts as amended. The nuclear safety requirements are defined in more detail in Decree of the Nuclear Regulatory Authority of the Slovak Republic No. 430/ 2011 Coll. As amended by Decree No. 103/2016 Coll. on nuclear safety requirements (consolidated version) [21].

In addition to abovementioned regulation also guides Requirements for deterministic safety analyses of VVER440 type reactors, BN 5/2019 and Requirements for PSA, BNS I.4.2/2017 [23] are relevant for BESEP project.

The J. Bohunice plant (Unit 3 and 4) and the Mochovce plant (Unit1 and 2) are in operation. The Mochovce plant (Unit 3 and 4) is under construction. The case studies developed by RELKO are related to these plants.

2.6 Sweden

The constitutional structure in Sweden is based on laws decided by the parliament, ordinances decided by the government and regulations decided by the Swedish Radiation Safety Authority. The level of detail is in general higher for the ordinances compared with the laws and higher for the regulations compared to the ordinances.

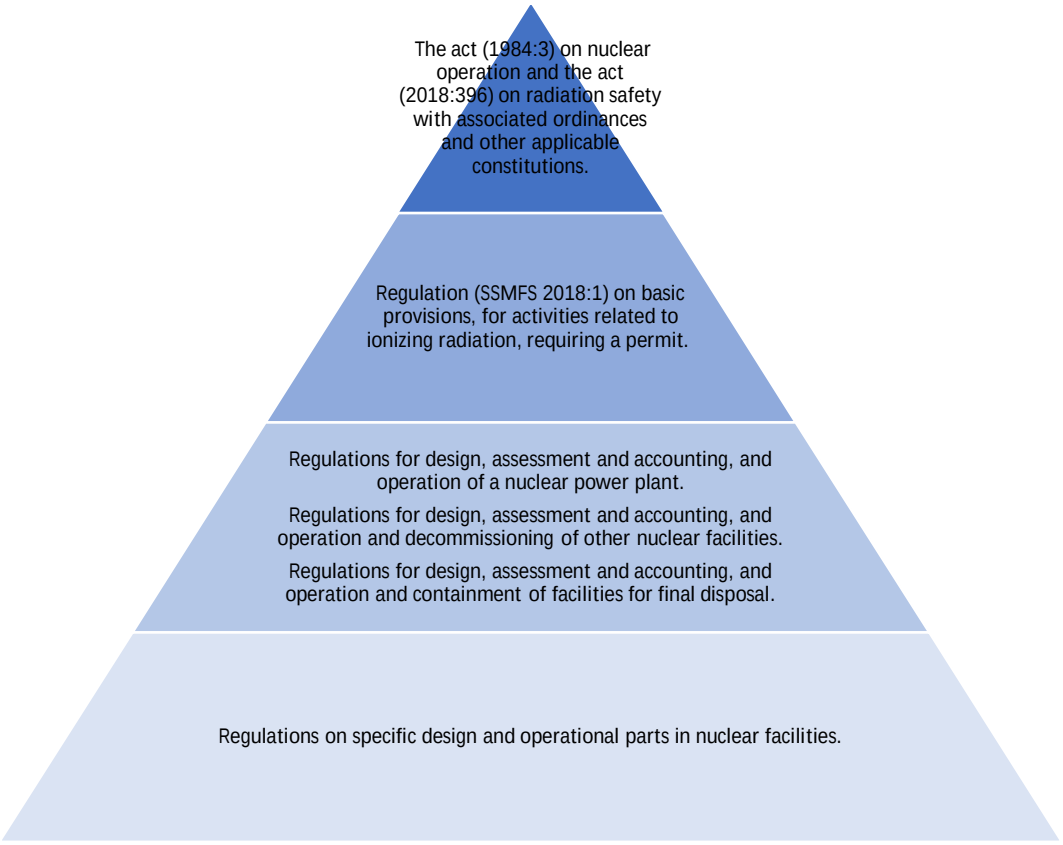


Figure 2.3 Swedish regulatory environment

The Swedish Radiation Safety Authority's (SSM) regulations concerning Safety in Nuclear Power Plants (NPPs), which are represented by level 2 in the Figure 2.3, are divided into three parts:

- SSMFS-K (SSM regulations concerning the design and construction work of NPPs) [25],
- SSMFS-A (SSM regulations concerning the assessment and reporting of NPPs design and operation) [24], and
- SSMFS-D (SSM regulations concerning the maintaining and assessment of design of NPPs) [26].

Briefly SSMFS-K contains regulations regarding the work that must be done in order to produce a basis for manufacturing and construction or installation as well as regulations regarding the expected characteristics for the result of this work. In other words, how a NPP should be constructed. SSMFS-A contains regulations about the assessment and accounting to confirm that there are prerequisites in order to maintain radiation safety at the NPP. SSMFS-D contains regulations regarding maintaining and assessment of the radiation safety during operation of the NPP.

The level 3 requirements, technical specifications, are specific to the different nuclear facilities in Sweden.

2.7 Comparison of Some Subjects in National Requirements

2.7.1 Event classification

The event classification varies to some extent between the BESEP partner countries. In this section they are grouped/listed based on IAEA classification to provide a holistic view on national event classification requirements. The event groups used in the comparison are:

- Anticipated operational occurrences
- Design basis accidents

- Design extension conditions without significant fuel degradation
- Design extension conditions with core melt.

Anticipated operational occurrences are listed in the Table 2.1 below and their acceptance criteria in the Table 2.2.

Table 2.1 Anticipated operational occurrences

	Occurrence (1/reactor year)	**Plant state**	**Terminology**
IAEA	> 10^{-2} events per year	Anticipated operational occurrences	-
Czech Republic	> 10^{-1} events per year	AOO (DBC1, DBC2)	high frequency events
	> 10^{-2} events per year	DBA (DBC3)	medium frequency events
Finland	> 10^{-2} events per year		DBC 2
France	> 10^{-2} events per year		DBC2
Hungary	> 10^{-2} events per year	Anticipated operational occurrences	DBC2
Slovak Republic	> 10^{-2} events per year		AOO
Sweden	> 10^{-2} events per year		H2

Table 2.2 Acceptance criteria for anticipated operational occurrences

	Acceptance criteria (fuel)	**Acceptance criteria (containment and dose)**	**Acceptance criteria (primary circuit)**	**Acceptance criteria (other)**
IAEA	No additional fuel damage			
Czech Republic	Adequate cooling of the cladding shall be ensured. Cooling of the cladding is considered adequate if there is a 95% probability at 95% confidence level that the hottest fuel rod does not reach heat transfer crisis. Temperature in any part of the fuel pellets shall not exceed the predefined value (used in some scenarios).	Annual dose of the representative person of the population shall not exceed 0.1 mSv from all exposition paths in AOO. Annual dose of the representative person of the population shall not exceed 1 mSv from all exposition paths in DBA.	The pressure in the primary circuit shall not exceed the predefined value.	The pressure in the secondary circuit shall not exceed the predefined value.

	Acceptance criteria (fuel)	Acceptance criteria (containment and dose)	Acceptance criteria (primary circuit)	Acceptance criteria (other)
Finland	In anticipated operational occurrences, the nuclear fuel shall fulfil the following conditions: - No melting shall occur in fuel pellets. - Adequate cooling of the cladding shall be ensured. Cooling of the cladding is considered adequate if there is a 95% probability at 95% confidence level that the hottest fuel rod does not reach heat transfer crisis. Alternatively, it may be demonstrated that the number of rods reaching heat transfer crisis does not exceed 0.1% of the total number of fuel rods in the reactor. - The probability of fuel failure caused by mechanical interaction between fuel and cladding shall be extremely low.	The containment shall be designed to maintain its integrity during DBC2 events. Annual dose of the representative person of the population arising as the result of DBC2 event shall not exceed 0.1 mSv.	The design pressure of primary circuit shall not be exceeded and primary circuit's safety valves shall not open in DBC2 events.	
France	Integrity of the fuel rods with respect to the different modes of damage is demonstrated, no fuel clad failure: various physical phenomena (hydraulic, thermohydraulic, mechanical and thermal) stressing the first barrier are taken into account.	Operating conditions do not lead to loss of integrity of a containment barrier.	Ensure that reference operating conditions do not induce release of primary fluid in the containment.	

	Acceptance criteria (fuel)	Acceptance criteria (containment and dose)	Acceptance criteria (primary circuit)	Acceptance criteria (other)
Hungary	For anticipated operational occurrences, the following thresholds shall be used as a minimum for fuel damage mechanisms and prevention of fuel damage: - Temperature of fuel cladding Cooling of the cladding is considered adequate if there is a 95% probability at 95% confidence level that the hottest fuel rod does not reach heat transfer crisis or departure from nucleate boiling. - Fragmentation of nuclear fuel pellets The fragmentation of the pellet material in any fuel is not allowed in such a manner that would result in fuel damage. Nuclear fuel failure is assumed if the radial average enthalpy of a fuel rod at any axial location exceeds the value 586 J/gUO2. - Melting of fuel pellets The fuel pellet temperature shall not exceed the melting point. - Other mechanisms that may cause damage Nuclear fuel shall not be damaged due to other reasons, e.g. mechanical hits.	The containment shall be designed to maintain its integrity during DBC2 events (containment pressure shall not exceed the design value (0.25 MPa) and the pressure drop on the bubble condenser shall not exceed the design value (30 KPa)). The dose determined for 1 person of the reference group of the population shall not exceed the value of the public dose constraint. DBC2 events shall not cause doses exceeding 1 Sv/event/person outside the controlled area of the nuclear power plant, in operational areas authorized for human presence.	The pressure in the primary circuit shall not exceed 110% of the design value (135 bar).	

	Acceptance criteria (fuel)	Acceptance criteria (containment and dose)	Acceptance criteria (primary circuit)	Acceptance criteria (other)
Slovak Republic	The realistic analyses should aim to demonstrate that no induced damage is caused to any of the physical barriers (fuel matrix, fuel cladding, and reactor coolant pressure boundary or containment) or the systems important to safety. Failures of physical barriers are typically prevented by providing assurance that, with 95% probability at a 95% confidence level, there will be no boiling crisis or dry-out anywhere in the core, no fuel melting anywhere in the core and that the pressure in the reactor coolant system and main steam system will not significantly (i.e. by more than 10–15%) exceed the design value.	There should be negligible radiological impact beyond the immediate vicinity of the plant from any anticipated operational occurrence. The radiological acceptance criteria for doses and correspondingly for releases for each anticipated operational occurrence should be comparable with annual limits for normal operation and more restrictive than for design basis accidents. Acceptable effective dose limits are similar to those for normal operation.	The pressure in the reactor coolant system will not significantly (i.e. by more than 10–15%) exceed the design value.	
Sweden	No damage on the fuel shall occur.	The containment shall be designed so that the basic functions can be performed during H2-H5 events. Annual dose of the representative person of the population arising as the result of H2 shall not exceed 1 mSv.	As far as reasonable and possible the safety valves on circuits that passes through the reactor wall shall be designed so that they can be closed tight in those cases that the containment is contributing to the fulfilling of the basic functions at events and conditions in event classes H1-H5.	

Design basis accidents are listed in the Table 2.3 below and their acceptance criteria in the Table 2.4.

Table 2.3 Design basis accidents

	Occurrence (1/reactor year)	**Plant state**	**Terminology**
IAEA	10^{-2} – 10^{-6} events per year	Design basis accidents	-
Czech Republic	10^{-2} – 10^{-4} events per year	DBA (DBC4)	low frequency events
Finland	10^{-2} – 10^{-4} events per year		DBC 3
	> 10^{-4} events per year		DBC 4
France	10^{-2} – 10^{-4} events per year		DBC3
	> 10^{-4} events per year		DBC4
Hungary	10^{-2} – 10^{-5} events per year	Design basis accidents	DBC 4
Slovak Republic	> 10^{-4} events per year		DBA
Sweden	10^{-2} – 10^{-4} events per year		H3
	10^{-4} – 10^{-6} events per year		H4A

Table 2.4 Acceptance criteria for design basis accidents

	Acceptance criteria (fuel)	**Acceptance criteria (containment and dose)**	**Acceptance criteria (primary circuit)**	**Acceptance criteria (other)**
IAEA	No radiological impact at all, or no radiological impact outside the exclusion area			
Czech Republic	The fuel cladding temperature shall not exceed 1200 °C. The radial average enthalpy of a fuel rod at any axial location shall not exceed the predefined value. The fuel oxidation shall not exceed the predefined value.	The pressure in containment shall not exceed predefined value. Two days dose of the representative person of the population shall not exceed 10 mSv, no dose from ingestion is considered.	The pressure in the primary circuit shall not exceed the predefined value.	The pressure in the secondary circuit shall not exceed the predefined value.

Finland	DBC 3 event shall not cause significant changes to the original fuel geometry. To ensure this, the nuclear fuel shall fulfil the following criteria: - The number of fuel rods reaching heat transfer crisis shall not exceed 1% of the total number of fuel rods in the reactor. - The maximum temperature of the nuclear fuel cladding shall not increase to the extent that oxidation of the cladding or changes in the cladding material properties could endanger the integrity of the cladding during an accident. This requirement can be considered fulfilled without a separate justification if the temperature does not exceed the value of 650°C. - The number of fuel failures caused by mechanical interaction between nuclear fuel and cladding shall not exceed 0.1% of the total number of fuel rods in the reactor. DBC 4 events: - The number of fuel rod failures in a Class 2 postulated accident shall not exceed 10% of the total number of fuel rods in the reactor. Nuclear fuel failure is assumed if the radial average enthalpy of a fuel rod at any axial location exceeds the value 586 J/gUO2	The containment shall maintain its integrity with a high degree of certainty during DBC 3 and DBC 4 events. Annual dose of the representative person of the population arising as the result of DBC3 event shall not exceed 1 mSv. Annual dose of the representative person of the population arising as the result of DBC4 event shall not exceed 5 mSv.	In DBC 3 events, primary circuit pressure shall not exceed pressure which is 1.1 times the design pressure of the protected target. In DBC 4 events, primary circuit pressure shall not exceed pressure which is 1.1 times the design pressure of the protected target	
France	In DBC3 events: Melting of fuel pellets	Integrity of the containment is	The primary circuit does not suffer any	

	Acceptance criteria (fuel)	Acceptance criteria (containment and dose)	Acceptance criteria (primary circuit)	Acceptance criteria (other)
	at the hot spot is avoided; damage to the structure of fuel assemblies and fuel rods fuel do not affect the possibility of unloading and storage of the fuel ; In DBC4 events: Melting of the fuel pellet at the hot spot of the core remains limited.	ensured and the other components of the 3rd barrier do not suffer damage affecting their integrity other than the direct consequences of the event. Consequences of damage to the 1st barrier is limited in terms of the number of fuel rods affected and of severity.	damage affecting its integrity other than the direct consequences of the event; Core geometry must remain coolable	

	Acceptance criteria (fuel)	Acceptance criteria (containment and dose)	Acceptance criteria (primary circuit)	Acceptance criteria (other)
Hungary	For design basis accidents, the following thresholds and limitations shall be used as a minimum: - The fuel cladding temperature shall not exceed 1200°C. - The extent of oxidation shall not exceed 17% (of the thickness of the fuel cladding). - Hydrogen generated in the chemical reaction between the fuel cladding and the coolant shall not exceed 1% of the amount that would be generated if the entire fuel cladding would be in reaction with the coolant. - The radial average enthalpy of a fuel rod attributable to the increase of fuel heat capacity at any axial location shall not exceed the value of 963 J/gUO2. - The deformation of reactor internals shall not prevent the flow of the coolant. - Control rod mechanisms shall not be fully or partially melted.	The containment shall be designed to maintain its integrity during DBC4 events (containment pressure shall not exceed the design value (0.25 MPa) and the pressure drop on the bubble condenser shall not exceed the design value (30 KPa)). The dose determined for 1 person of the reference group of the population shall not exceed 5mSv/event. DBC4 events shall not cause doses exceeding 10 mSv effective dose or 100 mGy dose for the thyroid outside the controlled area of the nuclear power plant and in operational areas authorized for human presence.	The pressure in the primary circuit shall not exceed 110% of the design value (135 bar).	
Slovak Republic	For DBA the technical acceptance criteria relating to fuel integrity should, in principle, be the same as for realistic analysis of anticipated operational occurrences.	The containment integrity is maintained. The acceptable limits of effective dose for members of the public beyond the immediate vicinity of the plant are typically in the order of a few millisieverts per event (5 mSv).		

	Acceptance criteria (fuel)	Acceptance criteria (containment and dose)	Acceptance criteria (primary circuit)	Acceptance criteria (other)
Sweden	Only a few of the fuel rods are allowed to be damaged.	The containment shall be designed so that the basic functions can be performed during H2-H5 events. Annual dose of the representative person of the population arising as the result of H3 shall not exceed 10 mSv. Annual dose of the representative person of the population arising as the result of H4A, H4B shall not exceed 100 mSv	As far as reasonable and possible the safety valves on circuits that passes through the reactor wall shall be designed so that they can be closed tight in those cases that the containment is contributing to the fulfilling of the basic functions at events and conditions in event classes H1-H5.	

Design extension conditions without significant fuel degradation are shown in the Table 2.5 below their acceptance criteria in the Table 2.6.

Table 2.5 Design extension conditions without significant fuel degradation

	Occurrence (1/reactor year)	**Plant state**	**Terminology**
IAEA	10^{-4} – 10^{-6} events per year	Design extension conditions without significant fuel degradation	-
Czech Republic	10^{-4} – 10^{-6} events per year	DEC-A	very low frequency events
Finland	no frequency, DBC 2/3 + CCF	-	DEC A
	no frequency, complex sequences	-	DEC B
	no frequency, rare external events	-	DEC C
France	-	-	DEC-A
Hungary	no frequency (>10^{-7} events per year)	complex accidents	DEC1
Slovak Republic	> 10^{-7} events per year	-	DEC-A
Sweden	-	-	H4B

Table 2.6 Acceptance criteria for design extension conditions without significant fuel degradation

	Acceptance criteria (fuel)	**Acceptance criteria (containment and dose)**	**Acceptance criteria (primary circuit)**	**Acceptance criteria (other)**
IAEA	Radiological consequences outside the exclusion area within limits			
Czech Republic	The fuel cladding temperature shall not exceed 1200 °C. The radial average enthalpy of a fuel rod at any axial location shall not exceed the predefined value. The fuel oxidation shall not exceed the predefined value.	The pressure in containment shall not exceed predefined value. Two days dose shall not exceed 10 mSv, no dose from ingestion is considered.	The pressure in the primary circuit shall not exceed the predefined value.	The pressure in the primary circuit shall not exceed the predefined value.

	Acceptance criteria (fuel)	Acceptance criteria (containment and dose)	Acceptance criteria (primary circuit)	Acceptance criteria (other)
Finland	In DEC events, no melting shall occur in the control rods and structural deformations in fuel rods, fuel assemblies, control rods or reactor internals shall not obstruct the movement of control rods in the reactor.	The containment shall maintain its integrity with a high degree of certainty during DEC events. Annual dose of the representative person of the population arising as the result of DEC event shall not exceed 20 mSv.	In DEC events, primary circuit pressure shall not exceed pressure which is 1.2 times the design pressure of the protected target.	In DEC events, primary circuit pressure shall not exceed pressure which is 1.2 times the design pressure of the protected target.
France	Reactivity is under control; sub-criticality of the core is ensured after activation of the provisions and maintained over the long term.	Containment of radioactive substances is ensured in such a way that the safety objectives applicable to accidents without fuel melting are respected.	Evacuation of the residual heat is ensured.	
Hungary	No criteria (The criteria specified for DBC4 events are applied to determine whether fuel damage occurs or not. If not, then no further assessment is required. If partial of full fuel damage is occurred, then the environmental impacts should be assessed.)	The criterion of limited environmental impacts (EUR) should be fulfilled:		

	Acceptance criteria (fuel)	Acceptance criteria (containment and dose)	Acceptance criteria (primary circuit)	Acceptance criteria (other)
Slovak Republic	Acceptance criteria for design extension conditions should meet the requirement established in para. 5.31A of SSR-2/1 (Rev. 1). The design shall be such that for design extension conditions, protective actions that are limited in terms of lengths of time and areas of application shall be sufficient for the protection of the public, and sufficient time shall			
Sweden		Large damage in the core shall not occur.	The containment shall be designed so that the basic functions can be performed during H2-H5 events. Annual dose of the representative person of the population arising as the result of H4A, H4B shall not exceed 100 mSv.	As far as reasonable and possible the safety valves on circuits that passes through the reactor wall shall be designed so that they can be closed tight in those cases that the containment is contributing to the fulfilling of the basic functions at events and conditions in event classes H1-H5.

Design extension conditions with core melt are shown in the Table 2.7 below and their acceptance criteria in the Table 2.8.

Table 2.7 Design extension conditions with core melt

	Occurrence (1/reactor year)	Plant state	Terminology
IAEA	$< 10^{-6}$ events per year		Design extension conditions with core melt
Czech Republic		DEC B, severe accidents	very low frequency events
Finland	no frequency		SA
France			DEC-B

	Occurrence (1/reactor year)	Plant state	Terminology
Hungary	no frequency (>10^{-7} events per year)	severe accidents	DEC2
Slovak Republic	CDF > 10^{-8}		DEC-B
Sweden	< 10^{-6} events per year		H5
	-		H6

Table 2.8 Acceptance criteria for design extension conditions with core melt

	Acceptance criteria (fuel)	Acceptance criteria (containment and dose)	Acceptance criteria (primary circuit)	Acceptance criteria (other)
IAEA	-			
Czech Republic		The overall dose during an accident shall not exceed 100 mSv, no dose from ingestion is considered.		
Finland		To limit the long-term effects, the limit value for cesium-137 emissions to ambient air is 100 TBq. The possibility of exceeding the limit value must be very small.		The release of radioactive substances must not be accompanied by the need for extensive protection measures for the population or long-term restrictions on the use of large areas of land and water.
France		Corium is cooled; sub-criticality and evacuation of the residual power are ensured. The containment of radioactive substances is controlled according to the objectives and applicable to accidents with fuel melting are respected.		
Hungary				

	Acceptance criteria (fuel)	Acceptance criteria (containment and dose)	Acceptance criteria (primary circuit)	Acceptance criteria (other)
Slovak Republic		Technical acceptance criteria should represent conditions such that the integrity of the containment is maintained. Examples of acceptance criteria for analysis of design extension conditions include limitation of the containment pressure, containment water level, temperature and flammable gas concentrations, and stabilization of molten corium.		
Sweden		As far as reasonable and possible the safety valves on circuits that passes through the reactor wall shall be designed so that they can be closed tight in those cases that the containment is contributing to the fulfilling of the basic functions at events and conditions in event classes H1-H5.	For the events taken into consideration, that are not extremely unlikely, the release frequency of more than 0,1 % of the cesium isotopes 134 and 137 in the core of a reactor with a thermal effect of 1800 MW must be lower than $1* 10^{-7}$ per reactor year.	

2.7.2 Core damage frequency and large early release frequency

The target values for Core damage frequency (CDF) and large early release frequency (LERF) vary to some extent between the BESEP partner countries. In this section they are shown in the Table 2.9 below to provide a holistic view on national event classification requirements.

Table 2.9 National event classification requirements

	Core Damage Frequency (CDF), events per year	**Large Early Release Frequency (LERF), events per year**	**Comment**
IAEA	< $1 * 10^{-4}$ for existing plants < $1 * 10^{-5}$ for future plants	N/A	-
Czech Republic	< $1 * 10^{-4}$ per year	< $1 * 10^{-5}$ per year	Recommended safety target for "older" plants, valid for both NPP Dukovany and NPP Temelin.
Finland	< $1 * 10^{-5}$ per year	< $5 * 10^{-7}$ per year	-
France	< $1 * 10^{-5}$ per year	N/A	LERF : must be made physically impossible or if not, extremely improbable with a high degree of confidence. New CDF: 10^{-5} (Internal events and hazards); 10^{-6} (internal events only).
Hungary	< $1 * 10^{-4}$ per year	< $1 * 10^{-5}$ per year	- for LERF criterion earthquake may be excluded. - < $1 * 10^{-6}$ per year shall be targeted.
Slovak Republic	< $1 * 10^{-4}$ for existing plants < $1 * 10^{-5}$ for future plants	< $1 * 10^{-5}$ for existing plants < $1 * 10^{-6}$ for future plants	-
Sweden	-	-	Unacceptable release is defined as more than 0,1 % of the cesium isotopes 134 and 137 in the core of a reactor with thermal effect of 1800 MW. No requirements are set on CDF or release frequencies, though by state of practice $1 * 10^{-5}$ per reactor year for CDF and $1 * 10^{-7}$ per reactor year for unacceptable release is used as safety goals.

3 Safety Analyses and the Related Safety Requirement Topics

As stated in the report *Assignment of safety requirement topics of selected external hazards* (BESEP deliverable 2.1) [27] the following safety analyses and safety engineering practices are needed to ensure compliance with safety requirements for the plant:

1. Deterministic safety analyses (DSA) – analyses of initiating events induced by external hazards, evaluating of plant response, plant performance or success criteria

2. Probabilistic safety analyses (PSA) – modelling of accident sequences, quantification of their risk significance

3. Human factors engineering (HFE) – scope of testing and maintenance, operator and emergency response actions on the basis of pre- and post-hazard procedures, SB EOPs and SAMGs.

4. Safety engineering practices (SEP) – implementation of safety requirements to exiting plant design for fulfilling the Defence-in-Depth principle.

In the report [27] the IAEA high-level requirements were used as a starting point to identify the safety requirement topics which are assigned to external hazards involved in the BESEP preliminary case studies. As the IAEA high-level requirements are more of technical nature it was discovered during the work in Task 2.2 that an updated set of requirement topics is needed to create a requirement baseline for the project. Based on the preliminary case studies and general experience of the BESEP partners the safety requirement topics have been defined to be used in the project. These safety requirement topics are presented in the following sub-sections. The list of topics is not comprehensive, i.e. there are several other topics related to the different types of safety analyses, but the selected topics are seen relevant to the BESEP project.

3.1 Deterministic Safety Analysis

Deterministic safety analyses approaches are conducted on different levels. Deterministic hazard analyses are performed for the site. Deterministic fragility analyses are typically performed for the systems, structures and components while deterministic safety margin analyses, such as seismic margin analyses are typically performed on the plant unit level. The overall objective of the different approaches is to support the evaluation of the plant response in different initiating events, including external hazards.

The DSA topics used in the forming of BESEP requirement baseline and short descriptions on the focus of each topic are given below. The presented list is not trying to be a comprehensive representation of DSA topics. The purpose is to identify DSA topics of interest supporting the benchmark and the objectives of BESEP project.

- **Physical separation and structural integrity**, this topic focuses on evaluating the protection of the safety functions (and their systems, structures and components) from the effects of external hazards and how the structural integrity is maintained;

- **Functional separation to provide defence against failure propagation**, this topic focuses on evaluating how the implemented or designed functional separation provides defence in case of external hazards;

- **Diversity and common-cause failure criteria**, this topic evaluates the adequacy of the diversity and the tolerability of the design against common-cause failures;

- **Redundancy and single failure criteria**, this topic evaluates the adequacy of the redundancy designed or implemented in the safety functions (and their systems, structures and components) and the tolerability against single failures;

- **Independence and strength of the individual defence-in-depth levels**, this topic focuses on larger view compared to the physical and functional separation topics, i.e. on the safety functions and their interrelations in individual defence-in-depth levels;

- J**ustification of the engineering assumptions used in analysis**, this topic focuses on the assumptions made in conducting the DSA and on their justification.

3.2 Probabilistic Safety Analysis

External hazards probabilistic safety analysis focuses on seismic, non-seismic natural hazards and human-induced hazards that may occur and affect the safety of the nuclear power plant. The failure probabilities of systems, structures and components are assessed. Uncertainties associated with the external hazard load, the responses of buildings and components and strength of structures and components are considered. Then, the occurrence probabilities (or frequencies) of various accident sequences and the magnitude of their consequences are estimated. The key elements of a Level 1 external hazard PSA as identified in deliverable 2.1 [27], are:

- hazard analyses for the site
- fragility analyses for systems, structures and components required to perform safety functions, and
- plant response and accident sequence analyses.

The PSA topics used in the forming of BESEP requirement baseline and short descriptions on the focus of each topic are given below. The presented list is not trying to be a comprehensive representation of PSA topics. The purpose is to identify PSA topics of interest supporting the benchmark and the objectives of BESEP project.

- **Risk-informed management and balance of nuclear power plant design**, this topic focuses on using PSA in risk-informed decision making to ensure adequate and balanced safety design against different kinds of external hazards;
- **Fulfilment of quantitative safety goals**, this topic focuses on meeting the quantitative safety goals/targets/criteria, including the evaluation of the risk significance of failure combinations initiated by external hazards;
- **Initiating event frequency estimation**, this topic focuses on estimating initiating event frequencies for design-basis exceeding external events;
- **Assessment of potential losses of safety functions**, this topic focuses on complex failure combinations arising or occurring simultaneously with an external event;
- **Uncertainty analysis of accident sequences and operating times**, this topic focuses on uncertainties related to hazard, fragility and plant response analyses, success criteria and human interventions in accidents initiated by external events;
- **Confidence provision for defence against the occurrence of cliff-edge effects**, this topic focuses on using PSA to evaluate and mitigate cliff-edge effects;
- **Support for developing abnormal and emergency operating procedures and severe accident guidelines**, this topic focuses on using PSA to develop emergency operating and severe accident procedures.

3.3 Human Factors Engineering

Human factors engineering shall be applied in the design and construction of new nuclear power plants. It shall also be applied in designing modification works in the existing NPPs to the extent applicable. It is especially relevant in design of control, testing, operation and maintenance of systems. HFE focuses on avoiding, detecting and correcting human errors and on limiting their effects. In the plant modifications HFE issues are commonly covered with HFE program plan.

The HFE topics used in the forming of BESEP requirement baseline and short descriptions on the focus of each topic are given below. The presented list is not trying to be a comprehensive representation of HFE topics. The purpose is to identify HFE topics of interest supporting the benchmark and the objectives of BESEP project.

- **Situation awareness and assessment**, this topic evaluates how the design of the NPP, MCR and guidance support the situation awareness and assessment of the control room personnel;
- **Guidance selection, decision making and intelligent use of guidance**, this topic focuses on evaluation how the guidance supports the decision making and how the intelligent use of guidance can be achieved in complex design extension conditions;
- **Applicable HSI (Human System Interface)**, this topic evaluates how HSI can and shall be applied especially in complex design extension conditions;
- **Team working, effective communication and collaboration**, this topic evaluates the possibilities and advantages of effective team work and how it appears in or supports communication and general collaboration;
- **Workload, stress and fatigue management**, this topic evaluates how the design of organisation roles, the NPP design and the guidance as well the trainings support the management of workload, stress and fatigue in complex events.

3.4 Safety engineering practices

In addition to three analysis types mentioned above, BESEP also benchmarks the safety engineering practices. Safety engineering activities in BESEP scope are supporting the interaction/interconnection of DSA, PSA and HFE, but it is also a separate discipline to ensure the safety of NPP design. In a more broad view, safety engineering is also seen as an entity managing the interaction between safety requirements, safety analyses and plant design (V&V activities).

During the work on Task 2.2 a set of requirement topics related to safety engineering were developed/listed to support the creation of the requirement baseline. The topics and short descriptions on the focus of each topic are given below. The presented list is not trying to be a comprehensive representation of safety engineering topics. The purpose is to identify safety engineering topics of interest supporting the benchmark and the objectives of BESEP project.

- **Safety engineering management**, this topic concerns the processes and models regarding the general structured management of safety engineering activities of NPP license holders;
- **Safety design and requirement management for external hazards**, this topic concerns managing the balance between the plant safety design and the allocated safety requirements;
- **Flow of information between safety analyses**, this topic concerns interactions and interconnections between the three analysis methods (DSA, PSA, HFE);
- **Verification and validation (V&V) of design**, this topic concerns interaction between the three main elements of safety engineering: safety requirements, plant design, and safety analyses;
- **System modification and configuration management,** this topic concerns system modification configuration management;
- **Validated modelling and simulation analysis tools**, this topic concerns the validation and improvement of models and the tools used for the analysis of effects of external hazards.

4 BESEP Requirement Baseline

In this section the collected national requirements related to external hazards and to the analysis methods or safety engineering process are used as a basis to elaborate and formulate the BESEP requirement baseline requirements to support the upcoming benchmarking tasks.

The basis for the requirement elaboration is the IAEA high-level requirements identified in Task 2.1 and the national requirements that were selected by the BESEP partners in the beginning of the work of this Task 2.2. The selection of the national requirements was based on the partner judgement on the relevance to the project. The translations from the national languages are either done by the national authorities (publicly available) or by the project partners. The input requirements for each requirement topic are listed in Appendix B.

The national requirements are classified related to the requirement topics. In the classification work some of the original requirements were screened out as not relevant to the topics. The original requirements and the high-level IAEA requirements used as input for each requirement topic are shown in Appendix A. Based on the input requirements the final BESEP requirements for each requirement topic related to analysis types and safety engineering practices are elaborated. The BESEP requirement baseline related to the requirement topic in question is defined in a table in the sub-sections of this chapter. All BESEP requirement baseline requirements are collected in a table in Appendix A.

In the tables coding is used to make requirement identification easier. For the original national requirements the coding is as follows:

Country code, underscore (_), Requirement source, underscore, increasing three-digit number for unique coding. E.g. FI_B.1_010.

For the BESEP baseline requirements the coding is as follows:

Project identifier (BESEP), underscore, Analysis method identifier, underscore, requirement topic identifier, underscore, increasing three-digit number for unique coding. E.g. BESEP_DSA_PSEP_001.

The codes are listed in the table below.

Table 4.1 Codes used for requirement identification

Abbreviation/ Term	Description
A.3	Leadership and management for safety (Guide, Finland)
A.4	Organisation and personnel of a nuclear facility (Guide, Finland)
A.6	Conduct of operations at a nuclear power plant (Guide, Finland)
A.7	Probabilistic risk assessment and risk management of a nuclear power plant (Guide, Finland)
ALSF	Uncertainty analysis for accident sequences
B.1	Safety design of a nuclear power plant (Guide, Finland)
B.3	Deterministic safety analyses for a nuclear power plant (Guide, Finland)
B.7	Provisions for internal and external hazards at a nuclear facility (Guide, Finland)
BAL	Risk-informed management and balance of nuclear power plant design
BESEP	Identifier for the elaborated requirements for BESEP project
BN-JB-2.5	BN-JB-2.5 (Czech Republic)
CEE	Confidence provision for defence against the occurrence of cliff-edge effects
CM	System modification and configuration management
CZ	Identifier for original requirements from the Czech Republic

DCCF	Diversity and common-cause failure criteria
DID	Independence and strength of the individual defence-in-depth levels
DSA	Safety analysis method Deterministic safety analysis
EOP	Support for developing abnormal and emergency operating procedures and severe accident guidelines
FI	Identifier for original requirements from Finland
FISA	Flow of information between safety analyses
FSEP	Functional separation to provide defence against failure propagation
GS	Guidance selection, decision making and intelligent use of guidance
HFE	Safety analysis method Human factors engineering
HSI	Applicable HSI (Human System Interface)
HU	Identifier for original requirements from Hungary
IEF	Initiating event frequency estimation
JEA	Justification of the engineering assumptions used in analysis
JMT	Justification of the mission times used in analysis
MST	Validated modelling and simulation tools
NSC-118/2011	NSC - Governmental Decree No. 118/2011(VII.11.) (Hungary)
PSA	Safety analysis method Probabilistic Safety Analysis
PSEP	Physical separation and structural integrity
QSG	Quantitative safety goals/criteria
RED	Redundancy and single failure criteria
SAA	Situation awareness and assessment
SE	Identifier for original requirements from Sweden
SEM	Safety engineering management
SEP	Safety engineering practices
SDRM	Safety design and requirement management for external hazards
SK	Identifier for original requirements from the Slovak Republic
SM	Workload, stress and fatigue management
SSMFS-A	Strålsäkerhetsmyndighetens föreskrifter och allmänna råd om värdering och redovisning av strålsäkerhet för kärnkraftsreaktorer, Swedish regulation on radiation safety
SSMFS-K	Strålsäkerhetsmyndighetens föreskrifter om konstruktion av kärnkraftsreaktorer, Swedish regulation on construction
SUJB-162/2017	SUJB (Regulatory body) Decree 162/2017 (Czech Republic)
TW	Team working, effective communication and collaboration
UJDSR-106/2016	Decree of UJD SR (Nuclear Regulatory Authority of Slovak Republic) on nuclear safety requirements - 430/2011
UJDSR-430/2011	Decree of UJD SR (Nuclear Regulatory Authority of Slovak Republic) on nuclear safety requirements - 430/2011
UJDSR-BNS-I.4.2	PSA guideline of UJD SR, BNS I.4.2/2017 (Slovak Republic)
UNC	Uncertainty, sensitivity and importance analysis for accident sequences
VV	Verification and validation (V&V) of design
Y/1	Radiation and Nuclear Safety Authority Regulation on the Safety of a Nuclear Power Plant (Finland)

For the IAEA high-level requirements no specific coding is applied.

4.1 Deterministic Safety Analysis

4.1.1 Physical separation and structural integrity

The elaborated BESEP requirements related to physical separation and structural integrity are shown in the following table.

Table 4.2 BESEP requirements related to physical separation and structural integrity

BESEP id	BESEP requirement text
BESEP_DSA_PSEP_001	Redundant safety systems that have a role in mitigating the effects of external hazards shall be located so that these effects cannot hinder the performance of safety functions of all redundant components simultaneously.
BESEP_DSA_PSEP_002	The systems, structures and components, including auxiliary or supporting systems thereof shall be protected from the effects of external hazards as far as reasonably practicable.

4.1.2 Functional separation to provide defence against failure propagation

The elaborated BESEP requirements related to functional separation to provide defence against failure propagation are shown in the following table.

Table 4.3 BESEP requirements related to functional separation to provide defence against failure propagation

BESEP id	BESEP requirement text
BESEP_DSA_FSEP_001	The safety systems, structures and components, including auxiliary or supporting systems thereof, shall be protected from interaction with failed systems, structures or components as far as reasonably practicable.
BESEP_DSA_FSEP_002	The safety divisions hosting redundant parts of safety systems shall be located in different buildings or housed in dedicated compartments to separate them from the other safety divisions in the same building in order to prevent faults from spreading from one redundant system part to another as a result of external events.
BESEP_DSA_FSEP_003	The systems of different safety classes shall be functionally separated so that failure of a system or component of a lower safety class does not affect a function of a higher safety class.

4.1.3 Diversity and common-cause failure criteria

The elaborated BESEP requirements related to diversity and common-cause failure criteria are shown in the following table.

Table 4.4 BESEP requirements related to diversity and common-cause failure criteria

BESEP id	BESEP requirement text
BESEP_DSA_DCCF_001	Common-cause failures shall only have minor impacts on NPP safety.

BESEP_DSA_DCCF_002	Diversity shall be applied within and between defence-in-depth levels so that a common-cause failure of any individual component type shall not prevent managing the initiating event.

4.1.4 Redundancy and single failure criteria

The elaborated BESEP requirements related to redundancy and single failure criteria are shown in the following table.

Table 4.5 BESEP requirements related to redundancy and single failure criteria

BESEP id	BESEP requirement text
BESEP_DSA_RED_001	Systems performing a safety function designed against external hazards shall be operable even if a single failure of systems, structures or system components of the safety function is assumed.
BESEP_DSA_RED_002	The redundant parts of a system shall be protected from the effects of external hazards and from the interaction between the failed systems, structures and components.

4.1.5 Independence and strength of the individual defence-in-depth levels

The elaborated BESEP requirements related to independence and strength of the individual defence-in-depth levels are shown in the following table.

Table 4.6 BESEP requirements related to independence and strength of the individual defence-in-depth levels

BESEP id	BESEP requirement text
BESEP_DSA_DID_001	The defence-in-depth levels shall be functionally separated so that a failure on one level shall not prevent the implementation of necessary functions at other levels of defence.
BESEP_DSA_DID_002	Independence between the defence-in-depth levels shall be based on the adequate application of functional isolation, the diversity principle and physical separation.
BESEP_DSA_DID_003	The individual levels of defence-in-depth shall be capable for fulfilling their tasks without safety functions of the other levels.

4.1.6 Justification of the engineering assumptions used in analysis

The elaborated BESEP requirements related to justification of the engineering assumptions used in analysis are shown in the following table.

Table 4.7 BESEP requirements related to justification of the engineering assumptions used in analysis

BESEP id	BESEP requirement text
BESEP_ DSA_JEA_001	The engineering assumptions applied in conducting the deterministic safety analysis shall be appropriately justified.
BESEP_ DSA_JEA_002	When estimating the manual operation times, they shall be based on actual operational data and possible engineering assumptions shall be justified.

4.2 Probabilistic Safety Analysis

4.2.1 Risk-informed management and balance of nuclear power plant design

The elaborated BESEP requirements related to risk-informed management and balance of nuclear power plant design are shown in the following table.

Table 4.8 BESEP requirements related to risk-informed management and balance of nuclear power plant design

BESEP id	**BESEP requirement text**
BESEP_PSA_BAL_001	The PSA shall be applied in the NPP layout and systems design to assess the probability of hazards and event sequences affecting the safety of the NPP.
BESEP_PSA_BAL_002	PSA shall be used to confirm that the risk related to a single external hazard does not dominate the overall risk results.
BESEP_PSA_BAL_003	PSA shall realistically model the performance of the NPP based on relevant design data, procedures and guides including human interventions and potential human errors.
BESEP_PSA_BAL_004	The PSA shall be applied in the NPP layout and systems design to ensure the adequate reliability of safety functions fulfillment and the balance of the design.

4.2.2 Quantitative safety goals/criteria

The elaborated BESEP requirements related to quantitative safety goals/criteria are shown in the following table.

Table 4.9 BESEP requirements related to quantitative safety goals/criteria

BESEP id	**BESEP requirement text**
BESEP_PSA_QSG_001	Failure combinations induced by external hazards and leading to the damage of nuclear fuel assemblies shall be identified and their risk significance shall be evaluated.
BESEP_PSA_QSG_002	Failure combinations induced by external hazards and leading to the large release of radiological substances to the environment shall be identified and their risk significance shall be evaluated.
BESEP_PSA_QSG_003	The overall core damage frequency (CDF) target shall be met taking also external hazards into account.
BESEP_PSA_QSG_004	The overall large early release frequency (LERF) target shall be met taking also external hazards into account.

4.2.3 Initiating event frequency estimation

The elaborated BESEP requirements related to initiating event frequency estimation are shown in the following table.

Table 4.10 BESEP requirements related to initiating event frequency estimation

BESEP id	BESEP requirement text
BESEP_PSA_IEF_001	The occurrence frequency of initiating events shall be estimated, including those caused by external hazards.
BESEP_PSA_IEF_002	The site-specific analysis for external hazard shall be used in the estimation of initiating event frequencies.
BESEP_PSA_IEF_003	The results from long-term monitoring of the NPP site and the surroundings shall be taken into account in the initiating event frequency estimation for external hazards.
BESEP_PSA_IEF_004	For initiating event frequency estimation on rare external events having sparse or no operational data, the basis for the engineering judgements shall be given.

4.2.4 Assessment of potential losses of safety functions

The elaborated BESEP requirements related to assessment of potential losses of safety functions are shown in the following table.

Table 4.11 BESEP requirements related to assessment of potential losses of safety functions

BESEP id	BESEP requirement text
BESEP_PSA_ALSF_001	The potential losses of safety functions shall be evaluated based on the resilience of the NPP against the hazards, taking into consideration current status of all systems, structures and components relevant to nuclear safety.
BESEP_PSA_ALSF_002	Complex failure combinations of systems, structures and components initiated by external hazards shall be identified and their significance to nuclear safety shall be evaluated.
BESEP_PSA_ALSF_003	The important functional dependencies on physical location and from operation, maintenance and the effects of human activities shall be considered in assessing the potential losses of safety functions.

4.2.5 Uncertainty analysis of accident sequences and operating times

The elaborated BESEP requirements related to uncertainty analysis of accident sequences and operating times are shown in the following table.

Table 4.12 BESEP requirements related to uncertainty analysis of accident sequences and operating times

BESEP id	BESEP requirement text
BESEP_PSA_UNC_001	In the accident sequence analysis the performance of the NPP shall be realistically modelled and the appropriateness of the operating times assumed in the probabilistic safety analyses shall be demonstrated.
BESEP_PSA_UNC_002	Reliabilities of fulfilling success criteria involving human interventions shall be analysed using best estimate methods and relevant uncertainties and their effects shall be evaluated.
BESEP_PSA_UNC_003	For each type of hazard the design parameters forming the design input shall be specified on the basis of the hazard curve, taking into account the screening criterion applicable to the given hazard and if possible, the maximum, but still justified severity of the hazard shall be determined.

BESEP_PSA_UNC_004	In analyses regarding the definition of success criteria for systems and human interventions best estimate methods shall be used.
BESEP_PSA_UNC_005	Fragility curves generated from real damage data shall be used in assessing damage and loss during external events.

4.2.6 Confidence provision for defence against the occurrence of cliff-edge effects

The elaborated BESEP requirements related to confidence provision for defence against the occurrence of cliff-edge effects are shown in the following table.

Table 4.13 BESEP requirements related to confidence provision for defence against the occurrence of cliff-edge effects

BESEP id	**BESEP requirement text**
BESEP_PSA_CEE_001	Probabilistic safety analyses shall be used to demonstrate that sufficient safety margins are available to avoid cliff-edge effects
BESEP_PSA_CEE_002	Probabilistic safety analyses shall be used to identify potential areas of improvement in the design to ensure the avoidance of the cliff edge effects.

4.2.7 Support for developing abnormal and emergency operating procedures and severe accident guidelines

The elaborated BESEP requirements related to support for developing abnormal and emergency operating procedures and severe accident guidelines are shown in the following table.

Table 4.14 BESEP requirements related to support of developing abnormal, emergency operating and severe accident procedures

BESEP id	**BESEP requirement text**
BESEP_PSA_EOP_001	PSA shall be used to support the development of abnormal and , emergency operating procedures and severe accident guidelines considering aspects that may influence the activities and performance of operating personnel.
BESEP_PSA_EOP_002	PSA shall be used in determining the initiating events for which abnormal and emergency operating procedures and severe accident guidelines are developed.

4.3 Human Factors Engineering

4.3.1 Situation awareness and assessment

The elaborated BESEP requirements related to situation awareness and assessment are shown in the following table.

Table 4.15 BESEP requirements related to situation awareness and assessment

BESEP id	**BESEP requirement text**
BESEP_HFE_SAA_001	The design of user interfaces in NPP shall support the operators in assessing any normal and abnormal situation so that they can

	perceive the situation, comprehend it and finally anticipate the future status of the event.
BESEP_HFE_SAA_002	The visual monitors or operating panels shall provide the operators a holistic view on the plant state and feedback from the course of event and effects from activations and passive or automatic functions.
BESEP_HFE_SAA_003	Relevant information related to the procedures and guides shall be presented for the operators to assess the situation, to see the plant response to actions and to assess the progress of the plant state.

4.3.2 Guidance selection, decision making and intelligent use of guidance

The elaborated BESEP requirements related to guidance selection, decision making and intelligent use of guidance are shown in the following table.

Table 4.16 BESEP requirements related to guidance selection, decision making and intelligent use of guidance

BESEP id	**BESEP requirement text**
BESEP_HFE_GS_001	The procedures and guides designed for any event shall be easy to identify and select during the event.
BESEP_HFE_GS_002	The procedures and guides shall be designed to support the human performance in decision making.
BESEP_HFE_GS_003	The procedures and guides shall be designed taking into account the human capabilities and limitations and the human reliability analyses.
BESEP_HFE_GS_004	To support the high-quality implementation of work the use of procedures and guides shall be based on experience, routines and training for the tasks.

4.3.3 Applicable HSI (Human System Interface)

The elaborated BESEP requirements related to applicable HSI (Human System Interface) are shown in the following table.

Table 4.17 BESEP requirements related to applicable HSI (Human System Interface)

BESEP id	**BESEP requirement text**
BESEP_HFE_HSI_001	The HSI shall be adapted to human capabilities and limitations and it shall prevent the risk of incorrect action as much as possible.
BESEP_HFE_HSI_002	When alarms are used to notify operators of abnormal conditions the HSI shall present information that is relevant and clear and HSI shall prioritize the alarms based on their significance for the radiation safety.
BESEP_HFE_HSI_003	The number of different interfaces shall be as low as possible and reasonable.
BESEP_HFE_HSI_004	The user interface interaction and management shall be as fluent as possible to reduce workload.

4.3.4 Team working, effective communication and collaboration

The elaborated BESEP requirements related to team working, effective communication and collaboration are shown in the following table.

Table 4.18 BESEP requirements related to team working, effective communication and collaboration

BESEP id	BESEP requirement text
BESEP_HFE_TW_001	Effective communication and collaboration shall be enhanced through the control room design.
BESEP_HFE_TW_002	Team working shall be enhanced through procedures, guides and tools.

4.3.5 Workload, stress and fatigue management

The requirements in the following table have been elaborated related to workload, stress and fatigue management.

Table 4.19 BESEP requirements related to workload, stress and fatigue management

BESEP id	BESEP requirement text
BESEP_HFE_SM_001	To reduce the stress simulator-based training of stressful events shall be arranged.
BESEP_HFE_SM_002	Training that improves control room personnel communications skills shall be applied to reduce the likelihood that communications will fail under stress.
BESEP_HFE_SM_003	The procedures designed for abnormal and emergency conditions, power plant outages and start-up activities and SAMGs shall support operator work by reducing memory load and need for complex decision making.

4.4 Safety engineering practices

4.4.1 Safety engineering management

The elaborated BESEP requirements related to safety engineering management are shown in the following table.

Table 4.20 BESEP requirements related to safety engineering management.

BESEP id	BESEP requirement text
BESEP_SEP_SEM_001	There shall be a life cycle model of the nuclear plant to identify the relevant stages during the nuclear plant's lifetime, for example, Concept stage; Development stage; Implementation stage; Deployment stage; Operation and support stage; Retirement stage. The stages must not be iterative.
BESEP_SEP_SEM_002	There shall be a formal system with defined processes for ensuring the safety of the nuclear plant throughout its lifetime.
BESEP_SEP_SEM_003	The safety design process of the plant shall be accompanied by comprehensive and documented safety engineering processes to ensure that the design meets all the safety requirements throughout the lifetime of the nuclear power plant.
BESEP_SEP_SEM_004	An organisation model shall be established, addressing at least well-defined roles for human resources.

BESEP_SEP_SEM_005	An information model shall be established to manage the information items in a formal way, addressing relations and traceability between the information items.
BESEP_SEP_SEM_006	The safety engineering and safety engineering management tools shall be selected and validated to enhance safety, not to make it worse.

4.4.2 Safety design and requirement management for external hazards

The elaborated BESEP requirements related to adequate safety design and requirement management for external hazards.

Table 4.21 BESEP requirements related to safety design and requirement management for external hazards.

BESEP id	**BESEP requirement text**
BESEP_SEP_SDRM_001	There shall be formal practices for management of the safety design process of systems, structures and components so that all relevant safety requirements concerning external hazards have been taken into account in a way that they can be verified and validated.
BESEP_SEP_SDRM_002	All relevant external hazards shall be considered in the design as phenomena that are related to the site of a nuclear power plant and its surroundings and have an environmental origin.
BESEP_SEP_ SDRM _003	The design basis hazard factors shall be selected based on site-specific analysis. They shall be specified based on the hazard curve, taking into account the screening criterion applicable to the given hazard factor. The analysis shall be performed by deterministic methods, and based on the state-of-the-art results of science and technology by probabilistic methods.
BESEP_SEP_ SDRM _004	The dependencies affecting the simultaneous occurrence of external events shall be taken into account in selecting design values and in applying the redundancy and separation principles.
BESEP_SEP_ SDRM _005	The stability of and changes in external hazards affecting the nuclear safety of nuclear power plant units shall be forecasted for their whole lifetime.
BESEP_SEP_ SDRM _006	Realistic combinations of the individual events shall be considered during initiating event frequency estimation, including external and internal events, and they shall be selected by taking into account both engineering considerations and probabilistic analyses.
BESEP_SEP_ SDRM _007	The decision whether a given hazard of low probability is relevant for the nuclear safety of the power plant, shall be based on engineering judgement, for example using fragility curves.
BESEP_SEP_ SDRM _008	The fulfillment of specified safety functions, the suitability of the planned interventions of the NPP operator, the availability of selected other safety-relevant equipment shall be analysed related to external hazards.
BESEP_SEP_ SDRM _009	Appropriate tools, functions and procedures shall be designed to ensure the mitigation of the consequences of the initiating event occurred in addition to or due to an external hazard.
BESEP_SEP_ SDRM _010	The applicability of the standards selected for the design process shall be justified.

4.4.3 Flow of information between safety analyses

The elaborated BESEP requirements related to flow of information between safety analyses are shown in the following table.

Table 4.22 BESEP requirements related to flow of information between safety analysis

BESEP id	BESEP requirement text
BESEP_SEP_FISA_001	When several different types of safety analyses are used to provide evidence, the information flow between safety analyses shall be defined.
BESEP_SEP_FISA_002	The flow of information shall support reaching the comprehensive understanding on the issue analysed.

4.4.4 Verification and validation (V&V) of design

The elaborated BESEP requirements related to verification and validation (V&V) of design are shown in the following table.

Table 4.23 BESEP requirements related to verification and validation (V&V) of design

BESEP id	BESEP requirement text
BESEP_SEP_VV_001	V&V shall demonstrate that the included areas, spaces, systems, structures and components, manual tasks and organizational conditions are working together as designed and meet the safety requirements set to them.
BESEP_SEP_VV_002	It shall be possible to trace the decisions made based on the results of V&V to safety design and safety requirements.
BESEP_SEP_VV_003	The procedures and guidelines shall be systematically validated and verified. Validation shall also address the role of human factors in the procedures and the correct signal generation under the conditions of external hazards.
BESEP_SEP_VV_004	In the case of external hazards the NPP shall be safely shut down and kept in a subcritical state, the residual heat removal shall be ensured and the leakages of radioactive substances shall be kept below the specified limits.
BESEP_SEP_VV_005	The operability of systems, structures and components shall be demonstrated in their design basis external environmental conditions.

4.4.5 System modification and configuration management

The elaborated BESEP requirements related to system modification and configuration are shown in the following table.

Table 4.24 BESEP requirements related to system modification and configuration management

BESEP id	BESEP requirement text
BESEP_SEP_CM_001	Configuration management shall be applied also during system modifications.
BESEP_SEP_CM_002	The system modification shall be traceable to V&V results regarding its safety design and safety requirement it is set to fulfil.

4.4.6 Validated modelling and simulation analysis tools

The elaborated BESEP requirements related to validated modelling and simulation analysis tools are shown in the following table.

Table 4.25 BESEP requirements related to validated modelling and simulation analysis tools

BESEP id	**BESEP requirement text**
BESEP_SEP_MST_001	There shall be a description available of the used model to enable the validation of the model correctness in relation to the plant modelled.
BESEP_SEP_MST_002	The results gained with modelling and simulation analysis tools shall be collected to enable comparison to previous and following results gained with comparable models and tools.
BESEP_SEP_MST_003	The results gained with a physical model or computer code shall be compared to separate effects tests, tests carried out on entire systems, to disturbances occurred at NPPs or to results gained with other validated models.

5 Conclusion

This report summarizes the work performed within Task 2.2 of the BESEP project. In Task 2.2 the BESEP requirement baseline related to external hazards and their analysis was created.

The BESEP project benchmarks three analysis types: deterministic safety analysis (DSA), probabilistic safety analysis (PSA), and human factors engineering (HFE). In addition, the effectiveness of safety engineering practices (SEP) is also benchmarked. Safety requirement topics for these four concepts were defined during the work in Task 2.2 to support the baseline creation. The topics were based on the relevant IAEA high-level requirements identified in Task 2.1, on knowledge of the BESEP partners and on the preliminary case studies collected in the project proposal stage.

The original national requirements were collected by the BESEP partners to form the requirement base for the benchmarking. Only topics and requirements seen relevant for the project were selected.

The original national requirements and the IAEA high-level requirements identified in Task 2.1 were classified into the defined requirement topics. The classified requirements were then elaborated to form the BESEP requirements for each safety requirement topic. These requirements form the BESEP requirement baseline to be used in further BESEP project tasks.

REFERENCES

[1] BESEP project plan Benchmark Exercise on Safety Engineering Practices (BESEP). BESEP consortium, Helsinki, 2019.

[2] Finnish Nuclear Energy Act 990/1987, Helsinki, 1987 (amendment 2021). Available: https://www.stuklex.fi/fi/ls/19870990

[3] Finnish Nuclear Energy Decree 161/1988, Helsinki, 1988 (amendment 2021). Available: https://www.stuklex.fi/fi/ls/19880161

[4] Radiation and Nuclear Safety Authority Regulation on the Safety of a Nuclear Power Plant STUK Y/1/2018, Helsinki, 2018. Available: https://www.stuklex.fi/en/maarays/stuk-y-1-2018

[5] Leadership and management for safety YVL A.3, Radiation and Nuclear Safety Authority, Helsinki, 2019. Available: https://www.stuklex.fi/en/ohje/YVLA-3

[6] Organisation and personnel of a nuclear facility YVL A.4, Radiation and Nuclear Safety Authority, Helsinki, 2019. Available: https://www.stuklex.fi/en/ohje/YVLA-4

[7] Conduct of operations at a nuclear power plant YVL A.6, Radiation and Nuclear Safety Authority, Helsinki, 2019. Available: https://www.stuklex.fi/en/ohje/YVLA-6

[8] Probabilistic risk assessment and risk management of a nuclear power plant YVL A.7, Radiation and Nuclear Safety Authority, Helsinki, 2019. Available: https://www.stuklex.fi/en/ohje/YVLA-7

[9] Safety design of a nuclear power plant YVL B.1, Radiation and Nuclear Safety Authority, Helsinki, 2019. Available: https://www.stuklex.fi/en/ohje/YVLB-1

[10] Deterministic safety analyses for a nuclear power plant YVL B.3, Radiation and Nuclear Safety Authority, Helsinki, 2019. Available: https://www.stuklex.fi/en/ohje/YVLB-3

[11] Provisions for internal and external hazards at a nuclear facility YVL B.7 Radiation and Nuclear Safety Authority, Helsinki, 2019. Available: https://www.stuklex.fi/en/ohje/YVLB-7

[12] Decree 2007-1557 of 2 November 2007 concerning basic nuclear installations and the supervision of the transport of radioactive materials with respect to nuclear safety, Official Journal no. 255 Ministry for Ecology, Sustainable Development and Spatial Planning, 2007. Available : http://www.french-nuclear-safety.fr/content/download/85423/594459/Version/1/file/2007-1557-BNI.pdf

[13] Order of 7 February 2012 setting the general rules relative to basic nuclear installations, Official Journal of the French Republic, 2012. Available : http://www.french-nuclear-safety.fr/Media/Files/Order-of-7-February-2012-setting-the-general-rules-relative-to-basic-nuclear-installations

[14] Guide de l'ASN n°22 : Conception des réacteurs à eau sous pression, ASN & IRSN, 2017. Available (in French only): https://www.asn.fr/Professionnels/Installations-nucleaires/Guides-de-l-ASN/Guide-de-l-ASN-n-22-Conception-des-reacteurs-a-eau-sous-pression

[15] Laurent Guimier, "Regulatory Framework of France for NPPs", Regional Workshop on the Regulatory Framework for the Nuclear Power Plants, 27-31 October 2014, Tunisia.

[16] Act CXVI of 1996 on Atomic Energy, Budapest, 2018. Available: http://www.oah.hu/web/v3/HAEAportal.nsf/6755F068760E38FFC1257EB4003D79F5/$FILE/1996_116_tv_EN_2018_07_01.pdf

[17] Annex 7 to the Govt. Decree No. 118/2011 (VII. 11.) on the nuclear safety requirements of nuclear facilities and on related regulatory activities - Nuclear Safety Code, Volume 7, Site survey and assessment of nuclear facilities, HAEA (Hungarian Atomic Energy Authority), Budapest, 2018. Available: http://www.oah.hu/web/v3/HAEAportal.nsf/8EE55B54901CDD60C1257CDD004367CB/$FILE/118%202011%20Korm.%20Rendelet%20_7.%20k%C3%B6tet_EN_2018_04_10.pdf

[18] Annex 3A to the Govt. Decree No. 118/2011 (VII. 11.) on the nuclear safety requirements of nuclear facilities and on related regulatory activities - Nuclear Safety Code, Volume 3a, Design requirements for

new nuclear power plants, HAEA (Hungarian Atomic Energy Authority), Budapest, 2018. Available: http://www.oah.hu/web/v3/HAEAportal.nsf/05F9A474178B5B8CC1257E370029DCE1/$FILE/118%202011%20Korm.%20Rendelet%20_3A_kotet_2018_10_04.pdf

[19] Annex 3 to the Govt. Decree No. 118/2011 (VII. 11.) on the nuclear safety requirements of nuclear facilities and on related regulatory activities - Nuclear Safety Code, Volume 3, Design requirements for operating nuclear power plants, HAEA (Hungarian Atomic Energy Authority), Budapest, 2018. Available: http://www.oah.hu/web/v3/HAEAportal.nsf/B102BE513911C437C1257CA70048EB3F/$FILE/118%202011%20Korm.%20Rendelet%20_3.%20k%C3%B6tet_EN_2018_04_10.pdf

[20] Act no. 541/2004 Coll. on the Peaceful use of nuclear energy (Atomic Act). Available: www.ujd.gov.sk in Slovak only

[21] Decree of the Nuclear Regulatory Authority of the Slovak Republic No. 430/ 2011 Coll. As amended by Decree No. 103/2016 Coll. on nuclear safety requirements (consolidated version). Available: www.ujd.gov.sk in Slovak only

[22] Requirements for deterministic safety analyses of VVER440 type reactors, BN 5/2019, UJD SR, Bratislava, 2019. Available: www.ujd.gov.sk in Slovak only

[23] Requirements for PSA, BNS I.4.2/2017, UJD SR, Bratislava, 2017. Available: www.ujd.gov.sk in Slovak only

[24] Strålsäkerhetsmyndighetens föreskrifter och allmänna råd om värdering och redovisning av strålsäkerhet för kärnkraftsreaktorer (SSMFS-A), Strålsäkerhetsmyndigheten, Solna. Available: https://www.stralsakerhetsmyndigheten.se/contentassets/d0d409df7e044b3caf4a6c2af75e5f11/foreskrifter---formell-remiss-ssmfs-a.pdf

[25] Strålsäkerhetsmyndighetens föreskrifter om konstruktion av kärnkraftsreaktorer (SSMFS-K), Strålsäkerhetsmyndigheten, Solna. Available: https://www.stralsakerhetsmyndigheten.se/contentassets/d0d409df7e044b3caf4a6c2af75e5f11/foreskrifter---formell-remiss-ssmfs-k.pdf

[26] Strålsäkerhetsmyndighetens föreskrifter om drift av kärnkraftsreaktorer (SSMFS-D), Strålsäkerhetsmyndigheten, Solna. Available: https://www.stralsakerhetsmyndigheten.se/contentassets/d0d409df7e044b3caf4a6c2af75e5f11/foreskrifter---formell-remiss-ssmfs-d.pdf

[27] BESEP Deliverable 2.1: Assignment of safety requirement topics of selected external hazards, RELKO spol. s r.o, Bratislava, 2021. Available: https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5d9f2625f&appId=PPGMS

[28] Human Factors Engineering Program Review Model, NUREG-0711 (Revision 3), New York 2012. Available: https://www.nrc.gov/docs/ML1232/ML12324A013.pdf

APPENDIX A: BESEP REQUIREMENT BASELINE

All requirements elaborated in Chapter 4 are collected in the following Table A.1.

Table A.1 BESEP requirement baseline

BESEP id	**BESEP requirement text**
BESEP_DSA_PSEP_001	Redundant safety systems that have a role in mitigating the effects of external hazards shall be located so that these effects cannot hinder the performance of safety functions of all redundant components simultaneously.
BESEP_DSA_PSEP_002	The systems, structures and components, including auxiliary or supporting systems thereof shall be protected from the effects of external hazards as far as reasonably practicable.
BESEP_DSA_FSEP_001	The safety systems, structures and components, including auxiliary or supporting systems thereof, shall be protected from interaction with failed systems, structures or components as far as reasonably practicable.
BESEP_DSA_FSEP_002	The safety divisions hosting redundant parts of safety systems shall be located in different buildings or housed in dedicated compartments to separate them from the other safety divisions in the same building in order to prevent faults from spreading from one redundant system part to another as a result of external events.
BESEP_DSA_FSEP_003	The systems of different safety classes shall be functionally separated so that failure of a system or component of a lower safety class does not affect a function of a higher safety class.
BESEP_DSA_DCCF_001	Common-cause failures shall only have minor impacts on NPP safety.
BESEP_DSA_DCCF_002	Diversity shall be applied within and between defence-in-depth levels so that a common-cause failure of any individual component type shall not prevent managing the initiating event.
BESEP_DSA_RED_001	Systems performing a safety function designed against external hazards shall be operable even if a single failure of systems, structures or system components of the safety function is assumed.
BESEP_DSA_RED_002	The redundant parts of a system shall be protected from the effects of external hazards and from the interaction between the failed systems, structures and components.
BESEP_DSA_DID_001	The defence-in-depth levels shall be functionally separated so that a failure on one level shall not prevent the implementation of necessary functions at other levels of defence.
BESEP_DSA_DID_002	Independence between the defence-in-depth levels shall be based on the adequate application of functional isolation, the diversity principle and physical separation.
BESEP_DSA_DID_003	The individual levels of defence-in-depth shall be capable for fulfilling their tasks without safety functions of the other levels.
BESEP_ DSA_JEA_001	The engineering assumptions applied in conducting the deterministic safety analysis shall be appropriately justified.
BESEP_ DSA_JEA_002	When estimating the manual operation times, they shall be based on actual operational data and possible engineering assumptions shall be justified.

BESEP_PSA_BAL_001	The PSA shall be applied in the NPP layout and systems design to assess the probability of hazards and event sequences affecting the safety of the NPP.
BESEP_PSA_BAL_002	PSA shall be used to confirm that the risk related to a single external hazard does not dominate the overall risk results.
BESEP_PSA_BAL_003	PSA shall realistically model the performance of the NPP based on relevant design data, procedures and guides including human interventions and potential human errors.
BESEP_PSA_BAL_004	The PSA shall be applied in the NPP layout and systems design to ensure the adequate reliability of safety functions fulfillment and the balance of the design.
BESEP_PSA_QSG_001	Failure combinations induced by external hazards and leading to the damage of nuclear fuel assemblies shall be identified and their risk significance shall be evaluated.
BESEP_PSA_QSG_002	Failure combinations induced by external hazards and leading to the large release of radiological substances to the environment shall be identified and their risk significance shall be evaluated.
BESEP_PSA_QSG_003	The overall core damage frequency (CDF) target shall be met taking also external hazards into account.
BESEP_PSA_QSG_004	The overall large early release frequency (LERF) target shall be met taking also external hazards into account.
BESEP_PSA_IEF_001	The occurrence frequency of initiating events shall be estimated, including those caused by external hazards.
BESEP_PSA_IEF_002	The site-specific analysis for external hazard is used in the estimation of initiating event frequencies.
BESEP_PSA_IEF_003	The results from long-term monitoring of the NPP site and the surroundings shall be taken into account in the initiating event frequency estimation for external hazards.
BESEP_PSA_IEF_004	For initiating event frequency estimation on rare external events having sparse or no operational data, the basis for the engineering judgements shall be given.
BESEP_PSA_ALSF_001	The potential losses of safety functions shall be evaluated based on the resilience of the NPP against the hazards, taking into consideration current status of all systems, structures and components relevant to nuclear safety.
BESEP_PSA_ALSF_002	Complex failure combinations of systems, structures and components initiated by external hazards shall be identified and their significance to nuclear safety shall be evaluated.
BESEP_PSA_ALSF_003	The important functional dependencies on physical location and from operation, maintenance and the effects of human activities shall be considered in assessing the potential losses of safety functions.
BESEP_PSA_UNC_001	In the accident sequence analysis the performance of the NPP shall be realistically modelled and the appropriateness of the operating times assumed in the probabilistic safety analyses shall be demonstrated.
BESEP_PSA_UNC_002	Reliabilities of fulfilling success criteria involving human interventions shall be analysed using best estimate methods and relevant uncertainties and their effects shall be evaluated.
BESEP_PSA_UNC_003	For each type of hazard the design parameters forming the design input shall be specified on the basis of the hazard curve, taking into account the screening criterion applicable to the given hazard and if possible, the maximum, but still justified severity of the hazard shall be determined.

BESEP_PSA_UNC_004	In analyses regarding the definition of success criteria for systems and human interventions best estimate methods shall be used.
BESEP_PSA_UNC_005	Fragility curves generated from real damage data shall be used in assessing damage and loss during external events.
BESEP_PSA_CEE_001	Probabilistic safety analyses shall be used to demonstrate that sufficient safety margins are available to avoid cliff-edge effects
BESEP_PSA_CEE_002	Probabilistic safety analyses shall be used to identify potential areas of improvement in the design to ensure the avoidance of the cliff edge effects.
BESEP_PSA_EOP_001	PSA shall be used to support the development of abnormal and , emergency operating procedures and severe accident guidelines considering aspects that may influence the activities and performance of operating personnel.
BESEP_PSA_EOP_002	PSA shall be used in determining the initiating events for which abnormal and emergency operating procedures and severe accident guidelines are developed.
BESEP_HFE_SAA_001	The design of user interfaces in NPP shall support the operators in assessing any normal and abnormal situation so that they can perceive the situation, comprehend it and finally anticipate the future status of the event.
BESEP_HFE_SAA_002	The visual monitors or operating panels shall provide the operators a holistic view on the plant state and feedback from the course of event and effects from activations and passive or automatic functions.
BESEP_HFE_SAA_003	Relevant information related to the procedures and guides shall be presented for the operators to assess the situation, to see the plant response to actions and to assess the progress of the plant state.
BESEP_HFE_GS_001	The procedures and guides designed for any event shall be easy to identify and select during the event.
BESEP_HFE_GS_002	The procedures and guides shall be designed to support the human performance in decision making.
BESEP_HFE_GS_003	The procedures and guides shall be designed taking into account the human capabilities and limitations and the human reliability analyses.
BESEP_HFE_GS_004	To support the high-quality implementation of work the use of procedures and guides shall be based on experience, routines and training for the tasks.
BESEP_HFE_HSI_001	The HSI shall be adapted to human capabilities and limitations and it shall prevent the risk of incorrect action as much as possible.
BESEP_HFE_HSI_002	When alarms are used to notify operators of abnormal conditions the HSI shall present information that is relevant and clear and HSI shall prioritize the alarms based on their significance for the radiation safety.
BESEP_HFE_HSI_003	The number of different interfaces shall be as low as possible and reasonable.
BESEP_HFE_HSI_004	The user interface interaction and management shall be as fluent as possible to reduce workload.
BESEP_HFE_TW_001	Effective communication and collaboration shall be enhanced through the control room design.
BESEP_HFE_TW_002	Team working shall be enhanced through procedures, guides and tools.
BESEP_HFE_SM_001	To reduce the stress simulator-based training of stressful events shall be arranged.

BESEP_HFE_SM_002	Training that improves control room personnel communications skills shall be applied to reduce the likelihood that communications will fail under stress.
BESEP_HFE_SM_003	The procedures designed for abnormal and emergency conditions, power plant outages and start-up activities shall support operator work by reducing memory load and need for complex decision making.
BESEP_SEP_SEM_001	There shall be a life cycle model of the nuclear plant to identify the relevant stages during the nuclear plant's lifetime, for example, Concept stage; Development stage; Implementation stage; Deployment stage; Operation and support stage; Retirement stage. The stages must not be iterative.
BESEP_SEP_SEM_002	There shall be a formal system with defined processes for ensuring the safety of the nuclear plant throughout its lifetime.
BESEP_SEP_SEM_003	The safety design process of the plant shall be accompanied by comprehensive and documented safety engineering processes to ensure that the design meets all the safety requirements throughout the lifetime of the nuclear power plant.
BESEP_SEP_SEM_004	An organisation model shall be established, addressing at least well-defined roles for human resources.
BESEP_SEP_SEM_005	An information model shall be established to manage the information items in a formal way, addressing relations and traceability between the information items.
BESEP_SEP_SEM_006	The safety engineering and safety engineering management tools shall be selected and validated to enhance safety, not to make it worse.
BESEP_SEP_SDRM_001	There shall be formal practices for management of the safety design process of systems, structures and components so that all relevant safety requirements concerning external hazards have been taken into account in a way that they can be verified and validated.
BESEP_SEP_SDRM_002	All relevant external hazards shall be considered in the design as phenomena that are related to the site of a nuclear power plant and its surroundings and have an environmental origin.
BESEP_SEP_ SDRM _003	The design basis hazard factors shall be selected based on site-specific analysis. They shall be specified based on the hazard curve, taking into account the screening criterion applicable to the given hazard factor. The analysis shall be performed by deterministic methods, and based on the state-of-the-art results of science and technology by probabilistic methods.
BESEP_SEP_ SDRM _004	The dependencies affecting the simultaneous occurrence of external events shall be taken into account in selecting design values and in applying the redundancy and separation principles.
BESEP_SEP_ SDRM _005	The stability of and changes in external hazards affecting the nuclear safety of nuclear power plant units shall be forecasted for their whole lifetime.
BESEP_SEP_ SDRM _006	Realistic combinations of the individual events shall be considered during initiating event frequency estimation, including external and internal events, and they shall be selected by taking into account both engineering considerations and probabilistic analyses.
BESEP_SEP_ SDRM _007	The decision whether a given hazard of low probability is relevant for the nuclear safety of the power plant, shall be based on engineering judgement, for example using fragility curves.
BESEP_SEP_ SDRM _008	The fulfillment of specified safety functions, the suitability of the planned interventions of the NPP operator, the availability of selected other safety-relevant equipment shall be analysed related to external hazards.

BESEP_SEP_ SDRM _009	Appropriate tools, functions and procedures shall be designed to ensure the mitigation of the consequences of the initiating event occurred in addition to or due to an external hazard.
BESEP_SEP_ SDRM _010	The applicability of the standards selected for the design process shall be justified.
BESEP_SEP_FISA_001	When several different types of safety analyses are used to provide evidence, the information flow between safety analyses shall be defined.
BESEP_SEP_FISA_002	The flow of information shall support reaching the comprehensive understanding on the issue analysed.
BESEP_SEP_VV_001	V&V shall demonstrate that the included areas, spaces, systems, structures and components, manual tasks and organizational conditions are working together as designed and meet the safety requirements set to them.
BESEP_SEP_VV_002	It shall be possible to trace the decisions made based on the results of V&V to safety design and safety requirements.
BESEP_SEP_VV_003	The procedures and guidelines shall be systematically validated and verified. Validation shall also address the role of human factors in the procedures and the correct signal generation under the conditions of external hazards.
BESEP_SEP_VV_004	In the case of external hazards the NPP shall be safely shut down and kept in a subcritical state, the residual heat removal shall be ensured and the leakages of radioactive substances shall be kept below the specified limits.
BESEP_SEP_VV_005	The operability of systems, structures and components shall be demonstrated in their design basis external environmental conditions.
BESEP_SEP_CM_001	Configuration management shall be applied also during system modifications.
BESEP_SEP_CM_002	The system modification shall be traceable to V&V results regarding its safety design and safety requirement it is set to fulfil.
BESEP_SEP_MST_001	There shall be a description available of the used model to enable the validation of the model correctness in relation to the plant modelled.
BESEP_SEP_MST_002	The results gained with modelling and simulation analysis tools shall be collected to enable comparison to previous and following results gained with comparable models and tools.
BESEP_SEP_MST_003	The results gained with a physical model or computer code shall be compared to separate effects tests, tests carried out on entire systems, to disturbances occurred at NPPs or to results gained with other validated models.

APPENDIX B: INPUT REQUIREMENTS FOR BESEP REQUIREMENT BASELINE (THE REQUIREMENT BASE)

In this section the input requirements, i.e. the IAEA high-level requirements and the original national requirements are linked to the requirement topics. The sub-sections have corresponding headers as in Chapter 4.

B.1 Deterministic Safety Analysis

B.1.1 Physical separation and structural integrity

The IAEA high-level requirements related to physical separation and structural integrity are shown in the following table.

Table B.1 IAEA high-level requirements related to physical separation and structural integrity

IAEA requirement	**IAEA Requirement text**
Requirement 16: Postulated initiating events	Requirement 16: Postulated initiating events. The design for the nuclear power plant shall apply a systematic approach to identifying a comprehensive set of postulated initiating events such that all foreseeable events with the potential for serious consequences and all foreseeable events with a significant frequency of occurrence are anticipated and are considered in the design. The postulated initiating events shall be identified on the basis of engineering judgement and a combination of deterministic assessment and probabilistic assessment. A justification of the extent of usage of deterministic safety analysis and probabilistic safety analysis shall be provided to show that all foreseeable events have been considered.
Requirement 21: Physical separation and independence of safety systems	Requirement 21: Physical separation and independence of safety systems. Interference between safety systems or between redundant elements of a system shall be prevented by means such as physical separation, electrical isolation, functional independence and independence of communication (data transfer), as appropriate.
Requirement 24: Common cause failures	Requirement 24: Common cause failures. The design of equipment shall take due account of the potential for common cause failures of items important to safety, to determine how the concepts of diversity, redundancy, physical separation and functional independence have to be applied to achieve the necessary reliability.
Requirement 40: Prevention of harmful interactions of systems important to safety	Requirement 40: Prevention of harmful interactions of systems important to safety. The potential for harmful interactions of systems important to safety at the nuclear power plant that might be required to operate simultaneously shall be evaluated, and effects of any harmful interactions shall be prevented. In the analysis of the potential for harmful interactions of systems important to safety, due account shall be taken of physical interconnections and of the possible effects of one system's operation, maloperation or malfunction on local environmental conditions of other essential systems, to ensure that changes in environmental conditions do not affect the reliability of systems or components in functioning as intended. If two fluid systems important to safety are interconnected and are operating at different pressures, either the systems shall both be designed to withstand the higher pressure, or provision shall be made to prevent the design pressure of the system operating at the lower pressure from being exceeded.

The original national requirements related to physical separation and structural integrity are shown in the following table.

Table B.2 National requirements related to physical separation and structural integrity

BESEP id	**Original requirement text**
CZ_BN-JB-2.5_005	Confirmation of sufficient separation among safety related components, systems and structures endangered by the hazards as fires or floods belongs to the elements of risk oriented decision making employing importance measures enumerated by PSA model.
HU_NSC-118/2011_001	During design of a nuclear power plant, in accordance with the defence in-depth principle: a) it shall be ensured by design solutions that the fundamental safety functions are performed by means of the safety barriers or mitigating the consequences of any abnormal operation or deviation. b) systems providing safety functions shall be applied to prevent or manage DBC2-4 and DEC1-2 and; c) the design of the barriers shall be conservative, their implementation shall be of the highest standards to ensure: ca) the probability of failures and deviations from normal operating conditions shall be as low as reasonably achievable, cb) DBC4 and DEC plant states shall be prevented to a reasonably achievable level, furthermore cc) no cliff edge effect can arise; d) the manageability of the condition of the nuclear power plant shall be ensured by technical means in such a way that in the event of a failure or deviation from normal operating conditions the necessity to operate the systems providing safety functions shall be as limited as possible; e) the control of nuclear power plant conditions shall be highly reliable even under conditions requiring the operation of the systems that provide safety functions, and shall not require human intervention in the preliminary phase of the process.
HU_NSC-118/2011_022	The safety systems, structures, components, and their auxiliary systems shall be protected as much as possible from the effects of internal and external hazard factors, and from the interaction between the failed systems, structure and system components.
HU_NSC-118/2011_023	The redundant safety class systems, influencing the management of the effects of external and internal hazard factors shall be placed so that the effect cannot hinder the performance of safety functions of all redundant components simultaneously.
HU_NSC-118/2011_024	The nuclear power plant shall be designed in such a way that the fundamental safety functions are also performed in the event of a safety earthquake, and that the nuclear power plant can reach controlled, safe shutdown conditions following the earthquake even if a single failure of systems, structures and system components is assumed.

BESEP id	Original requirement text
HU_NSC-118/2011_025	The systems, structures and system components performing safety functions and participating in the implementation of earthquake protection shall be designed and qualified in such a way that they shall maintain their required operability and function in the event of a safety earthquake. The design and qualification shall be performed in accordance with the safety class and the nuclear standards and testing procedures.
FI_B.1_010	437. The safety divisions hosting redundant parts of safety systems shall be located in different buildings or housed in dedicated compartments to separate them from the other safety divisions in the same building in order to prevent faults from spreading from one redundant system part to another as a result of internal events (e.g. fire, flood or dynamic effects) or external events.
FI_B.1_011	438. The requirement for the separation of redundant system parts also applies to all auxiliary systems of systems necessary for performing a safety function and to all I&C systems controlling the safety function, from the measurement indicating a need to actuate the system up to the equipment performing the safety function.
FI_B.7_001	321. The technical requirements to be set for structures between safety divisions and other separating structures as well as for separation by distance shall be determined on the basis of the internal or external hazards examined as well as the Finnish Building Code RakMK and applicable standards.
FI_B.7_002	326. Systems and fire loads in the safety divisions and in rooms adjacent to them and a fire considered possible in the said rooms, the release of poisonous gases, flooding and the related hydrostatic pressure, as well as other internal or external hazards considered possible shall be taken into account in the design of the separation of the safety divisions, separating structures and the boundary between a safety division and other rooms or outside areas.

B.1.2 Functional separation to provide defence against failure propagation

The IAEA high-level requirements related to functional separation to provide defence against failure propagation are shown in the following table.

Table B.3 IAEA high-level requirements related to functional separation to provide defence against failure propagation

IAEA requirement	IAEA Requirement text
Requirement 16: Postulated initiating events	Requirement 16: Postulated initiating events. The design for the nuclear power plant shall apply a systematic approach to identifying a comprehensive set of postulated initiating events such that all foreseeable events with the potential for serious consequences and all foreseeable events with a significant frequency of occurrence are anticipated and are considered in the design. The postulated initiating events shall be identified on the basis of engineering judgement and a combination of deterministic assessment and probabilistic assessment. A justification of the extent of usage of deterministic safety analysis

IAEA requirement	IAEA Requirement text
	and probabilistic safety analysis shall be provided to show that all foreseeable events have been considered.
Requirement 21: Physical separation and independence of safety systems	Requirement 21: Physical separation and independence of safety systems. Interference between safety systems or between redundant elements of a system shall be prevented by means such as physical separation, electrical isolation, functional independence and independence of communication (data transfer), as appropriate.
Requirement 24: Common cause failures	Requirement 24: Common cause failures. The design of equipment shall take due account of the potential for common cause failures of items important to safety, to determine how the concepts of diversity, redundancy, physical separation and functional independence have to be applied to achieve the necessary reliability.
Requirement 40: Prevention of harmful interactions of systems important to safety	Requirement 40: Prevention of harmful interactions of systems important to safety. The potential for harmful interactions of systems important to safety at the nuclear power plant that might be required to operate simultaneously shall be evaluated, and effects of any harmful interactions shall be prevented. In the analysis of the potential for harmful interactions of systems important to safety, due account shall be taken of physical interconnections and of the possible effects of one system's operation, maloperation or malfunction on local environmental conditions of other essential systems, to ensure that changes in environmental conditions do not affect the reliability of systems or components in functioning as intended. If two fluid systems important to safety are interconnected and are operating at different pressures, either the systems shall both be designed to withstand the higher pressure, or provision shall be made to prevent the design pressure of the system operating at the lower pressure from being exceeded.
Requirement 41: Interactions between the electric grid and the plant	Requirement 41: Interactions between the electrical power grid and the plant. The functionality of items important to safety at the nuclear power plant shall not be compromised by disturbances in the electrical power grid, including anticipated variations in the voltage and frequency of the grid supply.

The original national requirements related to functional separation to provide defence against failure propagation are shown in the following table.

Table B.4 National requirements related to functional separation to provide defence against failure propagation

BESEP id	Original requirement text
HU_NSC-118/2011_022	The safety systems, structures, components, and their auxiliary systems shall be protected as much as possible from the effects of internal and external hazard factors, and from the interaction between the failed systems, structure and system components.
FI_B.1_006	429. The systems required for implementing different levels of defence according to the defence-in-depth principle shall be functionally isolated from one another, in such a way that a failure on one level shall not prevent the implementation of necessary functions at other levels of defence.

BESEP id	Original requirement text
FI_B.1_009	435. The failure of a subsystem in a system executing safety functions shall not cause the failure of another redundant subsystem of the same system or the failure of several subsystems participating in the same safety function.
FI_B.1_010	437. The safety divisions hosting redundant parts of safety systems shall be located in different buildings or housed in dedicated compartments to separate them from the other safety divisions in the same building in order to prevent faults from spreading from one redundant system part to another as a result of internal events (e.g. fire, flood or dynamic effects) or external events.
FI_B.1_012	440. Systems and components assigned to different safety classes shall be functionally isolated from one another to ensure that the mode of operation or a failure of a system or component of a lower safety class does not result in the malfunction or loss of function of a system of a higher safety class.

B.1.3 Diversity and common-cause failure criteria

The IAEA high-level requirements related to diversity and common-cause failure criteria are shown in the following table.

Table B.5 IAEA high-level requirements related to diversity and common-cause failure criteria

IAEA requirement	IAEA Requirement text
Requirement 21: Physical separation and independence of safety systems	Requirement 21: Physical separation and independence of safety systems. Interference between safety systems or between redundant elements of a system shall be prevented by means such as physical separation, electrical isolation, functional independence and independence of communication (data transfer), as appropriate.
Requirement 24: Common cause failures	Requirement 24: Common cause failures. The design of equipment shall take due account of the potential for common cause failures of items important to safety, to determine how the concepts of diversity, redundancy, physical separation and functional independence have to be applied to achieve the necessary reliability.
Requirement 62: Reliability and testability of instrumentation and control systems	Requirement 62: Reliability and testability of instrumentation and control systems. Instrumentation and control systems for items important to safety at the nuclear power plant shall be designed for high functional reliability and periodic testability commensurate with the safety functions to be performed. Design techniques such as testability, including a self-checking capability where necessary, fail-safe characteristics, functional diversity and diversity in component design and in concepts of operation shall be used to the extent practicable to prevent the loss of a safety function.
Requirement 63: Use of computer-based equipment in systems important to safety	Requirement 63: Use of computer based equipment in systems important to safety. If a system important to safety at the nuclear power plant is dependent upon computer based equipment, appropriate standards and practices for the development and testing of computer hardware and software shall be established and implemented throughout the service life of the system, and in particular throughout the software development cycle. The entire development shall be

IAEA requirement	IAEA Requirement text
	subject to a quality management system. For computer based equipment in safety systems or safety related systems: • A high quality of, and best practices for, hardware and software shall be used, in accordance with the importance of the system to safety. • The entire development process, including control, testing and commissioning of design changes, shall be systematically documented and shall be reviewable. • An assessment of the equipment shall be undertaken by experts who are independent of the design team and the supplier team to provide assurance of its high reliability. • Where safety functions are essential for achieving and maintaining safe conditions, and the necessary high reliability of the equipment cannot be demonstrated with a high level of confidence, diverse means of ensuring fulfilment of the safety functions shall be provided. • Common cause failures deriving from software shall be taken into consideration. • Protection shall be provided against accidental disruption of, or deliberate interference with, system operation.

The original national requirements related to diversity and common-cause failure criteria are shown in the following table.

Table B.6 National requirements related to diversity and common-cause failure criteria

BESEP id	Original requirement text
HU_NSC-118/2011_010	In the case of a nuclear power plant having more than one unit, the possibility of the common cause failure of safety systems commonly applied by the units shall be examined during the design.
FI_Y/1_003	5. Common cause failures shall only have minor impacts on nuclear power plant safety.
FI_B.1_004	421c. A common cause failure of any individual component type (for example, a similar check valve, same type and manufacturer) shall not prevent the nuclear power plant from being brought to a controlled state or a safe state.

B.1.4 Redundancy and single failure criteria

The IAEA high-level requirements related to redundancy and single failure criteria are shown in the following table.

Table B.7 IAEA high-level requirements related to redundancy and single failure criteria

IAEA requirement	IAEA Requirement text
Requirement 21: Physical separation and independence of safety systems	Requirement 21: Physical separation and independence of safety systems. Interference between safety systems or between redundant elements of a system shall be prevented by means such as physical separation, electrical isolation, functional independence and independence of communication (data transfer), as appropriate.
Requirement 24: Common cause failures	Requirement 24: Common cause failures. The design of equipment shall take due account of the potential for common cause failures of items important to safety, to determine how the concepts of diversity,

IAEA requirement	IAEA Requirement text
	redundancy, physical separation and functional independence have to be applied to achieve the necessary reliability.
Requirement 25: Single failure criterion	Requirement 25: Single failure criterion. The single failure criterion shall be applied to each safety group incorporated in the plant design.

The original national requirements related to redundancy and single failure criteria are shown are shown in the following table.

Table B.8 National requirements related to redundancy and single failure criteria

BESEP id	Original requirement text
HU_NSC-118/2011_001	During design of a nuclear power plant, in accordance with the defence in-depth principle: a) it shall be ensured by design solutions that the fundamental safety functions are performed by means of the safety barriers or mitigating the consequences of any abnormal operation or deviation. b) systems providing safety functions shall be applied to prevent or manage DBC2-4 and DEC1-2 and; c) the design of the barriers shall be conservative, their implementation shall be of the highest standards to ensure: ca) the probability of failures and deviations from normal operating conditions shall be as low as reasonably achievable, cb) DBC4 and DEC plant states shall be prevented to a reasonably achievable level, furthermore cc) no cliff edge effect can arise; d) the manageability of the condition of the nuclear power plant shall be ensured by technical means in such a way that in the event of a failure or deviation from normal operating conditions the necessity to operate the systems providing safety functions shall be as limited as possible; e) the control of nuclear power plant conditions shall be highly reliable even under conditions requiring the operation of the systems that provide safety functions, and shall not require human intervention in the preliminary phase of the process.
HU_NSC-118/2011_022	The safety systems, structures, components, and their auxiliary systems shall be protected as much as possible from the effects of internal and external hazard factors, and from the interaction between the failed systems, structure and system components.
HU_NSC-118/2011_024	The nuclear power plant shall be designed in such a way that the fundamental safety functions are also performed in the event of a safety earthquake, and that the nuclear power plant can reach controlled, safe shutdown conditions following the earthquake even if a single failure of systems, structures and system components is assumed.
FI_B.1_007	433. Provisions shall be made for failures by ensuring that systems performing a safety function consist of two or more redundant systems or system parts in parallel, so that the safety function can be performed even if any of them is rendered inoperable.
FI_B.1_008	434. The redundant parts of a system performing safety functions shall be assigned to different safety divisions.

B.1.5 Independence and strength of the individual defence-in-depth levels

The IAEA high-level requirements related to independence and strength of the individual defence-in-depth levels are shown in the following table.

Table B.9 IAEA high-level requirements related to independence and strength of the individual defence-in-depth levels

IAEA requirement	**IAEA Requirement text**
Requirement 7: Application of defence in depth	Requirement 7: Application of defence in depth. The design of a nuclear power plant shall incorporate defence in depth. The levels of defence in depth shall be independent as far as is practicable.

The original national requirements related to independence and strength of the individual defence-in-depth levels are shown in the following table.

Table B.10 National requirements related to independence and strength of the individual defence-in-depth levels

BESEP id	**Original requirement text**
FI_B.1_005	426. Independence between the levels of defence shall be based on the adequate application of functional isolation, the diversity principle and physical separation.
FI_B.1_007	433. Provisions shall be made for failures by ensuring that systems performing a safety function consist of two or more redundant systems or system parts in parallel, so that the safety function can be performed even if any of them is rendered inoperable.
FI_B.1_008	434. The redundant parts of a system performing safety functions shall be assigned to different safety divisions.
FI_B.1_009	435. The failure of a subsystem in a system executing safety functions shall not cause the failure of another redundant subsystem of the same system or the failure of several subsystems participating in the same safety function.
FI_B.1_010	437. The safety divisions hosting redundant parts of safety systems shall be located in different buildings or housed in dedicated compartments to separate them from the other safety divisions in the same building in order to prevent faults from spreading from one redundant system part to another as a result of internal events (e.g. fire, flood or dynamic effects) or external events.
FI_B.1_011	438. The requirement for the separation of redundant system parts also applies to all auxiliary systems of systems necessary for performing a safety function and to all I&C systems controlling the safety function, from the measurement indicating a need to actuate the system up to the equipment performing the safety function.
FI_B.1_012	440. Systems and components assigned to different safety classes shall be functionally isolated from one another to ensure that the mode of operation or a failure of a system or component of a lower safety class does not result in the malfunction or loss of function of a system of a higher safety class.
FI_B.1_013	442a. The consequences caused by an initiating event to the systems needed to execute safety functions shall be identified. The failure criterion shall be applied in addition to any consequential failures possibly caused by the initiating event.

B.1.6 Justification of the engineering assumptions used in analysis

The IAEA high-level requirements related to justification of the engineering assumptions used in analysis are shown in the following table.

Table B.11 IAEA high-level requirements related to justification of the engineering assumptions used in analysis

IAEA requirement	**IAEA Requirement text**
Requirement 42: Safety analysis of the plant design	Requirement 42: Safety analysis of the plant design. A safety analysis of the design for the nuclear power plant shall be conducted in which methods of both deterministic analysis and probabilistic analysis shall be applied to enable the challenges to safety in the various categories of plant states to be evaluated and assessed. On the basis of a safety analysis, the design basis for items important to safety and their links to initiating events and event sequences shall be confirmed. It shall be demonstrated that the nuclear power plant as designed is capable of complying with authorized limits on discharges with regard to radioactive releases and with the dose limits in all operational states, and is capable of meeting acceptable limits for accident conditions. The safety analysis shall provide assurance that defence in depth has been implemented in the design of the plant. The safety analysis shall provide assurance that uncertainties have been given adequate consideration in the design of the plant and in particular that adequate margins are available to avoid cliff edge effects and early radioactive releases or large radioactive releases. The applicability of the analytical assumptions, methods and degree of conservatism used in the design of the plant shall be updated and verified for the current or as built design. The deterministic safety analysis shall mainly provide: • Establishment and confirmation of the design bases for all items important to safety; • Characterization of the postulated initiating events that are appropriate for the site and the design of the plant; • Analysis and evaluation of event sequences that result from postulated initiating events, to confirm the qualification requirements; • Comparison of the results of the analysis with acceptance criteria, design limits, dose limits and acceptable limits for purposes of radiation protection; • Demonstration that the management of anticipated operational occurrences and design basis accidents is possible by safety actions for the automatic actuation of safety systems in combination with prescribed actions by the operator; • Demonstration that the management of design extension conditions is possible by the automatic actuation of safety systems and the use of safety features in combination with expected actions by the operator. The probabilistic safety analysis of the plant is performed for all modes of operation and for all plant states, including shutdown, with particular reference to: • Establishing that a balanced design has been achieved such that no particular feature or postulated initiating event makes a

IAEA requirement	IAEA Requirement text
	disproportionately large or significantly uncertain contribution to the overall risks, and that, to the extent practicable, the levels of defence in depth are independent; • Providing assurance that situations in which small deviations in plant parameters could give rise to large variations in plant conditions (cliff edge effects) will be prevented; • Comparing the results of the analysis with the acceptance criteria for risk where these have been specified.

The original national requirements related to justification of the engineering assumptions used in analysis are shown in the following table.

Table B.12 National requirements related to justification of the engineering assumptions used in analysis

BESEP id	Original requirement text
SK_UJDSR-106/2016_003	(2) The permit holder shall review it by periodic evaluation b) determination of the characteristics of probable internal hazards and external hazards to the nuclear power plant, including analytical methods, models, assumptions, criteria and data used for their determination,

B.2 Probabilistic Safety Analysis

B.2.1 Risk-informed management and balance of nuclear power plant design

The IAEA high-level requirements related to risk-informed management and balance of nuclear power plant design are shown in the following table.

Table B.13 IAEA high-level requirements related to risk-informed management and balance of nuclear power plant design

IAEA requirement	IAEA Requirement text
Requirement 17: Internal and external hazards	Requirement 17: Internal and external hazards. All foreseeable internal hazards and external hazards, including the potential for human induced events directly or indirectly to affect the safety of the nuclear power plant, shall be identified and their effects shall be evaluated. […] External hazards: The design shall include due consideration of those natural and human induced external events (i.e., events of origin external to the plant) that have been identified in the site evaluation process. Causation and likelihood shall be considered in postulating potential hazards. […] The design of the plant shall provide for an adequate margin to protect items important to safety against levels of external hazards to be considered for design, derived from the hazard evaluation for the site, and to avoid cliff edge effects. A cliff edge effect, in a nuclear power plant, is an instance of severely abnormal plant behaviour caused by an abrupt transition from one plant status to another following a small deviation in a plant parameter, and thus a sudden large variation in plant conditions in response to a small variation in an input. [...]

IAEA requirement	IAEA Requirement text
Requirement 42: Safety analysis of the plant design	Requirement 42: Safety analysis of the plant design. A safety analysis of the design for the nuclear power plant shall be conducted in which methods of both deterministic analysis and probabilistic analysis shall be applied to enable the challenges to safety in the various categories of plant states to be evaluated and assessed. […] The safety analysis shall provide assurance that uncertainties have been given adequate consideration in the design of the plant and in particular that adequate margins are available to avoid cliff edge effects and early radioactive releases or large radioactive releases. The applicability of the analytical assumptions, methods and degree of conservatism used in the design of the plant shall be updated and verified for the current or as built design. […] The probabilistic safety analysis of the plant is performed for all modes of operation and for all plant states, including shutdown, with particular reference to: • Establishing that a balanced design has been achieved such that no particular feature or postulated initiating event makes a disproportionately large or significantly uncertain contribution to the overall risks, and that, to the extent practicable, the levels of defence in depth are independent; • Providing assurance that situations in which small deviations in plant parameters could give rise to large variations in plant conditions (cliff edge effects) will be prevented; • Comparing the results of the analysis with the acceptance criteria for risk where these have been specified.
Requirement 65: Control room	Requirement 65: Control room. […] Special attention shall be paid to identifying those events, both internal and external to the control room, that could challenge its continued operation, and the design shall provide for reasonably practicable measures to minimize the consequences of such events. The design of the control room shall provide an adequate margin against levels of natural hazards more severe than those considered for design, derived from the hazard evaluation for the site.
Requirement 66: Supplementary control room	Requirement 66: Supplementary control room. Instrumentation and control equipment shall be kept available, preferably at a single location (a supplementary control room) that is physically, electrically and functionally separate from the control room at the nuclear power plant. […]

The original national requirements related to risk-informed management and balance of nuclear power plant design are shown in the following table.

Table B.14 National requirements related to risk-informed management and balance of nuclear power plant design

BESEP id	Original requirement text
CZ_SUJB-162/2017_001	Probabilistic safety assessment has to address initiating events caused by both internal and external hazards, including hazards impacting large areas of NPP site.
CZ_SUJB-162/2017_002	When the PSA model is developed, the time window covered by modeling plant response to initiating event caused by internal and/or external hazards has to be justified.
CZ_SUJB-162/2017_003	The PSA documentation has to include detailed description of Level-1 and Level-2 aspects of PSA for all individual internal and external hazards.
CZ_SUJB-162/2017_004	Periodic safety assessment has to evaluate internal and external hazards from point of view of adequacy of existing resistance of NPP against the hazards, taking into consideration real status of all components, systems and structures impacting nuclear safety and the up-to-date values of probability of occurrence of hazard scenarios obtained from up-date of plant site data, where the NPP is operated. Possible impacts of climate change and changes of human related activities (transport and other industrial activities in plant vicinity), as well as newly adopted measures determined for prevention and mitigation of hazards effects, which are based on defence-in-depth principles, have to be considered.
CZ_BN-JB-2.5_003	It is required for broad PSA applications that Level-1 and Level-2 PSA model for both full power and shutdown is available, which covers full spectrum of possible IEs, including those caused by hazards.
CZ_BN-JB-2.5_004	Level-1 and Level-2 PSA model for both full power and shutdown should be available, which covers full spectrum of possible IEs, including those caused by hazards, when verification that the plant fulfills safety targets and criteria is carried out, with the exception when the safety targets/criteria are defined for the matters covered by reduced scope of PSA, or when alternative approaches are used to confirm that the risk related to the hazards is negligible from point of view of the safety targets and criteria under concern.
CZ_BN-JB-2.5_005	Confirmation of sufficient separation among safety related components, systems and structures endangered by the hazards as fires or floods belongs to the elements of risk oriented decision making employing importance measures enumerated by PSA model.
CZ_BN-JB-2.5_006	The examples of attributes used in definition of plant damage states include failure of containment structure, radioactive release from containment as well as failure of additional barriers (reactor building, other adjacent structures), where the analysis include also all external events, which can damage the structures under concern.
CZ_BN-JB-2.5_007	When the Level-2 PSA scope is extended by including hazards, the impact of the hazards included on plant systems used in severe accidents mitigation and the impact on containment integrity has to be addressed.
HU_NSC-118/2011_015	For the design of a nuclear power plant unit, including the systems for storage and manage spent fuel, level 1 and level 2 probabilistic safety analysis shall be developed, which considers all possible operating conditions, system configurations and all of the postulated initiating events for which it cannot be demonstrated by any other method that their contribution to the risk is insignificant. In the level 1 and 2 probabilistic safety analyses, considering the state-of-the-art results of science and technology, the external hazards shall be taken into account. Where it is not possible, proven alternative analysis solutions

BESEP id	Original requirement text
	shall be used to assess the contribution of the external hazard factors to the overall risk represented by the nuclear power plant.
HU_NSC-118/2011_016	In the probabilistic safety analysis important functional, territorial dependencies, dependencies of physical situation of system components, dependencies from operation, maintenance and other common cause failures, especially missiles, effects of liquid and steam jets, internal fire and floods, as well as the accidents of nearby industrial facilities and the effects of human activities shall be considered.
HU_NSC-118/2011_017	The probabilistic safety analysis shall realistically model the performance of the nuclear power plant, for which the relevant design data, operational and accident-related instructions, accident management guidelines or drafts shall be considered, including human interventions and potential human errors. The appropriateness of the operating times assumed in the probabilistic safety analyses shall be demonstrated.
HU_NSC-118/2011_019	In analyses regarding the definition of success criteria for systems and human interventions the best estimate method shall be used. Where the best estimate method cannot be used, the distortion effect resulting from the conservatism of the assumptions shall be evaluated.
HU_NSC-118/2011_038	If the capability of transferring the residual heat to the ultimate heat sink cannot be demonstrated for every operating condition with high reliability, then a secondary ultimate heat sink and systems required for its operation shall be provided, which ensure through their locations and design solutions that the heat removal safety function is not lost as a result of external hazard factors.
HU_NSC-118/2011_042	In the course of the survey and evaluation of the site, probabilistic hazard curves shall be determined for the hazard factors, i.e. the intensity of the hazard factors as a function of frequency. All hazard factors shall be examined from the point of view whether they can trigger a cliff edge effect.
HU_NSC-118/2011_043	The potential and the effect of simultaneous occurrence or the cause-effect occurrence of events and on-site environmental conditions shall be considered in the assessment of the site events. The criterion for the probability screening of individual events, prescribed in Annex 3, 3/A, 5 or 6 depending on the type of the nuclear facility, shall be coherently used in the assessment of the simultaneous occurrence of various external events and conditions.
FI_A.4_001	323. The competence development programmes and training shall ensure that the personnel are aware of the safety significance of the functions they perform. The training shall emphasise the overriding priority of safety and the importance of meeting the safety requirements. Where applicable, Probabilistic Risk Assessment (PRA) shall be used in planning the training.
FI_A.4_002	342a. The planning of simulator training for control room operators shall ensure that the most important accident sequences and risk-significant operator actions are covered by the training. Probabilistic Risk Assessment (PRA), covered by Guide YVL A.7 “Probabilistic risk assessment and risk management of a nuclear power plant”, shall be used in planning the training.
FI_A.7_003	309. The PRA shall be applied in the nuclear power plant’s layout and systems design to assess the probability of hazards and event sequences affecting the safety of the nuclear power plant and to ensure the adequate reliability of safety functions and the balance of the design.

BESEP id	Original requirement text
FI_A.7_004	401. In the PRA, the following shall be analysed as initiating events: the plant's internal failures, disturbances and human errors, loss of off-site power supply, fires, flooding, hoisting of heavy loads, abnormal weather conditions, seismic events and other environmental factors as well as external factors caused by human activities. In accordance with para 205, the PRA need not address risks arising from acts of sabotage.
FI_B.7_003	401. A design basis earthquake shall be determined for the nuclear facility. A design basis earthquake refers to facility site bedrock surface motion used as the basis for the nuclear facility's design. The design basis earthquake shall be so defined that in the current geological conditions the anticipated frequency of occurrence of stronger bedrock motions is less than once in a hundred thousand years (1·10-5/year) at a median confidence level.
FI_B.7_004	402. The external impact of the design basis earthquake on the nuclear facility shall be presented as a ground response spectrum. The ground response spectrum represents the maximum vibrations of a family of idealised single-degree-of-freedom damped oscillators anchored in site bedrock as a function of the natural frequencies for a given damping ratio.
FI_B.7_005	403. A ground response spectrum shall be determined for the nuclear facility site using information and measurement results describing the site as well as possible. In determining the ground response spectrum, data on earthquake locations and magnitudes collected in Finland and, if necessary, in nearby areas shall be used. Instrumental observation data and historical data obtained by sensory observations shall be used. Analyses shall take into account the various observation thresholds of different types of observation and the location-related uncertainty factors of historical observations.
FI_B.7_006	404. Acceleration induced at a facility site by an earthquake of a certain magnitude at a certain distance is evaluated by means of a ground motion prediction equation. The ground motion prediction equation shall be based on data measured in an area corresponding as well as possible to the geological conditions in the area of the facility site. The selection of the ground motion prediction equations used to determine the ground response spectrum shall be justified.
FI_B.7_007	405. The ground response spectrum used in the design shall be based on the ground response spectrum determined for the site. The ground response spectrum shall be scaled to correspond to vertical and horizontal peak ground acceleration (PGA) values at rock surfaces and, if necessary, a separate spectrum for both directions of vibration shall be given.
FI_B.7_008	407. The vertical and horizontal PGA values used shall be justified on a site-specific basis. The horizontal component minimum value shall be 0.1·g as prescribed in the Guides IAEA NS-G-1.6 [9] and IAEA SSG-9 [8]. The relation between the horizontal and vertical components at different acceleration and frequency levels can be determined, for example, in accordance with the Guide IAEA SSG-9 or report NUREG/CR-6728 [18].
FI_B.7_009	408. In connection with the design basis earthquake, a hazard curve for the peak ground acceleration (PGA) of the rock surface shall be presented at least up to the recurrence time of 107 years for the assessment of design extension conditions (DEC) in accordance with Guide YVL B.1 and for seismic PRA.

BESEP id	Original requirement text
FI_B.7_012	430. The probabilistic risk assessment (PRA) shall be applied to demonstrate that the implementation of seismic design is acceptable from the viewpoint of the nuclear facility's overall safety.
FI_B.7_015	440. The most important initiating events due to earthquake-induced failures and component malfunctions shall be incorporated in the PRA to be drawn up in accordance with Guide YVL A.7. The seismic PRA shall, irrespective of seismic classification, consider components plus their supports, as well as experiences of the susceptibility to failure of different types of structures and components in actual earthquakes of varying intensities. Failure sequences attributable to the simultaneous dynamic loading of large equipment aggregates and the possibility of common cause failures shall be analysed.
FI_B.7_016	441. PRA analyses shall demonstrate systems significant for safe shutdown and determine the HCLPF estimates for corresponding fragilities of components and structures. The fragility estimates shall be based on 3D analyses of structural framework and actual fixing methods in such a way that all directions of vibration have been appropriately evaluated.
FI_B.7_020	503. The following general principles shall be followed in selecting design values for systems, structures and components important to safety that pertain to external events and conditions: a. Design values shall include an adequate margin in relation to the peak values measured at the facility site and in its vicinity. b. In determining design values, at least phenomena whose estimated probability of occurrence at the site over one year is higher than 10-5 at a median confidence level shall be considered. c. If it can be reliably demonstrated that an external event or condition does not affect the probability of occurrence of a certain postulated accident, the design value regarding the external event or condition in question can be chosen for the systems required for the management of the postulated accident so that its maximum probability of exceedance in one year is 10-4. d. The safety significance of systems, structures and components important to safety shall be considered in selecting their design values, and the adequacy of the design values shall be justified.
FI_B.7_021	504. In addition to the above, to be ensured in selecting the sea water level design value is that the design value is higher than a. the water level estimated possible at the site at a median confidence level once in a hundred years added with two metres and a site-specifically evaluated wave margin, and b. the extreme level equivalent to the least favourable combination of factors evaluated in accordance with requirement 515 added with a site-specifically evaluated wave margin.
FI_B.7_026	508. The adequacy of design values for external events and conditions shall be verified by means of probabilistic risk assessment. The probabilistic studies shall take into account interdependencies between natural phenomena. Guide YVL A.7 presents the limits for core damage frequency and large release frequency, which also include the external hazard contribution.
FI_B.7_027	509. To determine the nuclear facility's design bases, the occurrence frequencies of external events affecting plant safety shall be assessed. A hazard curve shall be drawn up for phenomena for which measurements time series are available; the curve shall present the

BESEP id	Original requirement text
	exceedance frequency of the parameter value representing the phenomenon.
FI_B.7_028	510. If a hazard curve needs to be determined for a recurrence period exceeding the period covered by the measurement results, fitting of an extreme value distribution to the time series shall be employed. The mathematical form of the extreme value distribution shall be selected with the aim that the final outcome will not be non-conservatively sensitive to the effects of individual measurement results.

B.2.2 Quantitative safety goals/criteria

For this requirement topic there are no high-level IAEA requirements.

The original national requirements related to quantitative safety goals/criteria are shown in the following table.

Table B.15 National requirements related to quantitative safety goals/criteria

BESEP id	Original requirement text
SE_SSMFS-A_006	Radiological acceptance criteria for assessment on effective dose to representative individual of the population. H1: 0,025 mSv/year H2: 1 mSv per event or condition H3: 10 mSv per event or condition H4A: 100 mSv per event or condition H4B: 100 mSv per event or condition
SE_SSMFS-A_007	Acceptance criteria for assessment regarding release of radiological substances to the environment. H2: 0,1 TBq per event or condition H3: 1 TBq per event or condition H4A: 10 TBq per event or condition H4B: 10 TBq per event or condition H5: 100 TBq per event or condition
SE_SSMFS-A_010	The probabilistic safety analyses must take the events and conditions that are identified in accordance with 3 kap. 1 § SSMFS-K into account. The probabilistic safety analyses must refer to 1. the occurrence rate of damage to nuclear fuel assemblies (level 1), and 2. the occurrence rate of release of radiological substances to the environment as a consequence of the damage to the nuclear fuel assemblies (level 2). The probabilistic safety analyses do not have to take into account such events and conditions according to the first paragraph not considered relevant for the application of the analysis.
SK_UJDSR-BNS-I.4.2/2017_001	(a) the frequency of core damage frequency (CDF) is set at 1,0E-5 /year;
SK_UJDSR-BNS-I.4.2/2017_002	b) the large release frequency (LRF) and large early release frequency (LERF) of radioactive substances is set at 1.0E-6 / year. Contributions from the actual non-readiness of facilities affecting nuclear safety are included. The monitored period represents all modes of operation of nuclear power plants during the entire calendar year, on power and even when tripped. To compare with probabilistic safety targets, the mean values of the PSA results should be used, which include all initiating events triggered by both internal and external events. The

BESEP id	Original requirement text
	determination of probabilistic safety objectives and probabilistic safety criteria for NPP is legally required / 4 /. The permit holder may set more stringent values in the quality requirements for probability safety targets than those set out in this section of the BNS.
SK_UJDSR-BNS-I.4.2/2017_003	The probabilistic safety criteria specified in the quality requirements of the nuclear installation must be met. From the data contained in IAEA documents and the surveys prepared by show that the probability safety objectives set for nuclear power plants at the level of the core damage frequency, the moving range of 1.0E-4 / year - 1.0E-5 / year (the greater of the values is used for older units and lower value for the new units of nuclear power plants); the frequency of large or large early leakage of radioactive substances+C2 is set at least 10 times lower than the frequency of damage to nuclear fuel.
CZ_BN-JB-2.5_003	It is required for broad PSA applications that Level-1 and Level-2 PSA model for both full power and shutdown is available, which covers full spectrum of possible IEs, including those caused by hazards.
HU_NSC-118/2011_014	To define the exact risk of the nuclear power plant, to verify the fulfilment of relevant acceptance criteria, to evaluate the consistency and coherence of the design as well as to determine the suitability of the extended design basis a probabilistic safety analysis shall be performed. Probabilistic safety analyses shall be used to demonstrate that due margins are available to avoid cliff-edge effects.
HU_NSC-118/2011_020	With consideration to all designed operating conditions and postulated initiating events, excluding sabotage, the frequency of core damage shall not exceed 10^{-4}/year.
HU_NSC-118/2011_021	For all initial operating conditions and effects, excluding sabotage and earthquake, the collective frequency of severe accident event sequences resulting in large or early large releases shall not exceed 10^{-5}/year, but with every reasonable modification and intervention 10^{-6}/year shall be targeted. The fulfilment of criteria shall be demonstrated by Level 2 probabilistic safety analyses.
FI_A.7_001	305. The design of a nuclear power plant unit shall be such that the mean value of the frequency of reactor core damage is less than 10-5/year.
FI_A.7_002	306. A nuclear power plant unit shall be designed in compliance with the principles set forth in Section 22 b of the Nuclear Energy Decree (161/1988) in a way that a. the mean value of the frequency of a release of radioactive substances from the plant during an accident involving a cesium-137 release (Cs-137) into the atmosphere in excess of 100 TBq is less than 5·10-7/year; b. the accident sequences, in which the containment function fails or is lost in the early phase of a severe accident, have only a small contribution to the reactor core damage frequency. Release assessments shall take into account all of the nuclear fuel located at the plant unit. A spent nuclear fuel storage external to the plant unit is considered a separate nuclear facility that must meet the requirement laid down in item a.
FI_B.7_003	401. A design basis earthquake shall be determined for the nuclear facility. A design basis earthquake refers to facility site bedrock surface motion used as the basis for the nuclear facility's design. The design basis earthquake shall be so defined that in the current geological conditions the anticipated frequency of occurrence of stronger bedrock motions is less than once in a hundred thousand years (1·10-5/year) at a median confidence level.

BESEP id	Original requirement text
FI_B.7_007	405. The ground response spectrum used in the design shall be based on the ground response spectrum determined for the site. The ground response spectrum shall be scaled to correspond to vertical and horizontal peak ground acceleration (PGA) values at rock surfaces and, if necessary, a separate spectrum for both directions of vibration shall be given.
FI_B.7_008	407. The vertical and horizontal PGA values used shall be justified on a site-specific basis. The horizontal component minimum value shall be 0.1·g as prescribed in the Guides IAEA NS-G-1.6 and IAEA SSG-9. The relation between the horizontal and vertical components at different acceleration and frequency levels can be determined, for example, in accordance with the Guide IAEA SSG-9 or report NUREG/CR-6728.
FI_B.7_009	408. In connection with the design basis earthquake, a hazard curve for the peak ground acceleration (PGA) of the rock surface shall be presented at least up to the recurrence time of 107 years for the assessment of design extension conditions (DEC) in accordance with Guide YVL B.1 and for seismic PRA.
FI_B.7_026	508. The adequacy of design values for external events and conditions shall be verified by means of probabilistic risk assessment. The probabilistic studies shall take into account interdependencies between natural phenomena. Guide YVL A.7 presents the limits for core damage frequency and large release frequency, which also include the external hazard contribution.

B.2.3 Initiating event frequency estimation

The IAEA high-level requirements related to initiating event frequency estimation are shown in the following table.

Table B.16 IAEA high-level requirements related to initiating event frequency estimation

IAEA requirement	IAEA Requirement text
Requirement 16: Postulated initiating events	Requirement 16: Postulated initiating events. The design for the nuclear power plant shall apply a systematic approach to identifying a comprehensive set of postulated initiating events such that all foreseeable events with the potential for serious consequences and all foreseeable events with a significant frequency of occurrence are anticipated and are considered in the design. The postulated initiating events shall be identified on the basis of engineering judgement and a combination of deterministic assessment and probabilistic assessment. A justification of the extent of usage of deterministic safety analysis and probabilistic safety analysis shall be provided to show that all foreseeable events have been considered.
Requirement 17: Internal and external hazards	Requirement 17: Internal and external hazards. All foreseeable internal hazards and external hazards, including the potential for human induced events directly or indirectly to affect the safety of the nuclear power plant, shall be identified and their effects shall be evaluated. […] External hazards: The design shall include due consideration of those natural and human induced external events (i.e., events of origin external to the plant) that have been identified in the site evaluation process. Causation and likelihood shall be considered in postulating potential hazards. […] The design of the plant shall provide for an adequate margin to protect items important to safety against levels of

IAEA requirement	IAEA Requirement text
	external hazards to be considered for design, derived from the hazard evaluation for the site, and to avoid cliff edge effects. A cliff edge effect, in a nuclear power plant, is an instance of severely abnormal plant behaviour caused by an abrupt transition from one plant status to another following a small deviation in a plant parameter, and thus a sudden large variation in plant conditions in response to a small variation in an input. [...]
Requirement 42: Safety analysis of the plant design	Requirement 42: Safety analysis of the plant design. A safety analysis of the design for the nuclear power plant shall be conducted in which methods of both deterministic analysis and probabilistic analysis shall be applied to enable the challenges to safety in the various categories of plant states to be evaluated and assessed. […] The safety analysis shall provide assurance that uncertainties have been given adequate consideration in the design of the plant and in particular that adequate margins are available to avoid cliff edge effects and early radioactive releases or large radioactive releases. The applicability of the analytical assumptions, methods and degree of conservatism used in the design of the plant shall be updated and verified for the current or as built design. […] The probabilistic safety analysis of the plant is performed for all modes of operation and for all plant states, including shutdown, with particular reference to: • Establishing that a balanced design has been achieved such that no particular feature or postulated initiating event makes a disproportionately large or significantly uncertain contribution to the overall risks, and that, to the extent practicable, the levels of defence in depth are independent; • Providing assurance that situations in which small deviations in plant parameters could give rise to large variations in plant conditions (cliff edge effects) will be prevented; • Comparing the results of the analysis with the acceptance criteria for risk where these have been specified.
Requirement 65: Control room	Requirement 65: Control room. […] Special attention shall be paid to identifying those events, both internal and external to the control room, that could challenge its continued operation, and the design shall provide for reasonably practicable measures to minimize the consequences of such events. The design of the control room shall provide an adequate margin against levels of natural hazards more severe than those considered for design, derived from the hazard evaluation for the site.
Requirement 66: Supplementary control room	Requirement 66: Supplementary control room. Instrumentation and control equipment shall be kept available, preferably at a single location (a supplementary control room) that is physically, electrically and functionally separate from the control room at the nuclear power plant. […]

The original national requirements related to initiating event frequency estimation are shown in the following table.

Table B.17 National requirements related to initiating event frequency estimation

BESEP id	Original requirement text
SE_SSMFS-A_001	Identified events and conditions where specified conditions and restrictions for normal operation are exceeded, shall be assigned to event class H5 if 1. they are not assumed to occur at a frequency of occurrence of less than 10-6 per year and are not assigned to event class H6, 2. they are events and conditions with extensive release of radioactive substances from the reactor core of a new nuclear reactor, 3. there is a rupture in a steam line in the reactor containment for an existing BWR in combination with leaking diaphragm floor between drywell and wetwell, 4. there is a failure of all non-battery-powered power supply including any gravity-powered or steam-powered pumps for existing reactors, or 5. they are antagonistic events and conditions which in the dimensioning threat description decided by the Swedish Radiation Safety Authority are equated with events and conditions according to 1.
SE_SSMFS-A_002	Identified events and conditions where specified conditions and restrictions for normal operation are exceeded, shall be assigned to event class H2 if they 1. are assumed to occur during the expected lifetime of a nuclear power reactor that is greater or equal to 10-2 per year, or 2. are antagonistic events and conditions that in the dimensioning threat description decided by the Swedish Radiation Safety Authority are equated with events and conditions in accordance with 1.
SE_SSMFS-A_003	Identified events and conditions where specified terms and restrictions for normal operation are exceeded, shall be assigned to event class H3 if they 1. are not assumed to occur during the expected lifetime of a nuclear power reactor but are assumed to occur if more than one nuclear power reactor are taken into consideration with an occurrence rate that is less than 10-2 per year and greater or equal to 10-4 per year, or 2. are antagonistic events and conditions that inte the dimensioning threat description decided by the Swedish Radiation Safety Authority are equated with events and conditions in accordance with 1.
SE_SSMFS-A_004	Identified events and conditions where specified terms and restrictions for normal operation are exceeded, shall be assigned to event class H6 if it is not possible nor reasonable for them to be assigned to another event class.
SK_UJDSR-430/2011_002	(2) The project is in addition to conditions of physical protection of nuclear facilities and nuclear materials provided special regulation must be taken into account a) the most severe natural phenomena, historically reported in the area of location of nuclear installations and extrapolated with consideration of limited accuracy, if it comes to size and time of the event, b) a combination of the effects of phenomena caused by natural conditions and human activity, c) the maximum anticipated acceleration given for site placement, based on the evaluation of seismic load locations drawn up at placing nuclear installation, defined as seismic level 1 and seismic level 2, d) requirements for seismic resistance of systems, components and building structures of a nuclear installation or their parts, which must correspond to their safety function and expected earthquake effects according to the specified seismic level 1 and seismic level 2, (e) aircraft impacts.

BESEP id	Original requirement text
CZ_SUJB-162/2017_001	Probabilistic safety assessment has to address initiating events caused by both internal and external hazards, including hazards impacting large areas of NPP site.
CZ_SUJB-162/2017_004	Periodic safety assessment has to evaluate internal and external hazards from point of view of adequacy of existing resistance of NPP against the hazards, taking into consideration real status of all components, systems and structures impacting nuclear safety and the up-to-date values of probability of occurrence of hazard scenarios obtained from up-date of plant site data, where the NPP is operated. Possible impacts of climate change and changes of human related activities (transport and other industrial activities in plant vicinity), as well as newly adopted measures determined for prevention and mitigation of hazards effects, which are based on defence-in-depth principles, have to be considered.
CZ_BN-JB-2.5_001	Hazards can (similarly to full power operation) significantly contribute to the overall risk of low power and shutdown. They should be analyzed similarly to full power operation, with some exceptions. In the selection of initiating events, differences in lengths of individual plant regimes can be important. The consequences of hazards impact can differ from those specified for full power.
CZ_BN-JB-2.5_002	The identification of hazards related IE is performed similarly to the full power operation. As the first approximation, list of IEs developed for full power operation may be used, which is extended and modified.
CZ_BN-JB-2.5_004	Level-1 and Level-2 PSA model for both full power and shutdown should be available, which covers full spectrum of possible IEs, including those caused by hazards, when verification that the plant fulfills safety targets and criteria is carried out, with the exception when the safety targets/criteria are defined for the matters covered by reduced scope of PSA, or when alternative approaches are used to confirm that the risk related to the hazards is negligible from point of view of the safety targets and criteria under concern.
HU_NSC-118/2011_006	Among the external hazard factors, those included in the design basis shall be selected on the basis of a site-specific analysis.
HU_NSC-118/2011_007	All realistic combination of the individual occurrences shall be considered during design, including external and internal events, which may lead to DBC4 or DEC plant states. The event combinations to be taken into account in the design shall be selected by taking into account both engineering considerations and probabilistic analyses.
HU_NSC-118/2011_008	For the design, the following can be excluded from the scope of postulated initiating events: a) internal initiating event due to the failure of a system, structure or component, and/or human error, if the frequency of the occurrence is less than 10^{-5}/year; b) event resulting from external human activity typical of the site, if the frequency of the hazard factor is less than 10^{-7}/year, or if the hazard factor is at such a distance, that it can be justified that it will not have an effect on the nuclear power plant unit; and c) initiating events occurring due to a recurring external hazard factor of natural origin, with a frequency of less than 10^{-4}/year, or external hazard factor of natural origin for which it can be demonstrated that they are not able to pose a physical hazard to the power plant.
HU_NSC-118/2011_009	At a power plant site with several nuclear power plant units, for the design of the whole nuclear power plant as well as for the individual nuclear power plant units it shall be considered that some external hazard factor s may affect all nuclear power plant units simultaneously.

BESEP id	Original requirement text
HU_NSC-118/2011_012	In the selection of events leading to DEC1 plant states, all events or event combinations about which it cannot be established with high certainty that the probability of their occurrence is very low and may lead to conditions that have not been taken into account in the design basis shall be taken into account. In the selection of the events the following should be considered: a) events that occur during the possible operating conditions, b) events that occur for the effect of internal and external hazard factors, c) common cause failures, d) impact of the nuclear facilities in the vicinity, in case of site with multiple units the mutual impacts of the units, and e) those events that may impact all facilities in the vicinity together with the mutual effects assumed among them.
HU_NSC-118/2011_013	The design basis, the extended design basis and their substantiation shall be periodically reviewed at the completion of the design, as well as during the whole lifetime of the nuclear power plant, when significant new safety information is received and based on the results of deterministic and probabilistic calculations or engineering judgement, modifications shall be implemented if necessary. The identified defects and possible safety improvements shall be evaluated and the necessary actions shall be taken in time.
HU_NSC-118/2011_015	For the design of a nuclear power plant unit, including the systems for storage and manage spent fuel, level 1 and level 2 probabilistic safety analysis shall be developed, which considers all possible operating conditions, system configurations and all of the postulated initiating events for which it cannot be demonstrated by any other method that their contribution to the risk is insignificant. In the level 1 and 2 probabilistic safety analyses, considering the state-of-the-art results of science and technology, the external hazards shall be taken into account. Where it is not possible, proven alternative analysis solutions shall be used to assess the contribution of the external hazard factors to the overall risk represented by the nuclear power plant.
FI_A.7_003	309. The PRA shall be applied in the nuclear power plant's layout and systems design to assess the probability of hazards and event sequences affecting the safety of the nuclear power plant and to ensure the adequate reliability of safety functions and the balance of the design.
FI_A.7_004	401. In the PRA, the following shall be analysed as initiating events: the plant's internal failures, disturbances and human errors, loss of off-site power supply, fires, flooding, hoisting of heavy loads, abnormal weather conditions, seismic events and other environmental factors as well as external factors caused by human activities. In accordance with para 205, the PRA need not address risks arising from acts of sabotage.
FI_B.7_003	401. A design basis earthquake shall be determined for the nuclear facility. A design basis earthquake refers to facility site bedrock surface motion used as the basis for the nuclear facility's design. The design basis earthquake shall be so defined that in the current geological conditions the anticipated frequency of occurrence of stronger bedrock motions is less than once in a hundred thousand years (1·10-5/year) at a median confidence level.
FI_B.7_004	402. The external impact of the design basis earthquake on the nuclear facility shall be presented as a ground response spectrum. The ground response spectrum represents the maximum vibrations of a family of idealised single-degree-of-freedom damped oscillators

BESEP id	Original requirement text
	anchored in site bedrock as a function of the natural frequencies for a given damping ratio.
FI_B.7_005	403. A ground response spectrum shall be determined for the nuclear facility site using information and measurement results describing the site as well as possible. In determining the ground response spectrum, data on earthquake locations and magnitudes collected in Finland and, if necessary, in nearby areas shall be used. Instrumental observation data and historical data obtained by sensory observations shall be used. Analyses shall take into account the various observation thresholds of different types of observation and the location-related uncertainty factors of historical observations.
FI_B.7_008	407. The vertical and horizontal PGA values used shall be justified on a site-specific basis. The horizontal component minimum value shall be 0.1·g as prescribed in the Guides IAEA NS-G-1.6 and IAEA SSG-9. The relation between the horizontal and vertical components at different acceleration and frequency levels can be determined, for example, in accordance with the Guide IAEA SSG-9 or report NUREG/CR-6728.
FI_B.7_009	408. In connection with the design basis earthquake, a hazard curve for the peak ground acceleration (PGA) of the rock surface shall be presented at least up to the recurrence time of 107 years for the assessment of design extension conditions (DEC) in accordance with Guide YVL B.1 and for seismic PRA.
FI_B.7_020	503. The following general principles shall be followed in selecting design values for systems, structures and components important to safety that pertain to external events and conditions: a. Design values shall include an adequate margin in relation to the peak values measured at the facility site and in its vicinity. b. In determining design values, at least phenomena whose estimated probability of occurrence at the site over one year is higher than 10-5 at a median confidence level shall be considered. c. If it can be reliably demonstrated that an external event or condition does not affect the probability of occurrence of a certain postulated accident, the design value regarding the external event or condition in question can be chosen for the systems required for the management of the postulated accident so that its maximum probability of exceedance in one year is 10-4. d. The safety significance of systems, structures and components important to safety shall be considered in selecting their design values, and the adequacy of the design values shall be justified.
FI_B.7_021	504. In addition to the above, to be ensured in selecting the sea water level design value is that the design value is higher than a. the water level estimated possible at the site at a median confidence level once in a hundred years added with two metres and a site-specifically evaluated wave margin, and b. the extreme level equivalent to the least favourable combination of factors evaluated in accordance with requirement 515 added with a site-specifically evaluated wave margin.
FI_B.7_023	506. Exceptional external events and conditions with an estimated frequency of occurrence less than 10-5/year shall be considered design extension conditions (DEC C events). The licence applicant/licensee shall present and justify external phenomena considered as DEC C events. In selecting the phenomena and their magnitude, the limit values for core damage and large release frequency presented in Guide YVL A.7 shall be taken into account. To be incorporated in the DEC C design values is a justified marginal in relation to the observed maximum values of the phenomena analysed.

BESEP id	Original requirement text
FI_B.7_027	509. To determine the nuclear facility's design bases, the occurrence frequencies of external events affecting plant safety shall be assessed. A hazard curve shall be drawn up for phenomena for which measurements time series are available; the curve shall present the exceedance frequency of the parameter value representing the phenomenon.
FI_B.7_028	510. If a hazard curve needs to be determined for a recurrence period exceeding the period covered by the measurement results, fitting of an extreme value distribution to the time series shall be employed. The mathematical form of the extreme value distribution shall be selected with the aim that the final outcome will not be non-conservatively sensitive to the effects of individual measurement results.

B.2.4 Assessment of potential losses of safety functions

The IAEA high-level requirements related to assessment of potential losses of safety functions are shown in the following table.

Table B.18 IAEA high-level requirements related to assessment of potential losses of safety functions

IAEA requirement	IAEA Requirement text
Requirement 23: Reliability of items important to safety	Requirement 23: Reliability of items important to safety. The reliability of items important to safety shall be commensurate with their safety significance.
Requirement 32: Design for optimal operator performance	Requirement 32: Design for optimal operator performance. Systematic consideration of human factors, including the human–machine interface, shall be included at an early stage in the design process for a nuclear power plant and shall be continued throughout the entire design process. The design shall support operating personnel in the fulfilment of their responsibilities and in the performance of their tasks and shall limit the likelihood and the effects of operating errors on safety. The design process shall give due consideration to plant layout and equipment layout, and to procedures, including procedures for maintenance and inspection, to facilitate interaction between the operating personnel and the plant, in all plant states. The human–machine interface shall be designed to provide the operators with comprehensive but easily manageable information, in accordance with the necessary decision times and action times. The information necessary for the operator to make decisions to act shall be simply and unambiguously presented. The operator shall be provided with the necessary information: To assess the general state of the plant in any condition; • To operate the plant within the specified limits on parameters associated with plant systems and equipment (operational limits and conditions); • To confirm that safety actions for the actuation of safety systems are automatically initiated when needed and that the relevant systems perform as intended; • To determine both the need for and the time for manual initiation of the specified safety actions.

IAEA requirement	IAEA Requirement text
	The design shall be such as to promote the success of operator actions with due regard for the time available for action, the conditions to be expected and the psychological demands being made on the operator. The need for intervention by the operator on a short time scale shall be kept to a minimum, and it shall be demonstrated that the operator has sufficient time to make a decision and sufficient time to act. The design shall be such as to ensure that, following an event affecting the plant, environmental conditions in the control room or the supplementary control room and in locations on the access route to the supplementary control room do not compromise the protection and safety of the operating personnel. The design of workplaces and the working environment of the operating personnel shall be in accordance with ergonomic concepts. Verification and validation, including by the use of simulators, of features relating to human factors shall be included at appropriate stages to confirm that necessary actions by the operator have been identified and can be correctly performed.
Requirement 63: Use of computer-based equipment in systems important to safety	Requirement 63: Use of computer based equipment in systems important to safety. If a system important to safety at the nuclear power plant is dependent upon computer based equipment, appropriate standards and practices for the development and testing of computer hardware and software shall be established and implemented throughout the service life of the system, and in particular throughout the software development cycle. The entire development shall be subject to a quality management system. For computer based equipment in safety systems or safety related systems: • A high quality of, and best practices for, hardware and software shall be used, in accordance with the importance of the system to safety. • The entire development process, including control, testing and commissioning of design changes, shall be systematically documented and shall be reviewable. • An assessment of the equipment shall be undertaken by experts who are independent of the design team and the supplier team to provide assurance of its high reliability. • Where safety functions are essential for achieving and maintaining safe conditions, and the necessary high reliability of the equipment cannot be demonstrated with a high level of confidence, diverse means of ensuring fulfilment of the safety functions shall be provided. • Common cause failures deriving from software shall be taken into consideration. • Protection shall be provided against accidental disruption of, or deliberate interference with, system operation.

The original national requirements related to assessment of potential losses of safety functions are shown in the following table.

Table B.19 National requirements related to assessment of potential losses of safety functions

BESEP id	Original requirement text
SK_UJDSR-106/2016_004	(2) The permit holder shall review it by periodic evaluation c) the strategy and programs for long-term monitoring of the territory and surroundings of the nuclear power plant as well as the use of the obtained results in the prevention, mitigation and prediction of the impact of natural phenomena on the nuclear power plant,
SK_UJDSR-430/2011_002	(2) The project is in addition to conditions of physical protection of nuclear facilities and nuclear materials provided special regulation must be taken into account a) the most severe natural phenomena, historically reported in the area of location of nuclear installations and extrapolated with consideration of limited accuracy, if it comes to size and time of the event, b) a combination of the effects of phenomena caused by natural conditions and human activity, c) the maximum anticipated acceleration given for site placement, based on the evaluation of seismic load locations drawn up at placing nuclear installation, defined as seismic level 1 and seismic level 2, d) requirements for seismic resistance of systems, components and building structures of a nuclear installation or their parts, which must correspond to their safety function and expected earthquake effects according to the specified seismic level 1 and seismic level 2, (e) aircraft impacts.
CZ_SUJB-162/2017_004	Periodic safety assessment has to evaluate internal and external hazards from point of view of adequacy of existing resistance of NPP against the hazards, taking into consideration real status of all components, systems and structures impacting nuclear safety and the up-to-date values of probability of occurrence of hazard scenarios obtained from up-date of plant site data, where the NPP is operated. Possible impacts of climate change and changes of human related activities (transport and other industrial activities in plant vicinity), as well as newly adopted measures determined for prevention and mitigation of hazards effects, which are based on defence-in-depth principles, have to be considered.
CZ_BN-JB-2.5_005	Confirmation of sufficient separation among safety related components, systems and structures endangered by the hazards as fires or floods belongs to the elements of risk oriented decision making employing importance measures enumerated by PSA model.
HU_NSC-118/2011_012	In the selection of events leading to DEC1 plant states, all events or event combinations about which it cannot be established with high certainty that the probability of their occurrence is very low and may lead to conditions that have not been taken into account in the design basis shall be taken into account. In the selection of the events the following should be considered: a) events that occur during the possible operating conditions, b) events that occur for the effect of internal and external hazard factors, c) common cause failures, d) impact of the nuclear facilities in the vicinity, in case of site with multiple units the mutual impacts of the units, and e) those events that may impact all facilities in the vicinity together with the mutual effects assumed among them.
HU_NSC-118/2011_013	The design basis, the extended design basis and their substantiation shall be periodically reviewed at the completion of the design, as well as during the whole lifetime of the nuclear power plant, when significant new safety information is received and based on the results of deterministic and probabilistic calculations or engineering judgement, modifications shall be implemented if necessary. The

BESEP id	Original requirement text
	identified defects and possible safety improvements shall be evaluated and the necessary actions shall be taken in time.
HU_NSC-118/2011_014	To define the exact risk of the nuclear power plant, to verify the fulfilment of relevant acceptance criteria, to evaluate the consistency and coherence of the design as well as to determine the suitability of the extended design basis a probabilistic safety analysis shall be performed. Probabilistic safety analyses shall be used to demonstrate that due margins are available to avoid cliff-edge effects.
HU_NSC-118/2011_015	For the design of a nuclear power plant unit, including the systems for storage and manage spent fuel, level 1 and level 2 probabilistic safety analysis shall be developed, which considers all possible operating conditions, system configurations and all of the postulated initiating events for which it cannot be demonstrated by any other method that their contribution to the risk is insignificant. In the level 1 and 2 probabilistic safety analyses, considering the state-of-the-art results of science and technology, the external hazards shall be taken into account. Where it is not possible, proven alternative analysis solutions shall be used to assess the contribution of the external hazard factors to the overall risk represented by the nuclear power plant.
HU_NSC-118/2011_016	In the probabilistic safety analysis important functional, territorial dependencies, dependencies of physical situation of system components, dependencies from operation, maintenance and other common cause failures, especially missiles, effects of liquid and steam jets, internal fire and floods, as well as the accidents of nearby industrial facilities and the effects of human activities shall be considered.
HU_NSC-118/2011_017	The probabilistic safety analysis shall realistically model the performance of the nuclear power plant, for which the relevant design data, operational and accident-related instructions, accident management guidelines or drafts shall be considered, including human interventions and potential human errors. The appropriateness of the operating times assumed in the probabilistic safety analyses shall be demonstrated.
FI_A.7_003	309. The PRA shall be applied in the nuclear power plant's layout and systems design to assess the probability of hazards and event sequences affecting the safety of the nuclear power plant and to ensure the adequate reliability of safety functions and the balance of the design.

B.2.5 Uncertainty analysis of accident sequences and operating times

The IAEA high-level requirements related to uncertainty analysis of accident sequences and operating times are shown in the following table.

Table B.20 IAEA high-level requirements related to uncertainty analysis of accident sequences and operating times

IAEA requirement	IAEA Requirement text
Requirement 42: Safety analysis of the plant design	Requirement 42: Safety analysis of the plant design. A safety analysis of the design for the nuclear power plant shall be conducted in which methods of both deterministic analysis and probabilistic analysis shall be applied to enable the challenges to safety in the various categories of plant states to be evaluated and assessed.

IAEA requirement	IAEA Requirement text
	[…] The safety analysis shall provide assurance that uncertainties have been given adequate consideration in the design of the plant and in particular that adequate margins are available to avoid cliff edge effects and early radioactive releases or large radioactive releases. The applicability of the analytical assumptions, methods and degree of conservatism used in the design of the plant shall be updated and verified for the current or as built design. […] The probabilistic safety analysis of the plant is performed for all modes of operation and for all plant states, including shutdown, with particular reference to: • Establishing that a balanced design has been achieved such that no particular feature or postulated initiating event makes a disproportionately large or significantly uncertain contribution to the overall risks, and that, to the extent practicable, the levels of defence in depth are independent; • Providing assurance that situations in which small deviations in plant parameters could give rise to large variations in plant conditions (cliff edge effects) will be prevented; • Comparing the results of the analysis with the acceptance criteria for risk where these have been specified.

The original national requirements related to uncertainty analysis of accident sequences and operating times are shown in the following table.

Table B.21 National requirements related to uncertainty analysis of accident sequences and operating times

BESEP id	Original requirement text
SE_SSMFS-A_005	The specification of scenarios for radiological emergencies that are referred to in 4 kap. 1 § SSMFS-K regarding the design and construction of nuclear power reactors, shall be implemented taking into account events and conditions in event class H1-H5 and, as far as possible and reasonable events and conditions in event class H6. The specification of scenarios shall furthermore take simultaneous radiological emergencies that includes or affects all nuclear power reactors or nuclear technical facilities within the site during a long timespan.
SK_UJDSR-430/2011_002	(2) The project is in addition to conditions of physical protection of nuclear facilities and nuclear materials provided special regulation must be taken into account a) the most severe natural phenomena, historically reported in the area of location of nuclear installations and extrapolated with consideration of limited accuracy, if it comes to size and time of the event, b) a combination of the effects of phenomena caused by natural conditions and human activity, c) the maximum anticipated acceleration given for site placement, based on the evaluation of seismic load locations drawn up at placing nuclear installation, defined as seismic level 1 and seismic level 2, d) requirements for seismic resistance of systems, components and building structures of a nuclear installation or their parts, which must correspond to their safety function and expected earthquake effects

BESEP id	Original requirement text
	according to the specified seismic level 1 and seismic level 2, (e) aircraft impacts.
CZ_SUJB-162/2017_004	Periodic safety assessment has to evaluate internal and external hazards from point of view of adequacy of existing resistance of NPP against the hazards, taking into consideration real status of all components, systems and structures impacting nuclear safety and the up-to-date values of probability of occurrence of hazard scenarios obtained from up-date of plant site data, where the NPP is operated. Possible impacts of climate change and changes of human related activities (transport and other industrial activities in plant vicinity), as well as newly adopted measures determined for prevention and mitigation of hazards effects, which are based on defence-in-depth principles, have to be considered.
CZ_BN-JB-2.5_006	The examples of attributes used in definition of plant damage states include failure of containment structure, radioactive release from containment as well as failure of additional barriers (reactor building, other adjacent structures), where the analysis include also all external events, which can damage the structures under concern.
CZ_BN-JB-2.5_007	When the Level-2 PSA scope is extended by including hazards, the impact of the hazards included on plant systems used in severe accidents mitigation and the impact on containment integrity has to be addressed.
HU_NSC-118/2011_012	In the selection of events leading to DEC1 plant states, all events or event combinations about which it cannot be established with high certainty that the probability of their occurrence is very low and may lead to conditions that have not been taken into account in the design basis shall be taken into account. In the selection of the events the following should be considered: a) events that occur during the possible operating conditions, b) events that occur for the effect of internal and external hazard factors, c) common cause failures, d) impact of the nuclear facilities in the vicinity, in case of site with multiple units the mutual impacts of the units, and e) those events that may impact all facilities in the vicinity together with the mutual effects assumed among them.
HU_NSC-118/2011_013	The design basis, the extended design basis and their substantiation shall be periodically reviewed at the completion of the design, as well as during the whole lifetime of the nuclear power plant, when significant new safety information is received and based on the results of deterministic and probabilistic calculations or engineering judgement, modifications shall be implemented if necessary. The identified defects and possible safety improvements shall be evaluated and the necessary actions shall be taken in time.
HU_NSC-118/2011_014	To define the exact risk of the nuclear power plant, to verify the fulfilment of relevant acceptance criteria, to evaluate the consistency and coherence of the design as well as to determine the suitability of the extended design basis a probabilistic safety analysis shall be performed. Probabilistic safety analyses shall be used to demonstrate that due margins are available to avoid cliff-edge effects.
HU_NSC-118/2011_015	For the design of a nuclear power plant unit, including the systems for storage and manage spent fuel, level 1 and level 2 probabilistic safety analysis shall be developed, which considers all possible operating conditions, system configurations and all of the postulated initiating events for which it cannot be demonstrated by any other method that their contribution to the risk is insignificant. In the level 1 and 2 probabilistic safety analyses, considering the state-of-the-art results of

BESEP id	Original requirement text
	science and technology, the external hazards shall be taken into account. Where it is not possible, proven alternative analysis solutions shall be used to assess the contribution of the external hazard factors to the overall risk represented by the nuclear power plant.
HU_NSC-118/2011_016	In the probabilistic safety analysis important functional, territorial dependencies, dependencies of physical situation of system components, dependencies from operation, maintenance and other common cause failures, especially missiles, effects of liquid and steam jets, internal fire and floods, as well as the accidents of nearby industrial facilities and the effects of human activities shall be considered.
HU_NSC-118/2011_017	The probabilistic safety analysis shall realistically model the performance of the nuclear power plant, for which the relevant design data, operational and accident-related instructions, accident management guidelines or drafts shall be considered, including human interventions and potential human errors. The appropriateness of the operating times assumed in the probabilistic safety analyses shall be demonstrated.
HU_NSC-118/2011_019	In analyses regarding the definition of success criteria for systems and human interventions the best estimate method shall be used. Where the best estimate method cannot be used, the distortion effect resulting from the conservatism of the assumptions shall be evaluated.
HU_NSC-118/2011_028	Regarding each type of hazard factor being characteristic of the site and associated with the natural phenomena and processes in the design basis, the design parameters forming the design input shall be specified on the basis of the hazard curve, taking into account the screening criterion applicable to the given hazard factor. The analysis shall be performed by deterministic methods, and based on the state-of-the-art results of science and technology by probabilistic methods. The analysis shall take into account all available, validated data and, if possible, connections shall be established between the severity of the hazard factors, especially the extent and duration. If it is possible, the maximum, but still justified severity of the hazard factors shall be determined. Design basis design parameters and key properties shall be so specified that they shall ensure the avoidance of the cliff edge effect from the side of design inputs.
FI_B.7_026	508. The adequacy of design values for external events and conditions shall be verified by means of probabilistic risk assessment. The probabilistic studies shall take into account interdependencies between natural phenomena. Guide YVL A.7 presents the limits for core damage frequency and large release frequency, which also include the external hazard contribution.
FI_B.7_027	509. To determine the nuclear facility's design bases, the occurrence frequencies of external events affecting plant safety shall be assessed. A hazard curve shall be drawn up for phenomena for which measurements time series are available; the curve shall present the exceedance frequency of the parameter value representing the phenomenon.
FI_B.7_028	510. If a hazard curve needs to be determined for a recurrence period exceeding the period covered by the measurement results, fitting of an extreme value distribution to the time series shall be employed. The mathematical form of the extreme value distribution shall be selected with the aim that the final outcome will not be non-conservatively sensitive to the effects of individual measurement results.
HU_NSC-118/2011_017	The probabilistic safety analysis shall realistically model the performance of the nuclear power plant, for which the relevant design data, operational and accident-related instructions, accident

BESEP id	Original requirement text
	management guidelines or drafts shall be considered, including human interventions and potential human errors. The appropriateness of the operating times assumed in the probabilistic safety analyses shall be demonstrated.
HU_NSC-118/2011_019	In analyses regarding the definition of success criteria for systems and human interventions the best estimate method shall be used. Where the best estimate method cannot be used, the distortion effect resulting from the conservatism of the assumptions shall be evaluated.

B.2.6 Confidence provision for defence against the occurrence of cliff-edge effects

The IAEA high-level requirements related to confidence provision for defence against the occurrence of cliff-edge effects are shown in the following table.

Table B.22 IAEA high-level requirements related to confidence provision for defence against the occurrence of cliff-edge effects

IAEA requirement	IAEA Requirement text
Requirement 17: Internal and external hazards	Requirement 17: Internal and external hazards. All foreseeable internal hazards and external hazards, including the potential for human induced events directly or indirectly to affect the safety of the nuclear power plant, shall be identified and their effects shall be evaluated. […] External hazards: The design shall include due consideration of those natural and human induced external events (i.e., events of origin external to the plant) that have been identified in the site evaluation process. Causation and likelihood shall be considered in postulating potential hazards. […] The design of the plant shall provide for an adequate margin to protect items important to safety against levels of external hazards to be considered for design, derived from the hazard evaluation for the site, and to avoid cliff edge effects. A cliff edge effect, in a nuclear power plant, is an instance of severely abnormal plant behaviour caused by an abrupt transition from one plant status to another following a small deviation in a plant parameter, and thus a sudden large variation in plant conditions in response to a small variation in an input. [...]
Requirement 42: Safety analysis of the plant design	Requirement 42: Safety analysis of the plant design. A safety analysis of the design for the nuclear power plant shall be conducted in which methods of both deterministic analysis and probabilistic analysis shall be applied to enable the challenges to safety in the various categories of plant states to be evaluated and assessed. […] The safety analysis shall provide assurance that uncertainties have been given adequate consideration in the design of the plant and in particular that adequate margins are available to avoid cliff edge effects and early radioactive releases or large radioactive releases. The applicability of the analytical assumptions, methods and degree of conservatism used in the design of the plant shall be updated and verified for the current or as built design. […] The probabilistic safety analysis of the plant is performed for all modes of operation and for all plant states, including shutdown, with particular reference to:

IAEA requirement	IAEA Requirement text
	• Establishing that a balanced design has been achieved such that no particular feature or postulated initiating event makes a disproportionately large or significantly uncertain contribution to the overall risks, and that, to the extent practicable, the levels of defence in depth are independent; • Providing assurance that situations in which small deviations in plant parameters could give rise to large variations in plant conditions (cliff edge effects) will be prevented; • Comparing the results of the analysis with the acceptance criteria for risk where these have been specified.

The original national requirements related to confidence provision for defence against the occurrence of cliff-edge effects are shown in the following table.

Table B.23 National requirements related to confidence provision for defence against the occurrence of cliff-edge effects

BESEP id	Original requirement text
HU_NSC-118/2011_001	During design of a nuclear power plant, in accordance with the defence in-depth principle: a) it shall be ensured by design solutions that the fundamental safety functions are performed by means of the safety barriers or mitigating the consequences of any abnormal operation or deviation. b) systems providing safety functions shall be applied to prevent or manage DBC2-4 and DEC1-2 and; c) the design of the barriers shall be conservative, their implementation shall be of the highest standards to ensure: ca) the probability of failures and deviations from normal operating conditions shall be as low as reasonably achievable, cb) DBC4 and DEC plant states shall be prevented to a reasonably achievable level, furthermore cc) no cliff edge effect can arise; d) the manageability of the condition of the nuclear power plant shall be ensured by technical means in such a way that in the event of a failure or deviation from normal operating conditions the necessity to operate the systems providing safety functions shall be as limited as possible; e) the control of nuclear power plant conditions shall be highly reliable even under conditions requiring the operation of the systems that provide safety functions, and shall not require human intervention in the preliminary phase of the process.
HU_NSC-118/2011_014	To define the exact risk of the nuclear power plant, to verify the fulfilment of relevant acceptance criteria, to evaluate the consistency and coherence of the design as well as to determine the suitability of the extended design basis a probabilistic safety analysis shall be performed. Probabilistic safety analyses shall be used to demonstrate that due margins are available to avoid cliff-edge effects.
HU_NSC-118/2011_028	Regarding each type of hazard factor being characteristic of the site and associated with the natural phenomena and processes in the design basis, the design parameters forming the design input shall be specified on the basis of the hazard curve, taking into account the screening criterion applicable to the given hazard factor. The analysis shall be performed by deterministic methods, and based on the state-of-the-art results of science and technology by probabilistic methods. The analysis shall take into account all available, validated data and, if

BESEP id	Original requirement text
	possible, connections shall be established between the severity of the hazard factors, especially the extent and duration. If it is possible, the maximum, but still justified severity of the hazard factors shall be determined. Design basis design parameters and key properties shall be so specified that they shall ensure the avoidance of the cliff edge effect from the side of design inputs.

B.2.7 Support for developing abnormal and emergency operating procedures and severe accident guidelines

The IAEA high-level requirements related to support for developing abnormal and emergency operating procedures and severe accident guidelines are shown in the following table.

Table B.24 IAEA high-level requirements related to support for developing abnormal and emergency operating procedures and severe accident guidelines

IAEA requirement	IAEA Requirement text
Requirement 42: Safety analysis of the plant design	Requirement 42: Safety analysis of the plant design. A safety analysis of the design for the nuclear power plant shall be conducted in which methods of both deterministic analysis and probabilistic analysis shall be applied to enable the challenges to safety in the various categories of plant states to be evaluated and assessed. […] The safety analysis shall provide assurance that uncertainties have been given adequate consideration in the design of the plant and in particular that adequate margins are available to avoid cliff edge effects and early radioactive releases or large radioactive releases. The applicability of the analytical assumptions, methods and degree of conservatism used in the design of the plant shall be updated and verified for the current or as built design. […] The probabilistic safety analysis of the plant is performed for all modes of operation and for all plant states, including shutdown, with particular reference to: • Establishing that a balanced design has been achieved such that no particular feature or postulated initiating event makes a disproportionately large or significantly uncertain contribution to the overall risks, and that, to the extent practicable, the levels of defence in depth are independent; • Providing assurance that situations in which small deviations in plant parameters could give rise to large variations in plant conditions (cliff edge effects) will be prevented; • Comparing the results of the analysis with the acceptance criteria for risk where these have been specified.

The original national requirements related to support for developing abnormal and emergency operating procedures and severe accident guidelines are shown in the following table.

Table B.25 National requirements related to support for developing abnormal and emergency operating procedures and severe accident guidelines

BESEP id	Original requirement text
SE_SSMFS-A_005	The specification of scenarios for radiological emergencies that are referred to in 4 kap. 1 § SSMFS-K regarding the design and construction of nuclear power reactors, shall be implemented taking into account events and conditions in event class H1-H5 and, as far as possible and reasonable events and conditions in event class H6. The specification of scenarios shall furthermore take simultaneous radiological emergencies that includes or affects all nuclear power reactors or nuclear technical facilities within the site during a long timespan.
HU_NSC-118/2011_018	Human reliability analyses shall be performed, considering those aspects that may influence the activities and performance of operating personnel in the different operating conditions of the nuclear power plant unit.
FI_A.7_004	322. The most significant event sequences analysed in the PRA shall be used to support the development of the abnormal and emergency operating procedures.
FI_A.7_005	324. The PRA shall be used as support in deciding which severe accident event sequences are analysed in accordance with Guide YVL B.3 for radiation effects (releases and doses) caused by an accident and also in deciding which accident sequences are used in emergency planning in accordance with Guide YVL C.5.
FI_A.7_006	332. The PRA shall be used to develop abnormal and emergency operating procedures.

B.3 Human Factors Engineering

B.3.1 Situation awareness and assessment

The IAEA high-level requirements related to situation awareness and assessment are shown in the following table.

Table B.26 IAEA high-level requirements related to situation awareness and assessment

IAEA requirement	IAEA Requirement text
Requirement 32: Design for optimal operator performance	Requirement 32: Design for optimal operator performance. Systematic consideration of human factors, including the human–machine interface, shall be included at an early stage in the design process for a nuclear power plant and shall be continued throughout the entire design process. The design shall support operating personnel in the fulfilment of their responsibilities and in the performance of their tasks and shall limit the likelihood and the effects of operating errors on safety. The design process shall give due consideration to plant layout and equipment layout, and to procedures, including procedures for maintenance and inspection, to facilitate interaction between the operating personnel and the plant, in all plant states. The human–machine interface shall be designed to provide the operators with comprehensive but easily manageable information, in accordance with the necessary decision times and action times. The

IAEA requirement	IAEA Requirement text
	information necessary for the operator to make decisions to act shall be simply and unambiguously presented. The operator shall be provided with the necessary information: To assess the general state of the plant in any condition; • To operate the plant within the specified limits on parameters associated with plant systems and equipment (operational limits and conditions); • To confirm that safety actions for the actuation of safety systems are automatically initiated when needed and that the relevant systems perform as intended; • To determine both the need for and the time for manual initiation of the specified safety actions. The design shall be such as to promote the success of operator actions with due regard for the time available for action, the conditions to be expected and the psychological demands being made on the operator. The need for intervention by the operator on a short time scale shall be kept to a minimum, and it shall be demonstrated that the operator has sufficient time to make a decision and sufficient time to act. The design shall be such as to ensure that, following an event affecting the plant, environmental conditions in the control room or the supplementary control room and in locations on the access route to the supplementary control room do not compromise the protection and safety of the operating personnel. The design of workplaces and the working environment of the operating personnel shall be in accordance with ergonomic concepts. Verification and validation, including by the use of simulators, of features relating to human factors shall be included at appropriate stages to confirm that necessary actions by the operator have been identified and can be correctly performed.

The original national requirements related to situation awareness and assessment are shown in the following table.

Table B.27 National requirements related to situation awareness and assessment

BESEP id	Original requirement text
SE_SSMFS-K_001	The design of a nuclear power reactor must be adapted to human capabilities, so that the risk of incorrect action is as small as possible and reasonable in events and conditions in event class H1-H5 and in scenarios for radiological emergencies, by taking into account performance factors for 1. manual tasks, 2. structures, systems and components, non-installed equipment and the areas and spaces where manual tasks are performed, 3. surrounding physical environment, and 4. organizational conditions.
HU_NSC-118/2011_026	Special emergency operating and accident management procedures and actions shall be developed for the event of an earthquake. The organisation of the operation and service of the nuclear power plant, the condition assessment, the scope of inspections following an

BESEP id	Original requirement text
	earthquake, their methods and the conditions of restart shall be regulated in the procedures and action plans.
FI_A.4_001	323. The competence development programmes and training shall ensure that the personnel are aware of the safety significance of the functions they perform. The training shall emphasise the overriding priority of safety and the importance of meeting the safety requirements. Where applicable, Probabilistic Risk Assessment (PRA) shall be used in planning the training.
FI_A.4_002	342a. The planning of simulator training for control room operators shall ensure that the most important accident sequences and risk-significant operator actions are covered by the training. Probabilistic Risk Assessment (PRA), covered by Guide YVL A.7 “Probabilistic risk assessment and risk management of a nuclear power plant”, shall be used in planning the training.

B.3.2 Guidance selection, decision making and intelligent use of guidance

The IAEA high-level requirements related to guidance selection, decision making and intelligent use of guidance are shown in the following table.

Table B.28 IAEA high-level IAEA high-level requirements related to guidance selection, decision making and intelligent use of guidance

IAEA requirement	IAEA Requirement text
Requirement 32: Design for optimal operator performance	Requirement 32: Design for optimal operator performance. Systematic consideration of human factors, including the human–machine interface, shall be included at an early stage in the design process for a nuclear power plant and shall be continued throughout the entire design process. The design shall support operating personnel in the fulfilment of their responsibilities and in the performance of their tasks and shall limit the likelihood and the effects of operating errors on safety. The design process shall give due consideration to plant layout and equipment layout, and to procedures, including procedures for maintenance and inspection, to facilitate interaction between the operating personnel and the plant, in all plant states. The human–machine interface shall be designed to provide the operators with comprehensive but easily manageable information, in accordance with the necessary decision times and action times. The information necessary for the operator to make decisions to act shall be simply and unambiguously presented. The operator shall be provided with the necessary information: To assess the general state of the plant in any condition; • To operate the plant within the specified limits on parameters associated with plant systems and equipment (operational limits and conditions); • To confirm that safety actions for the actuation of safety systems are automatically initiated when needed and that the relevant systems perform as intended; • To determine both the need for and the time for manual initiation of the specified safety actions.

IAEA requirement	IAEA Requirement text
	The design shall be such as to promote the success of operator actions with due regard for the time available for action, the conditions to be expected and the psychological demands being made on the operator. The need for intervention by the operator on a short time scale shall be kept to a minimum, and it shall be demonstrated that the operator has sufficient time to make a decision and sufficient time to act. The design shall be such as to ensure that, following an event affecting the plant, environmental conditions in the control room or the supplementary control room and in locations on the access route to the supplementary control room do not compromise the protection and safety of the operating personnel. The design of workplaces and the working environment of the operating personnel shall be in accordance with ergonomic concepts. Verification and validation, including by the use of simulators, of features relating to human factors shall be included at appropriate stages to confirm that necessary actions by the operator have been identified and can be correctly performed.

The original national requirements related to guidance selection, decision making and intelligent use of guidance are shown in the following table.

Table B.29 National requirements related to guidance selection, decision making and intelligent use of guidance

BESEP id	Original requirement text
SE_SSMFS-K_001	The design of a nuclear power reactor must be adapted to human capabilities, so that the risk of incorrect action is as small as possible and reasonable in events and conditions in event class H1-H5 and in scenarios for radiological emergencies, by taking into account performance factors for 1. manual tasks, 2. structures, systems and components, non-installed equipment and the areas and spaces where manual tasks are performed, 3. surrounding physical environment, and 4. organizational conditions.
SE_SSMFS-K_002	A nuclear power reactor must be designed so that the manual tasks that contribute to the completion of the functions given in 4 kap. 2-4 §§ SSMFS-K during events and conditions in event class H1-H5 and during scenarios for radiological emergencies can be carried out by 1. there is sufficient time to complete the tasks, 2. there are routines and training for the tasks, 3. relevant information is presented making it possible to read out courses of events and see effects of activations, other operational changes and passive functions so that needs for actions can be identified and actions can be performed, and 4. areas, spaces, structures, systems and components that are necessary to perform tasks are available, accessible, and possible to access with respect to the environmental conditions, strains and other effects that may occur during events and conditions in event class H1-H5.
HU_NSC-118/2011_018	Human reliability analyses shall be performed, considering those aspects that may influence the activities and performance of operating

BESEP id	Original requirement text
	personnel in the different operating conditions of the nuclear power plant unit.
HU_NSC-118/2011_026	Special emergency operating and accident management procedures and actions shall be developed for the event of an earthquake. The organisation of the operation and service of the nuclear power plant, the condition assessment, the scope of inspections following an earthquake, their methods and the conditions of restart shall be regulated in the procedures and action plans.
FI_A.4_001	323. The competence development programmes and training shall ensure that the personnel are aware of the safety significance of the functions they perform. The training shall emphasise the overriding priority of safety and the importance of meeting the safety requirements. Where applicable, Probabilistic Risk Assessment (PRA) shall be used in planning the training.
FI_A.4_002	342a. The planning of simulator training for control room operators shall ensure that the most important accident sequences and risk-significant operator actions are covered by the training. Probabilistic Risk Assessment (PRA), covered by Guide YVL A.7 “Probabilistic risk assessment and risk management of a nuclear power plant”, shall be used in planning the training.
FI_Y/1_002	1. Human factors relating to safety shall be controlled with systematic procedures throughout the entire life cycle of the nuclear facility. Human factors shall be taken into account in the design of the nuclear facility and in the planning of its operations, maintenance and decommissioning in a manner that supports the high-quality implementation of the work and ensures that human activities do not endanger plant safety. Attention shall be paid to the avoidance, detection and correction of human errors and the limiting of their effects.

B.3.3 Applicable HSI (Human System Interface)

The IAEA high-level requirements related to applicable HSI (Human System Interface) are shown in the following table.

Table B.30 IAEA high-level requirements related to applicable HSI (Human System Interface)

IAEA requirement	IAEA Requirement text
Requirement 32: Design for optimal operator performance	Requirement 32: Design for optimal operator performance. Systematic consideration of human factors, including the human–machine interface, shall be included at an early stage in the design process for a nuclear power plant and shall be continued throughout the entire design process. The design shall support operating personnel in the fulfilment of their responsibilities and in the performance of their tasks and shall limit the likelihood and the effects of operating errors on safety. The design process shall give due consideration to plant layout and equipment layout, and to procedures, including procedures for maintenance and inspection, to facilitate interaction between the operating personnel and the plant, in all plant states.

IAEA requirement	IAEA Requirement text
	The human–machine interface shall be designed to provide the operators with comprehensive but easily manageable information, in accordance with the necessary decision times and action times. The information necessary for the operator to make decisions to act shall be simply and unambiguously presented. The operator shall be provided with the necessary information: To assess the general state of the plant in any condition; • To operate the plant within the specified limits on parameters associated with plant systems and equipment (operational limits and conditions); • To confirm that safety actions for the actuation of safety systems are automatically initiated when needed and that the relevant systems perform as intended; • To determine both the need for and the time for manual initiation of the specified safety actions. The design shall be such as to promote the success of operator actions with due regard for the time available for action, the conditions to be expected and the psychological demands being made on the operator. The need for intervention by the operator on a short time scale shall be kept to a minimum, and it shall be demonstrated that the operator has sufficient time to make a decision and sufficient time to act. The design shall be such as to ensure that, following an event affecting the plant, environmental conditions in the control room or the supplementary control room and in locations on the access route to the supplementary control room do not compromise the protection and safety of the operating personnel. The design of workplaces and the working environment of the operating personnel shall be in accordance with ergonomic concepts. Verification and validation, including by the use of simulators, of features relating to human factors shall be included at appropriate stages to confirm that necessary actions by the operator have been identified and can be correctly performed.

The original national requirements related to applicable HSI (Human System Interface) are shown in the following table.

Table B.31 National requirements related to applicable HSI (Human System Interface)

BESEP id	Original requirement text
SE_SSMFS-K_001	The design of a nuclear power reactor must be adapted to human capabilities, so that the risk of incorrect action is as small as possible and reasonable in events and conditions in event class H1-H5 and in scenarios for radiological emergencies, by taking into account performance factors for 1. manual tasks, 2. structures, systems and components, non-installed equipment and the areas and spaces where manual tasks are performed, 3. surrounding physical environment, and 4. organizational conditions.
SE_SSMFS-K_002	A nuclear power reactor must be designed so that the manual tasks that contribute to the completion of the functions given in 4 kap. 2-4 §§

BESEP id	Original requirement text
	SSMFS-K during events and conditions in event class H1-H5 and during scenarios for radiological emergencies can be carried out by 1. there is sufficient time to complete the tasks, 2. there are routines and training for the tasks, 3. relevant information is presented making it possible to read out courses of events and see effects of activations, other operational changes and passive functions so that needs for actions can be identified and actions can be performed, and 4. areas, spaces, structures, systems and components that are necessary to perform tasks are available, accessible, and possible to access with respect to the environmental conditions, strains and other effects that may occur during events and conditions in event class H1-H5.
SE_SSMFS-K_003	A nuclear power reactor's control rooms must be designed and constructed so that their functions that are of significance for the fulfillment of the functions given in 4 kap. 2-4 §§ SSMFS-K and support functions can function together within each control room and between different control rooms. Information and interface must be designed so that the number of different interfaces are as few as possible and reasonable.
SE_SSMFS-K_004	An integrated system validation of the design and construction of the central control room must, in appropriate comprehensiveness, be carried out to ensure that included areas, spaces, structures, systems and components, manual tasks and organizational conditions are working together at intended application.
HU_NSC-118/2011_018	Human reliability analyses shall be performed, considering those aspects that may influence the activities and performance of operating personnel in the different operating conditions of the nuclear power plant unit.
HU_NSC-118/2011_026	Special emergency operating and accident management procedures and actions shall be developed for the event of an earthquake. The organisation of the operation and service of the nuclear power plant, the condition assessment, the scope of inspections following an earthquake, their methods and the conditions of restart shall be regulated in the procedures and action plans.
HU_NSC-118/2011_035	The human-machine relations and ergonomic establishment of systems and system components shall be so designed that, taking into consideration the assumed physical environment and the expected psychical condition, the appropriately trained personnel are able to successfully complete their tasks within the expected period of time if necessary.
HU_NSC-118/2011_036	In order that the members of the operating personnel possess complete information, to the extent corresponding to their positions, which can be efficiently processed in each operating mode of the nuclear power plant, appropriately qualified measuring instruments and traditional or computerised displays shall be placed in the relevant working areas. It shall be provided that the instrumentation enables the measurement of each parameter significant with respect to the reactor core, the reactor cooling systems and the performance of the containment function, the availability of the information necessary for the reliable and safe operation of the nuclear power plant unit, and the automatic recording of measured or derived parameters important in terms of safety.

B.3.4 Team working, effective communication and collaboration

The IAEA high-level requirements related to team working, effective communication and collaboration are shown in the following table.

Table B.32 IAEA high-level requirements related to team working, effective communication and collaboration

IAEA requirement	**IAEA Requirement text**
Requirement 42: Safety analysis of the plant design	Requirement 42: Safety analysis of the plant design. A safety analysis of the design for the nuclear power plant shall be conducted in which methods of both deterministic analysis and probabilistic analysis shall be applied to enable the challenges to safety in the various categories of plant states to be evaluated and assessed. On the basis of a safety analysis, the design basis for items important to safety and their links to initiating events and event sequences shall be confirmed. It shall be demonstrated that the nuclear power plant as designed is capable of complying with authorized limits on discharges with regard to radioactive releases and with the dose limits in all operational states, and is capable of meeting acceptable limits for accident conditions. The safety analysis shall provide assurance that defence in depth has been implemented in the design of the plant. The safety analysis shall provide assurance that uncertainties have been given adequate consideration in the design of the plant and in particular that adequate margins are available to avoid cliff edge effects and early radioactive releases or large radioactive releases. The applicability of the analytical assumptions, methods and degree of conservatism used in the design of the plant shall be updated and verified for the current or as built design. The deterministic safety analysis shall mainly provide: • Establishment and confirmation of the design bases for all items important to safety; • Characterization of the postulated initiating events that are appropriate for the site and the design of the plant; • Analysis and evaluation of event sequences that result from postulated initiating events, to confirm the qualification requirements; • Comparison of the results of the analysis with acceptance criteria, design limits, dose limits and acceptable limits for purposes of radiation protection; • Demonstration that the management of anticipated operational occurrences and design basis accidents is possible by safety actions for the automatic actuation of safety systems in combination with prescribed actions by the operator; • Demonstration that the management of design extension conditions is possible by the automatic actuation of safety systems and the use of safety features in combination with expected actions by the operator. The probabilistic safety analysis of the plant is performed for all modes of operation and for all plant states, including shutdown, with particular reference to: • Establishing that a balanced design has been achieved such that no particular feature or postulated initiating event makes a disproportionately large or significantly uncertain contribution to the overall risks, and that, to the extent practicable, the levels of defence in depth are independent;

IAEA requirement	IAEA Requirement text
	• Providing assurance that situations in which small deviations in plant parameters could give rise to large variations in plant conditions (cliff edge effects) will be prevented; • Comparing the results of the analysis with the acceptance criteria for risk where these have been specified.

The original national requirements related to team working, effective communication and collaboration are shown in the following table.

Table B.33 National requirements related to team working, effective communication and collaboration

BESEP id	Original requirement text
SE_SSMFS-K_001	The design of a nuclear power reactor must be adapted to human capabilities, so that the risk of incorrect action is as small as possible and reasonable in events and conditions in event class H1-H5 and in scenarios for radiological emergencies, by taking into account performance factors for 1. manual tasks, 2. structures, systems and components, non-installed equipment and the areas and spaces where manual tasks are performed, 3. surrounding physical environment, and 4. organizational conditions.
SE_SSMFS-K_002	A nuclear power reactor must be designed so that the manual tasks that contribute to the completion of the functions given in 4 kap. 2-4 §§ SSMFS-K during events and conditions in event class H1-H5 and during scenarios for radiological emergencies can be carried out by 1. there is sufficient time to complete the tasks, 2. there are routines and training for the tasks, 3. relevant information is presented making it possible to read out courses of events and see effects of activations, other operational changes and passive functions so that needs for actions can be identified and actions can be performed, and 4. areas, spaces, structures, systems and components that are necessary to perform tasks are available, accessible, and possible to access with respect to the environmental conditions, strains and other effects that may occur during events and conditions in event class H1-H5.

B.3.5 Workload, stress and fatigue management

The IAEA high-level requirements related to workload, stress and fatigue management are shown in the following table.

Table B.34 IAEA high-level requirements related to workload, stress and fatigue management

IAEA requirement	IAEA Requirement text
Requirement 42: Safety analysis of the plant design	Requirement 42: Safety analysis of the plant design. A safety analysis of the design for the nuclear power plant shall be conducted in which methods of both deterministic analysis and probabilistic analysis shall be applied to enable the challenges to safety in the various categories of plant states to be evaluated and assessed.

IAEA requirement	IAEA Requirement text
	On the basis of a safety analysis, the design basis for items important to safety and their links to initiating events and event sequences shall be confirmed. It shall be demonstrated that the nuclear power plant as designed is capable of complying with authorized limits on discharges with regard to radioactive releases and with the dose limits in all operational states, and is capable of meeting acceptable limits for accident conditions. The safety analysis shall provide assurance that defence in depth has been implemented in the design of the plant. The safety analysis shall provide assurance that uncertainties have been given adequate consideration in the design of the plant and in particular that adequate margins are available to avoid cliff edge effects and early radioactive releases or large radioactive releases. The applicability of the analytical assumptions, methods and degree of conservatism used in the design of the plant shall be updated and verified for the current or as built design. The deterministic safety analysis shall mainly provide: • Establishment and confirmation of the design bases for all items important to safety; • Characterization of the postulated initiating events that are appropriate for the site and the design of the plant; • Analysis and evaluation of event sequences that result from postulated initiating events, to confirm the qualification requirements; • Comparison of the results of the analysis with acceptance criteria, design limits, dose limits and acceptable limits for purposes of radiation protection; • Demonstration that the management of anticipated operational occurrences and design basis accidents is possible by safety actions for the automatic actuation of safety systems in combination with prescribed actions by the operator; • Demonstration that the management of design extension conditions is possible by the automatic actuation of safety systems and the use of safety features in combination with expected actions by the operator. The probabilistic safety analysis of the plant is performed for all modes of operation and for all plant states, including shutdown, with particular reference to: • Establishing that a balanced design has been achieved such that no particular feature or postulated initiating event makes a disproportionately large or significantly uncertain contribution to the overall risks, and that, to the extent practicable, the levels of defence in depth are independent; • Providing assurance that situations in which small deviations in plant parameters could give rise to large variations in plant conditions (cliff edge effects) will be prevented; • Comparing the results of the analysis with the acceptance criteria for risk where these have been specified.

For workload, stress and fatigue management there are no requirements selected to the BESEP requirement base from the national requirements. However, selected NUREG-0711 [28] requirements are used as input for the topic workload, stress and fatigue management. These are shown in the following table.

Table B.35 NUREG requirements related to workload, stress and fatigue management

ID	NUREG requirement text
10.4.3 Learning Objectives	(1) The applicant should derive learning objectives from the analysis describing the desired performance after training. This analysis should include, but not be limited to, the training needs identified in the following: […] • Task Analysis - tasks identified during task analysis as posing unusual demands, including new or different tasks, and tasks requiring a high degree of coordination, high workload, or special skills • Treatment of Important Human Actions – coordinating individual roles to reduce the likelihood and/or consequences of human error associated with important HAs, and the use of advanced technology
10.4.5 Content of Training Program	[…] (4) The applicant's training for performance under degraded conditions should support personnel in: • understanding how and why the I&C subsystems might degrade or fail • knowing the implications of degradations in the HSIs for their own task performance • monitoring the I&C system's performance, so degradations are detected and recognized via the control room's HSIs • performing recovery actions and compensatory actions in the event of a degraded condition, for example through the use of procedures • smoothly transitioning to backup systems when needed • comprehending how the roles and responsibilities of personnel and the concept of use will be impacted
11.4.1.1	(3) The applicant should include the following situational factors or error-forcing contexts known to challenge human performance. It also should include situations specifically designed to create human errors to assess the system's error tolerance, and the ability of personnel to recover from any errors, should these occur, for example: • High-Workload Situations – The sample should include situations where variations in human performance due to high workload and multitasking situations can be assessed. • Varying-Workload Situations – The sample should include situations wherein variations in human performance due to workload transitions can be determined. These include conditions where there is (1) a sudden increase in the number of signals that must be detected and processed after a period in which signals were infrequent, and (2) a rapid reduction in the need for detecting signals and processing demands following a time of high sustained task-demand. • Fatigue Situations – To the extent possible, the sample should include situations that may be associated with fatigue, such as work on backshifts and tasks performed frequently with repetitive actions, such as repeated inputs to a touch screen during plant operations or pulling rods. • Environmental Factors – To the extent possible, the sample should include environmental conditions that may cause human performance to vary, e.g., poor lighting, extreme temperatures, high noise, and simulated radiological contamination.

13.4 Review Criteria	(1) The scope of the applicant's performance monitoring program should provide reasonable assurance that: • personnel can use the design effectively, including within the control room and between the control room, local control stations, and support centers • changes made to the HSIs, procedures, and training do not adversely affect human performance, e.g., they do not interfere with previously trained skills • important human actions can be accomplished within the criteria for time and performance

B.4 Safety engineering practices

B.4.1 Safety engineering management

The IAEA high-level requirement related to adequate design for safety engineering management are shown in the following table

Table B.36 IAEA high-level requirements related to safety engineering management

IAEA requirement	**IAEA Requirement text**
Requirement 1: Responsibilities in the management of safety in plant design	[…] All organizations, including the design organization, engaged in activities important to the safety of the design of a nuclear power plant shall be responsible for ensuring that safety matters are given the highest priority.
Requirement 2: Management system for plant design	The design organization shall establish and implement a management system for ensuring that all safety requirements established for the design of the plant are considered and implemented in all phases of the design process and that they are met in the final design. The management system shall include provision for ensuring the quality of the design of each structure, system and component, as well as of the overall design of the nuclear power plant, at all times. This includes the means for identifying and correcting design deficiencies, for checking the adequacy of the design and for controlling design changes. […]
Requirement 3: Safety of the plant design throughout the lifetime of the plant	The operating organization shall establish a formal system for ensuring the continuing safety of the plant design throughout the lifetime of the nuclear power plant. The formal system for ensuring the continuing safety of the plant design shall include a formally designated entity responsible for the safety of the plant design within the operating organization's management system. Tasks that are assigned to external organizations (referred to as responsible designers) for the design of specific parts of the plant shall be taken into account in the arrangements. The formally designated entity shall ensure that the plant design meets the acceptance criteria for safety, reliability and quality in accordance with relevant national and international codes and standards, laws and

	regulations. A series of tasks and functions shall be established and implemented to ensure the following: […]
Requirement 10: Safety assessment	Comprehensive deterministic safety assessments and probabilistic safety assessments shall be carried out throughout the design process for a nuclear power plant to ensure that all safety requirements on the design of the plant are met throughout all stages of the lifetime of the plant, and to confirm that the design, as delivered, meets requirements for manufacture and for construction, and as built, as operated and as modified. The safety assessments shall be commenced at an early point in the design process, with iterations between design activities and confirmatory analytical activities, and shall increase in scope and level of detail as the design programme progresses. The safety assessments shall be documented in a form that facilitates independent evaluation.

The original national requirements related to safety engineering management are shown in the following table.

Table B.37 National requirements related to safety engineering management

BESEP id	**Original requirement text**
FI_B.1_016	311. A nuclear facility and the systems important to safety shall be designed by using design processes and methods appropriate for the required level of quality, and by applying the relevant safety regulations, guidelines and standards. The selection of the standards applied in design shall be justified in terms of suitability and coverage.
FI_B.1_017	312. The design and implementation of a system important to safety shall be based on a lifecycle model where design and implementation are divided into stages. The life-cycle model shall comprise all successive stages from defining the applicable requirements to the operation stage. In the life-cycle model, the requirements shall be defined before the phase that will be steered by them.
FI_A.3_001	302. In the management system, the organisational structure and the responsibilities, authorities, and decision-making procedures of the personnel shall be defined and their safety implications shall be taken into account and justified. The internal interfaces of the organisation and its interfaces with other organisations shall be described.

B.4.2 Safety design and requirement management for external hazards

The IAEA high-level requirements related to safety design and requirement management for external hazards are shown in the following table.

Table B.38 IAEA high-level requirements related to safety design and requirement management for external hazards

IAEA requirement	**IAEA Requirement text**
Requirement 4: Fundamental safety functions	Fulfilment of the following fundamental safety functions for a nuclear power plant shall be ensured for all plant states: (i) control of reactivity;

IAEA requirement	IAEA Requirement text
	(ii) removal of heat from the reactor and from the fuel store; and (iii) confinement of radioactive material, shielding against radiation and control of planned radioactive releases, as well as limitation of accidental radioactive releases.
Requirement 17: Internal and external hazards	All foreseeable internal hazards and external hazards, including the potential for human induced events directly or indirectly to affect the safety of the nuclear power plant, shall be identified and their effects shall be evaluated. Hazards shall be considered in designing the layout of the plant and in determining the postulated initiating events and generated loadings for use in the design of relevant items important to safety for the plant. [..] External hazards The design shall include due consideration of those natural and human induced external events (i.e., events of origin external to the plant) that have been identified in the site evaluation process. Causation and likelihood shall be considered in postulating potential hazards. In the short term, the safety of the plant shall not be permitted to be dependent on the availability of off-site services such as electricity supply and firefighting services. The design shall take due account of site specific conditions to determine the maximum delay time by which off-site services need to be available. Features shall be provided to minimize any interactions between buildings containing items important to safety (including power cabling and control cabling) and any other plant structure as a result of external events considered in the design. The design of the plant shall provide for an adequate margin to protect items important to safety against levels of external hazards to be considered for design, derived from the hazard evaluation for the site, and to avoid cliff edge effects. […] The design of the plant shall also provide for an adequate margin to protect items ultimately necessary to prevent an early radioactive release or a large radioactive release in the event of levels of natural hazards exceeding those considered for design, derived from the hazard evaluation for the site.
Requirement 41: Interactions between the electric grid and the plant	The functionality of items important to safety at the nuclear power plant shall not be compromised by disturbances in the electrical power grid, including anticipated variations in the voltage and frequency of the grid supply.
Requirement 42: Safety analysis of the plant design	A safety analysis of the design for the nuclear power plant shall be conducted in which methods of both deterministic analysis and probabilistic analysis shall be applied to enable the challenges to safety in the various categories of plant states to be evaluated and assessed. On the basis of a safety analysis, the design basis for items important to safety and their links to initiating events and event sequences shall be confirmed. It shall be demonstrated that the nuclear power plant as designed is capable of complying with authorized limits on discharges with regard to radioactive releases and with the dose limits in all operational states, and is capable of meeting acceptable limits for accident conditions. The safety analysis shall provide assurance that defence in depth has been implemented in the design of the plant. The safety analysis shall provide assurance that uncertainties have been

IAEA requirement	IAEA Requirement text
	given adequate consideration in the design of the plant and in particular that adequate margins are available to avoid cliff edge effects and early radioactive releases or large radioactive releases. The applicability of the analytical assumptions, methods and degree of conservatism used in the design of the plant shall be updated and verified for the current or as built design. The deterministic safety analysis shall mainly provide: • Establishment and confirmation of the design bases for all items important to safety; • Characterization of the postulated initiating events that are appropriate for the site and the design of the plant; • Analysis and evaluation of event sequences that result from postulated initiating events, to confirm the qualification requirements; • Comparison of the results of the analysis with acceptance criteria, design limits, dose limits and acceptable limits for purposes of radiation protection; • Demonstration that the management of anticipated operational occurrences and design basis accidents is possible by safety actions for the automatic actuation of safety systems in combination with prescribed actions by the operator; • Demonstration that the management of design extension conditions is possible by the automatic actuation of safety systems and the use of safety features in combination with expected actions by the operator. The probabilistic safety analysis of the plant is performed for all modes of operation and for all plant states, including shutdown, with particular reference to: • Establishing that a balanced design has been achieved such that no particular feature or postulated initiating event makes a disproportionately large or significantly uncertain contribution to the overall risks, and that, to the extent practicable, the levels of defence in depth are independent; • Providing assurance that situations in which small deviations in plant parameters could give rise to large variations in plant conditions (cliff edge effects) will be prevented; Comparing the results of the analysis with the acceptance criteria for risk where these have been specified.
Requirement 51: Removal of residual heat from the reactor core	Means shall be provided for the removal of residual heat from the reactor core in the shutdown state of the nuclear power plant such that the design limits for fuel, the reactor coolant pressure boundary and structures important to safety are not exceeded.
Requirement 52: Emergency cooling of the reactor core	Means of cooling the reactor core shall be provided to restore and maintain cooling of the fuel under accident conditions at the nuclear power plant, even if the integrity of the pressure boundary of the primary coolant system is not maintained. The means provided for cooling of the reactor core shall be such as to ensure that: • The limiting parameters for the cladding or for integrity of the fuel (such as temperature) will not be exceeded; • Possible chemical reactions are kept to an acceptable level;

IAEA requirement	IAEA Requirement text
	• The effectiveness of the means of cooling of the reactor core compensates for possible changes in the fuel and in the internal geometry of the reactor core; Cooling of the reactor core will be ensured for a sufficient time.
Requirement 53: Heat transfer to an ultimate heat sink	The capability to transfer heat to an ultimate heat sink shall be ensured for all plant states. […] The heat transfer function shall be fulfilled for levels of natural hazards more severe than those considered for design, derived from the hazard evaluation for the site.
Requirement 54: Containment system for the reactor	A containment system shall be provided to ensure, or to contribute to, the fulfilment of the following safety functions at the nuclear power plant: • confinement of radioactive substances in operational states and in accident conditions; • protection of the reactor against natural external events and human induced events; and radiation shielding in operational states and in accident conditions.
Requirement 55: Control of radioactive releases from the containment	The design of the containment shall be such as to ensure that any radioactive release from the nuclear power plant to the environment is as low as reasonably achievable, is below the authorized limits on discharges in operational states and is below acceptable limits in accident conditions.
Requirement 65: Control room	A control room shall be provided at the nuclear power plant from which the plant can be safely operated in all operational states, either automatically or manually, and from which measures can be taken to maintain the plant in a safe state or to bring it back into a safe state after anticipated operational occurrences and accident conditions. Appropriate measures shall be taken, including the provision of barriers between the control room at the nuclear power plant and the external environment, and adequate information shall be provided for the protection of occupants of the control room, for a protracted period of time, against hazards such as high radiation levels resulting from accident conditions, releases of radioactive material, fire, or explosive or toxic gases. Special attention shall be paid to identifying those events, both internal and external to the control room, that could challenge its continued operation, and the design shall provide for reasonably practicable measures to minimize the consequences of such events. The design of the control room shall provide an adequate margin against levels of natural hazards more severe than those considered for design, derived from the hazard evaluation for the site.
Requirement 66: Supplementary control room	Instrumentation and control equipment shall be kept available, preferably at a single location (a supplementary control room) that is physically, electrically and functionally separate from the control room at the nuclear power plant. The supplementary control room shall be so equipped that the reactor can be placed and maintained in a shutdown state, residual heat can be removed, and essential plant variables can be monitored if there is a loss of ability to perform these essential safety functions in the control room. The requirements for taking appropriate measures and providing adequate information for the protection of occupants against hazards also apply for the supplementary control room at the nuclear power plant.

IAEA requirement	IAEA Requirement text
Requirement 68: Design for withstanding the loss of off-site power	The design of the nuclear power plant shall include an emergency power supply capable of supplying the necessary power in anticipated operational occurrences and design basis accidents, in the event of a loss of off-site power. The design shall include an alternate power source to supply the necessary power in design extension conditions. The design specifications for the emergency power supply and for the alternate power source at the nuclear power plant shall include the requirements for capability, availability, duration of the required power supply, capacity and continuity. The combined means to provide emergency power (such as water, steam or gas turbines, diesel engines or batteries) shall have a reliability and type that are consistent with all the requirements of the safety systems to be supplied with power, and their functional capability shall be testable. The design basis for any diesel engine or other prime mover that provides an emergency power supply to items important to safety shall include: • The capability of the associated fuel oil storage and supply systems to satisfy the demand within the specified time period; • The capability to start and to function successfully under all specified conditions and at the required time; Auxiliary systems, such as coolant systems
Requirement 69: Performance of supporting systems and auxiliary systems	The design of supporting systems and auxiliary systems shall be such as to ensure that the performance of these systems is consistent with the safety significance of the system or component that they serve at the nuclear power plant.
Requirement 70: Heat transport systems	Auxiliary systems shall be provided as appropriate to remove heat from systems and components at the nuclear power plant that are required to function in operational states and in accident conditions. The design of heat transport systems shall be such as to ensure that non-essential parts of the systems can be isolated.
Requirement 73: Air conditioning systems and ventilation systems	Systems for air conditioning, air heating, air cooling and ventilation shall be provided as appropriate in auxiliary rooms or other areas at the nuclear power plant to maintain the required environmental conditions for systems and components important to safety in all plant states. Systems shall be provided for the ventilation of buildings at the nuclear power plant with appropriate capability for the cleaning of air: • To prevent unacceptable dispersion of airborne radioactive substances within the plant; • To reduce the concentration of airborne radioactive substances to levels compatible with the need for access by personnel to the area; • To keep the levels of airborne radioactive substances in the plant below authorized limits and as low as reasonably achievable; • To ventilate rooms containing inert gases or noxious gases without impairing the capability to control radioactive effluents; To control gaseous radioactive releases to the environment below the authorized limits on discharges and to keep them as low as reasonably achievable.

The original national requirements related to safety design and requirement management are shown in the following table.

Table B.39 National requirements related to safety design and requirement management

BESEP id	**Original requirement text**
SE_SSMFS-A_001	A nuclear power reactor shall be designed so that the functions that contribute to the completion of the basic functions during events and conditions in event classes H2-H5, if they are completed by structures, systems and components that contribute to the completion of the basic functions during events and conditions in event classes H3-H4B, as far as is practicable 1. are passive, or 2. automatically performs necessary activations and other operational changes.
SE_SSMFS-K_003	A nuclear power reactor's control rooms must be designed and constructed so that their functions that are of significance for the fulfillment of the functions given in 4 kap. 2-4 §§ SSMFS-K and support functions can function together within each control room and between different control rooms. Information and interface must be designed so that the number of different interfaces are as few as possible and reasonable.
SE_SSMFS-K_004	An integrated system validation of the design and construction of the central control room must, in appropriate comprehensiveness, be carried out to ensure that included areas, spaces, structures, systems and components, manual tasks and organizational conditions are working together at intended application.
SK_UJDSR-106/2016_001	(1) The aim of the periodic assessment of internal hazards and external hazards to a nuclear power plant is to assess the adequacy of protection of the nuclear power plant against possible effects of internal and external hazards on the nuclear power plant with regard to the current state of design and operation, current status of selected equipment and other safety-relevant equipment, the site of the nuclear power plant, analytical methods, safety standards and the level of knowledge achieved, as well as with regard to the state expected at the date of the next periodic evaluation.
SK_UJDSR-106/2016_002	(2) The permit holder shall review it by periodic evaluation (a) a list of considered internal hazards and external hazards to the nuclear power plant and their likely combinations that may affect the safety of the nuclear power plant, in particular in case of internal hazards - internal fire and explosions, internal floods, pipeline swings, internal flying objects, load drop, leakage, steam leakage, leakage of the hot or cold gases, vibration, collapse of structures, loss or reduction in the performance of air conditioning equipment; in case of external hazards - external fire, flood, extreme meteorological conditions including the occurrence of a tornado, electromagnetic interference, human activity and industrial activities, including explosions near a nuclear power plant, earthquakes, lightning, biological effects, aircraft impact,
SK_UJDSR-106/2016_003	(2) The permit holder shall review it by periodic evaluation b) determination of the characteristics of probable internal hazards and external hazards to the nuclear power plant, including analytical methods, models, assumptions, criteria and data used for their determination,
SK_UJDSR-106/2016_005	(2) The permit holder shall review it by periodic evaluation d) analyses of the response of a nuclear power plant to internal hazards and external hazards to a nuclear power plant, including an

BESEP id	Original requirement text
	assessment of the mutual impact of several nuclear power plants located in the same territory,
SK_UJDSR-106/2016_006	(2) The permit holder shall review it by periodic evaluation e) the fulfillment of specified safety functions, the suitability of the required interventions of the nuclear power plant operator to prevent the development or mitigation of internal and external hazards to the nuclear power plant, the availability of selected equipment and other safety-relevant equipment, including the operation control room, emergency control room and emergency control center.
SK_UJDSR-430/2011_001	(1) The selected facility shall be designed so that when natural disasters or extreme natural conditions, which may be reasonably anticipated, such as, for example, earthquake, storm, flood, floods, extreme outdoor temperatures, extreme temperature of cooling water, rainfall all forms. humidity, icing, exposure to flora, fauna and the like, or in the event of human - caused events outside the nuclear installation or in a combination thereof, was possible a) safely shut down and maintain the nuclear installation in a subcritical state, b) dissipate residual heat from spent nuclear fuel or radioactive waste, c) keep leakages of radioactive substances below specified values.
SK_UJDSR-430/2011_002	(2) The project is in addition to conditions of physical protection of nuclear facilities and nuclear materials provided special regulation must be taken into account a) the most severe natural phenomena, historically reported in the area of location of nuclear installations and extrapolated with consideration of limited accuracy, if it comes to size and time of the event, b) a combination of the effects of phenomena caused by natural conditions and human activity, c) the maximum anticipated acceleration given for site placement, based on the evaluation of seismic load locations drawn up at placing nuclear installation, defined as seismic level 1 and seismic level 2, d) requirements for seismic resistance of systems, components and building structures of a nuclear installation or their parts, which must correspond to their safety function and expected earthquake effects according to the specified seismic level 1 and seismic level 2, (e) aircraft impacts.
CZ_SUJB-162/2017_004	Periodic safety assessment has to evaluate internal and external hazards from point of view of adequacy of existing resistance of NPP against the hazards, taking into consideration real status of all components, systems and structures impacting nuclear safety and the up-to-date values of probability of occurrence of hazard scenarios obtained from up-date of plant site data, where the NPP is operated. Possible impacts of climate change and changes of human related activities (transport and other industrial activities in plant vicinity), as well as newly adopted measures determined for prevention and mitigation of hazards effects, which are based on defence-in-depth principles, have to be considered.
CZ_BN-JB-2.5_001	Hazards can (similarly to full power operation) significantly contribute to the overall risk of low power and shutdown. They should be analyzed similarly to full power operation, with some exceptions. In the selection of initiating events, differences in lengths of individual plant regimes can be important. The consequences of hazards impact can differ from those specified for full power.
CZ_BN-JB-2.5_004	Level-1 and Level-2 PSA model for both full power and shutdown should be available, which covers full spectrum of possible IEs, including those caused by hazards, when verification that the plant fulfills safety targets and criteria is carried out, with the exception when the safety targets/criteria are defined for the matters covered by

BESEP id	Original requirement text
	reduced scope of PSA, or when alternative approaches are used to confirm that the risk related to the hazards is negligible from point of view of the safety targets and criteria under concern.
CZ_BN-JB-2.5_005	Confirmation of sufficient separation among safety related components, systems and structures endangered by the hazards as fires or floods belongs to the elements of risk oriented decision making employing importance measures enumerated by PSA model.
HU_NSC-118/2011_002	Systems, structures and components that are important to safety shall be designed according to proven standards of nuclear industry. The standards selected for the design process shall be preliminarily defined, their applicability shall be justified.
HU_NSC-118/2011_003	Among the postulated initiating events all those occurrences shall be considered that: a) are related to the site of nuclear power plant and its surroundings and have an environmental origin; b) are intentional, but not purposefully directed against the nuclear power plant, or are the result of unintentional human actions within or outside of the plant site; or c) derive from the operation of the nuclear power plant, or the failure of its systems, structures and components.
HU_NSC-118/2011_004	During the design of the nuclear power plant all possible internal and external hazards shall be determined.
HU_NSC-118/2011_005	The following external hazards shall at least be considered in the design of the nuclear power plant: a) extreme wind load, b) extreme external temperatures, c) extreme precipitation conditions, d) lightning, e) floods, icy floods, summer floods, and low water level, f) the danger of damage to upstream and downstream facilities, g) flying objects moved by wind, h) extreme cooling water temperatures and icing, i) geological characteristics used to justify suitability of the site (in particular earthquake characteristics, and soil liquefaction susceptibility), j) crash of a military or civilian aircraft, k) transport or industrial activities near the plant site, l) disturbances in the connecting external electric grid including total and lasting failure of the electric network, m) such buildings on the site or in the vicinity of the site that may present fire, explosion or other dangers to the plant, n) other fire started off-site, o) electromagnetic interference, and p) biohazards.
HU_NSC-118/2011_006	Among the external hazard factors, those included in the design basis shall be selected on the basis of a site-specific analysis.
HU_NSC-118/2011_007	All realistic combination of the individual occurrences shall be considered during design, including external and internal events, which may lead to DBC4 or DEC plant states. The event combinations to be taken into account in the design shall be selected by taking into account both engineering considerations and probabilistic analyses.
HU_NSC-118/2011_008	For the design, the following can be excluded from the scope of postulated initiating events: a) internal initiating event due to the failure of a system, structure or component, and/or human error, if the frequency of the occurrence is less than 10^{-5}/year; b) event resulting from external human activity typical of the site, if the

BESEP id	Original requirement text
	frequency of the hazard factor is less than 10^{-7}/year, or if the hazard factor is at such a distance, that it can be justified that it will not have an effect on the nuclear power plant unit; and c) initiating events occurring due to a recurring external hazard factor of natural origin, with a frequency of less than 10^{-4}/year, or external hazard factor of natural origin for which it can be demonstrated that they are not able to pose a physical hazard to the power plant.
HU_NSC-118/2011_009	At a power plant site with several nuclear power plant units, for the design of the whole nuclear power plant as well as for the individual nuclear power plant units it shall be considered that some external hazard factor s may affect all nuclear power plant units simultaneously.
HU_NSC-118/2011_011	The stability of, and changes in external factors affecting the nuclear safety of nuclear power plant units shall be forecasted for their whole lifetime.
HU_NSC-118/2011_012	In the selection of events leading to DEC1 plant states, all events or event combinations about which it cannot be established with high certainty that the probability of their occurrence is very low and may lead to conditions that have not been taken into account in the design basis shall be taken into account. In the selection of the events the following should be considered: a) events that occur during the possible operating conditions, b) events that occur for the effect of internal and external hazard factors, c) common cause failures, d) impact of the nuclear facilities in the vicinity, in case of site with multiple units the mutual impacts of the units, and e) those events that may impact all facilities in the vicinity together with the mutual effects assumed among them.
HU_NSC-118/2011_013	The design basis, the extended design basis and their substantiation shall be periodically reviewed at the completion of the design, as well as during the whole lifetime of the nuclear power plant, when significant new safety information is received and based on the results of deterministic and probabilistic calculations or engineering judgement, modifications shall be implemented if necessary. The identified defects and possible safety improvements shall be evaluated and the necessary actions shall be taken in time.
HU_NSC-118/2011_027	A comprehensive strategy shall be prepared to manage the external hazard factors within the design basis, that ensures the compliance with the requirements determined in Section 3.2.1.0900.
HU_NSC-118/2011_028	Regarding each type of hazard factor being characteristic of the site and associated with the natural phenomena and processes in the design basis, the design parameters forming the design input shall be specified on the basis of the hazard curve, taking into account the screening criterion applicable to the given hazard factor. The analysis shall be performed by deterministic methods, and based on the state-of-the-art results of science and technology by probabilistic methods. The analysis shall take into account all available, validated data and, if possible, connections shall be established between the severity of the hazard factors, especially the extent and duration. If it is possible, the maximum, but still justified severity of the hazard factors shall be determined. Design basis design parameters and key properties shall be so specified that they shall ensure the avoidance of the cliff edge effect from the side of design inputs.
HU_NSC-118/2011_029	The safe operation of the nuclear power plant shall also be ensured under circumstances of natural external hazard factors. The reasonably assumable combination of the natural hazard factors shall be taken into account. The effect on the safety functions arising from

BESEP id	Original requirement text
	the failure of systems, structures and system components without safety function due to natural hazard factors shall be taken into consideration.
HU_NSC-118/2011_030	In the case of systems and organisational solutions designed to prevent the effects of external hazard factors, the situation shall be taken into account when access to the site or the service and operation of the systems face permanent difficulties.
HU_NSC-118/2011_031	The comprehensive management strategy shall comply with Sections 3.2.1.2000., 3.2.2.5800. and 3.3.2.3200., and with the following aspects: a) predictability and evolution of the anticipated events in time shall be taken into account, b) appropriate tools and procedures shall be ensured to make it possible that during and after the events taken into account in the design basis the condition of the plant can be confirmed, c) preparations shall be made for such events that affect more units, more systems, structures and components at the same time; in the case of a redundant system it shall be assumed that all trains are affected; effect on the regional infrastructure, off-site services and protective actions shall also be considered, d) in the case of a multiunit nuclear power plant the necessary resources shall be ensured also for such events, where common equipment and services are to be used; this shall not unfavourably influence the protection against the events within the design basis.
HU_NSC-118/2011_032	The potential effects of public road and water transport activities in the vicinity of the nuclear power plant and the risks arising from it shall be analysed, with special regard to the transport of hazardous materials.
HU_NSC-118/2011_034	The parameters of all permanent or temporary facilities that may become the source of fire or explosion shall be identified and determined on the site of the nuclear power plant and in its vicinity, and it shall be evaluated to what extent it poses a hazard to the nuclear power plant. If necessary, appropriate precautionary measures shall be taken.
HU_NSC-118/2011_037	At least one of the technical solutions designed for the removal of the residual heat from the reactor and the spent fuel pool shall fulfil its function also during DEC events caused by external hazard factors.
HU_NSC-118/2011_039	The purpose of the site survey and evaluation shall be the identification of site characteristics that may exclude the construction, the assessment and evaluation of hazard factors relating to the site, and the establishment of data on the site and the nuclear facility, to be taken into account during design: a) for the design of the nuclear facility; b for the analysis of the nuclear safety of the nuclear facility and the effects of potential radioactive discharges; and c) for planning the nuclear emergency response measures and for the assessment of their feasibility.
HU_NSC-118/2011_040	The site survey and evaluation shall be carried out in the following major stages, taking into account the specifications of Annex 3, 3/A, 5 or 6, depending on the type of the nuclear facility: a) hazard factors of natural or human origin shall be identified, which may potentially jeopardise nuclear safety and are to be considered in the design and the safety assessment of the nuclear facilities,; b) the events and conditions that are verifiably not relevant to the nuclear safety of the nuclear facility shall be excluded from further investigation; c) hazard factors of natural or human origin that are not excluded on the basis of paragraph b) and the effects thereof shall be assessed

BESEP id	Original requirement text
	and evaluated; d) the suitability of the site shall be evaluated; and e) the site characteristics to be taken into account during design shall be identified.
HU_NSC-118/2011_041	In the course of the investigation and assessment of the potential site, those possible hazard factors can be excluded from further investigation with appropriate verification, which are at a distance from the plant site that, considering the mitigation effect of such a distance between the location of the hazard factor and the plant site and based on engineering considerations, experience, normative limit value or vulnerability analysis of the nuclear facility, the effect of the hazard factor on the nuclear facility is neutral or tolerable for the nuclear safety functions and for any person staying on the site of the nuclear facility.
HU_NSC-118/2011_042	In the course of the survey and evaluation of the site, probabilistic hazard curves shall be determined for the hazard factors, i.e. the intensity of the hazard factors as a function of frequency. All hazard factors shall be examined from the point of view whether they can trigger a cliff edge effect.
HU_NSC-118/2011_043	The potential and the effect of simultaneous occurrence or the cause-effect occurrence of events and on-site environmental conditions shall be considered in the assessment of the site events. The criterion for the probability screening of individual events, prescribed in Annex 3, 3/A, 5 or 6 depending on the type of the nuclear facility, shall be coherently used in the assessment of the simultaneous occurrence of various external events and conditions.
HU_NSC-118/2011_044	The site and the immediate environment thereof shall be assessed for the potential effects of nuclear facilities or hazardous industrial, agricultural, commercial and military facilities being present in the area independently of the planned nuclear facility. This shall include the facilities, which are in connection with the given nuclear facility, even though their site is separated in legal sense, but their potential effects may reach the planned nuclear facility.
HU_NSC-118/2011_045	The decision whether a given hazard of low probability is relevant for the nuclear safety of the power plant, shall be based on engineering judgement. The screening by distance may take place on the basis of technical assessment, by demonstration that the effect originating from the potential source cannot reach the nuclear power plant. In the absence of very low occurrence probabilities and empirical data, such technical assessments and judgements shall be verified by independent technical experts.
HU_NSC-118/2011_046	In the framework of the assessment specified in Sections 7.3.3 to 7.3.5, the typical values of the wet and dry air temperatures shall be assessed with regard to the availability of the ultimate heat sink medium, and the availability of fresh cooling water, required for maintaining nuclear safety with regard to the volume of water, the minimum water level and the durability of the minimum water level and the water quantity. The occurrence of unfavourable conditions shall also be considered.
FI_Y/1_001	12) design extension condition shall refer to: a) an accident where an anticipated operational occurrence or class 1 postulated accident involves a common cause failure in a system required to execute a safety function; b) an accident caused by a combination of failures identified as significant on the basis of a probabilistic risk assessment; or

BESEP id	Original requirement text
	c) an accident caused by a rare external event which the nuclear facility is required to withstand without severe fuel failure;
FI_Y/1_002	1. Human factors relating to safety shall be controlled with systematic procedures throughout the entire life cycle of the nuclear facility. Human factors shall be taken into account in the design of the nuclear facility and in the planning of its operations, maintenance and decommissioning in a manner that supports the high-quality implementation of the work and ensures that human activities do not endanger plant safety. Attention shall be paid to the avoidance, detection and correction of human errors and the limiting of their effects.
FI_Y/1_004	1. The design of a nuclear facility shall take account of external hazards that may endanger safety. Systems, structures, components and access shall be designed, located and protected so that the impacts of external hazards deemed possible on nuclear facility safety remain minor. The operability of systems, structures and components shall be demonstrated in their design basis external environmental conditions.
FI_B.1_003	414. The nuclear power plant design shall take into account events that may cause a deviation of the plant parameters from normal values and threaten integrity of the nuclear fuel or other barriers. Such events may be caused, for example, by a rupture in pressure equipment or piping; a component failure; a fault in the plant's operation or automatic control; or an internal or external threat.
FI_B.1_015	450a. It shall be possible to carry out the removal of residual heat from the reactor outside the containment in rare external events (DEC C) so that that the limit values set for fuel integrity, radiological consequences and overpressure protection are not exceeded under design extension conditions. Systems needed in the events shall be stationary and meet the self-sufficiency criterion. Measures related to the use of the systems and conducted at the plant site shall not require the use of vehicles during the first eight hours. Components designed for use shall be accessible even if any individual route or hatch were blocked by an external obstacle. It is not necessary to apply the single failure criterion to the arrangements.
FI_B.1_016	455a. It shall be possible to cool the reactor from a controlled state to a safe state and keep it in the safe state on a long-term basis in events involving a combination of failures (DEC B) and rare external events (DEC C). It is not necessary to apply the single failure criterion to the required systems.
FI_B.7_010	428. The licence applicant shall demonstrate that seismic category S1 and S2A structures and components meet the requirements for earthquake resistance established in chapter 4.2. Demonstration may be in the form of analyses, tests, up-to-date empirical assessments or combinations thereof. Such demonstrations or corresponding result documentation are to be presented in connection with STUK's inspections required for the types of structure or component in question before commissioning. The specification of a seismic category-dependent requirement level for the functionality and integrity of systems, structures and components is discussed in Guide YVL B.2. Analyses and experimental methods are addressed in more detail in the Guide IAEA SG NS-G-1.6.
FI_B.7_011	428a. Earthquakes stronger than the design basis earthquake shall be considered design extension conditions (DEC C) in accordance with Guide YVL B.1. This can be done using the seismic fragility curves of equipment needed for bringing the plant to a safe state.

BESEP id	Original requirement text
FI_B.7_013	438. The nuclear power plant's safe shutdown after an earthquake shall be based on unambiguous procedures. The pre-shutdown vibration acceleration level and the method of its establishment are presented in the procedures. Shutdown procedures shall be based on appropriately qualified category S1 systems, structures and components.
FI_B.7_014	438a. The nuclear facility shall have instructions describing the inspections and other measures to be carried out after an earthquake, their dependency on the intensity of the earthquake (acceleration levels at the site) and the conditions for continued operation after the earthquake.
FI_B.7_017	443. The scope and implementation of the seismic design of structures and components shall be ensured by facility walkdowns prior to the nuclear facility's commissioning. The inspections shall be carried out by competent technical experts and under STUK's oversight. Experts participating in the facility walkdowns shall acquaint themselves with the seismic design documents. The facility walkdowns include verification of the appropriateness of seismic support and fixing solutions as well as identification and assessment of potential seismic risk factors requiring further measures.
FI_B.7_018	443a. The need for a walkdown and its necessary extent shall be assessed. If necessary, the walkdown shall also be carried out after extensive modifications and in connection with the periodic safety review, the seismic PRA and its updates.
FI_B.7_019	444. A plan for facility walkdowns shall be drawn up. Approved construction plans as well as the seismic PRA and fragilities shall be taken into account in the planning, among other documents and information. A facility walkdown report shall be drawn up describing walkdown implementation and any detected non-conformances detected affecting safety.
FI_B.7_020	503. The following general principles shall be followed in selecting design values for systems, structures and components important to safety that pertain to external events and conditions: a. Design values shall include an adequate margin in relation to the peak values measured at the facility site and in its vicinity. b. In determining design values, at least phenomena whose estimated probability of occurrence at the site over one year is higher than 10-5 at a median confidence level shall be considered. c. If it can be reliably demonstrated that an external event or condition does not affect the probability of occurrence of a certain postulated accident, the design value regarding the external event or condition in question can be chosen for the systems required for the management of the postulated accident so that its maximum probability of exceedance in one year is 10-4. d. The safety significance of systems, structures and components important to safety shall be considered in selecting their design values, and the adequacy of the design values shall be justified.
FI_B.7_021	504. In addition to the above, to be ensured in selecting the sea water level design value is that the design value is higher than a. the water level estimated possible at the site at a median confidence level once in a hundred years added with two metres and a site-specifically evaluated wave margin, and b. the extreme level equivalent to the least favourable combination of factors evaluated in accordance with requirement 515 added with a site-specifically evaluated wave margin.
FI_B.7_022	505. To be taken into account in selecting design values as well as in applying the redundancy and separation principles (YVL B.1) are

BESEP id	Original requirement text
	dependencies affecting the simultaneous occurrence of external events. A hazard arising from unlawful action need not be taken into account as a load simultaneously with external hazards caused by exceptional natural phenomena or regular human activities.
FI_B.7_023	506. Exceptional external events and conditions with an estimated frequency of occurrence less than 10-5/year shall be considered design extension conditions (DEC C events). The licence applicant/licensee shall present and justify external phenomena considered as DEC C events. In selecting the phenomena and their magnitude, the limit values for core damage and large release frequency presented in Guide YVL A.7 shall be taken into account. To be incorporated in the DEC C design values is a justified marginal in relation to the observed maximum values of the phenomena analysed.
FI_B.7_025	507a. The nuclear facility shall have instructions describing the inspections and other measures to be carried out after exceptional weather phenomena and other external events that affect safety and the conditions for continued operation.
FI_B.7_029	512. The design of the nuclear facility shall take into consideration the exceptional meteorological phenomena and comparable natural phenomena assessed as possible at the facility site. At least the following phenomena shall be considered in the design: * high and low atmospheric temperature * high winds including tornadoes and downbursts * high and low air pressure as well as fluctuations of air pressure * rain, snow, hail * freezing rain and splashes from sea or watercourses * atmospheric moisture, fog, mist, rime ice * lightning * drought * electromagnetic interference caused by solar flares.
FI_B.7_030	513. Design solutions shall ensure that freezing, snow or other events causing clogging do not prevent cooling air supply to systems important to safety or combustion air supply to emergency power engines.
FI_B.7_031	515. Hazard curves in accordance with chapter 5.2 shall be drawn up for high and low sea water levels. In addition to a statistical approach, factors affecting sea water level shall be specified, and the maximum impact of every identified factor shall be evaluated, along with the extreme level corresponding to the least favourable combination of factors. As factors affecting sea water level, at least the total volume of water in the Baltic Sea, air pressure, wind, seiche and tide shall be examined. The analysis shall include the estimated change in the water level of oceans and the uncertainties arising from it during the nuclear facility's design lifetime.
FI_B.7_032	519. The hazard posed by the blockage of sea water intakes by frazil ice and other forms of ice shall be evaluated and reduced as far as possible by appropriate design solutions. The solutions chosen shall be presented and their adequacy justified in the Preliminary and Final Safety Analysis Reports.
FI_B.7_033	520. The nuclear facility's sea water systems shall be equipped with suitable temperature measurements to identify the hazard posed by frazil ice. During the nuclear facility's operation, the sea water freezing point shall be determined at regular intervals under conditions favourable for the formation of frazil ice (low atmospheric temperature and sea without ice cover).

B.4.3 Flow of information between safety analyses

The IAEA high-level requirements related to flow of information between safety analysis are shown in the following table.

Table B.40 IAEA high-level requirements related to flow of information between safety analysis

IAEA requirement	**IAEA Requirement text**
Requirement 42: Safety analysis of the plant design	A safety analysis of the design for the nuclear power plant shall be conducted in which methods of both deterministic analysis and probabilistic analysis shall be applied to enable the challenges to safety in the various categories of plant states to be evaluated and assessed. On the basis of a safety analysis, the design basis for items important to safety and their links to initiating events and event sequences shall be confirmed. It shall be demonstrated that the nuclear power plant as designed is capable of complying with authorized limits on discharges with regard to radioactive releases and with the dose limits in all operational states, and is capable of meeting acceptable limits for accident conditions. The safety analysis shall provide assurance that defence in depth has been implemented in the design of the plant. The safety analysis shall provide assurance that uncertainties have been given adequate consideration in the design of the plant and in particular that adequate margins are available to avoid cliff edge effects and early radioactive releases or large radioactive releases. The applicability of the analytical assumptions, methods and degree of conservatism used in the design of the plant shall be updated and verified for the current or as built design. The deterministic safety analysis shall mainly provide: • Establishment and confirmation of the design bases for all items important to safety; • Characterization of the postulated initiating events that are appropriate for the site and the design of the plant; • Analysis and evaluation of event sequences that result from postulated initiating events, to confirm the qualification requirements; • Comparison of the results of the analysis with acceptance criteria, design limits, dose limits and acceptable limits for purposes of radiation protection; • Demonstration that the management of anticipated operational occurrences and design basis accidents is possible by safety actions for the automatic actuation of safety systems in combination with prescribed actions by the operator; • Demonstration that the management of design extension conditions is possible by the automatic actuation of safety systems and the use of safety features in combination with expected actions by the operator. The probabilistic safety analysis of the plant is performed for all modes of operation and for all plant states, including shutdown, with particular reference to: • Establishing that a balanced design has been achieved such that no particular feature or postulated initiating event makes a disproportionately large or significantly uncertain contribution to the overall risks, and that, to the extent practicable, the levels of defence in depth are independent;

IAEA requirement	IAEA Requirement text
	• Providing assurance that situations in which small deviations in plant parameters could give rise to large variations in plant conditions (cliff edge effects) will be prevented; • Comparing the results of the analysis with the acceptance criteria for risk where these have been specified.

The original national requirements related to flow of information between safety analysis are shown in the following table.

Table B.41 National requirements related to flow of information between safety analysis

BESEP id	Original requirement text
CZ_BN-JB-2.5_004	Level-1 and Level-2 PSA model for both full power and shutdown should be available, which covers full spectrum of possible IEs, including those caused by hazards, when verification that the plant fulfills safety targets and criteria is carried out, with the exception when the safety targets/criteria are defined for the matters covered by reduced scope of PSA, or when alternative approaches are used to confirm that the risk related to the hazards is negligible from point of view of the safety targets and criteria under concern.
FI_B.7_010	428. The licence applicant shall demonstrate that seismic category S1 and S2A structures and components meet the requirements for earthquake resistance established in chapter 4.2. Demonstration may be in the form of analyses, tests, up-to-date empirical assessments or combinations thereof. Such demonstrations or corresponding result documentation are to be presented in connection with STUK's inspections required for the types of structure or component in question before commissioning. The specification of a seismic category-dependent requirement level for the functionality and integrity of systems, structures and components is discussed in Guide YVL B.2. Analyses and experimental methods are addressed in more detail in the Guide IAEA SG NS-G-1.6 [9].

B.4.4 Verification and validation (V&V) of design

The IAEA high-level requirements related to verification and validation (V&V) of design are shown in the following table.

Table B.42 IAEA high-level requirements related to verification and validation (V&V) of design

IAEA requirement	IAEA Requirement text
Requirement 42: Safety analysis of the plant design	A safety analysis of the design for the nuclear power plant shall be conducted in which methods of both deterministic analysis and probabilistic analysis shall be applied to enable the challenges to safety in the various categories of plant states to be evaluated and assessed. On the basis of a safety analysis, the design basis for items important to safety and their links to initiating events and event sequences shall be confirmed. It shall be demonstrated that the nuclear power plant as designed is capable of complying with authorized limits on discharges with regard to radioactive releases and with the dose limits in all

IAEA requirement	IAEA Requirement text
	operational states, and is capable of meeting acceptable limits for accident conditions. The safety analysis shall provide assurance that defence in depth has been implemented in the design of the plant. The safety analysis shall provide assurance that uncertainties have been given adequate consideration in the design of the plant and in particular that adequate margins are available to avoid cliff edge effects and early radioactive releases or large radioactive releases. The applicability of the analytical assumptions, methods and degree of conservatism used in the design of the plant shall be updated and verified for the current or as built design. The deterministic safety analysis shall mainly provide: • Establishment and confirmation of the design bases for all items important to safety; • Characterization of the postulated initiating events that are appropriate for the site and the design of the plant; • Analysis and evaluation of event sequences that result from postulated initiating events, to confirm the qualification requirements; • Comparison of the results of the analysis with acceptance criteria, design limits, dose limits and acceptable limits for purposes of radiation protection; • Demonstration that the management of anticipated operational occurrences and design basis accidents is possible by safety actions for the automatic actuation of safety systems in combination with prescribed actions by the operator; • Demonstration that the management of design extension conditions is possible by the automatic actuation of safety systems and the use of safety features in combination with expected actions by the operator. The probabilistic safety analysis of the plant is performed for all modes of operation and for all plant states, including shutdown, with particular reference to: • Establishing that a balanced design has been achieved such that no particular feature or postulated initiating event makes a disproportionately large or significantly uncertain contribution to the overall risks, and that, to the extent practicable, the levels of defence in depth are independent; • Providing assurance that situations in which small deviations in plant parameters could give rise to large variations in plant conditions (cliff edge effects) will be prevented; • Comparing the results of the analysis with the acceptance criteria for risk where these have been specified.
Requirement 52: Emergency cooling of the reactor core	Means of cooling the reactor core shall be provided to restore and maintain cooling of the fuel under accident conditions at the nuclear power plant, even if the integrity of the pressure boundary of the primary coolant system is not maintained. The means provided for cooling of the reactor core shall be such as to ensure that: • The limiting parameters for the cladding or for integrity of the fuel (such as temperature) will not be exceeded; • Possible chemical reactions are kept to an acceptable level;

IAEA requirement	IAEA Requirement text
	• The effectiveness of the means of cooling of the reactor core compensates for possible changes in the fuel and in the internal geometry of the reactor core; • Cooling of the reactor core will be ensured for a sufficient time.
Requirement 55: Control of radioactive releases from the containment	The design of the containment shall be such as to ensure that any radioactive release from the nuclear power plant to the environment is as low as reasonably achievable, is below the authorized limits on discharges in operational states and is below acceptable limits in accident conditions.

The original national requirements related to verification and validation (V&V) of design are shown in the following table.

Table B.43 National requirements related to verification and validation (V&V) of design

BESEP id	Original requirement text
SE_SSMFS-K_004	An integrated system validation of the design and construction of the central control room must, in appropriate comprehensiveness, be carried out to ensure that included areas, spaces, structures, systems and components, manual tasks and organizational conditions are working together at intended application.
SE_SSMFS-A_008	The assessments on the influence on the condition of the radiation sources must be carried out for events and conditions in event classes H2-H5. The assessments must either prove that the radiation sources' condition are not affected or determine which conditions will apply during the assessment of the continued course of events according to 10 §.
SE_SSMFS-A_009	The assessments of the continued course of events which follows after the affection of a radiation source's condition must be performed for events and conditions in event classes H2-H5 with respect to the conditions that have been determined to apply according to 9 § second paragraph. The assessments must demonstrate 1. that the nuclear power reactor is returned to operation within the specified terms and limitations for normal operation as far as is practicable without the reactor protection system being initiated during events and conditions in event class H2, and 2. that the nuclear power reactor achieves a safe state during events and conditions in event classes H2-H5 and that the technical acceptance criteria regarding the affection on the barriers for the radiation sources are met. The technical acceptance criteria that are applied must be motivated and well constructed.
SE_SSMFS-K_005	A nuclear power reactor must be designed and constructed so that the events and conditions that are of importance for the radiation safety and that directly or indirectly are assumed to in a negative way affect the exposure of workers, the general public or the environment for ionized radiation or are assumed to be able to lead to illegal possession of radioactive substances (postulated events and conditions of importance for the radiation safety) can be prevented and taken care of. The postulated events and conditions referred to in the first paragraph must

BESEP id	Original requirement text
	1. be identified with respect to the categories of events and conditions that are of importance for the radiation safety which is presented in appendix 1, SSMFS-K, 2. be divided into these event classes, or similar, a. normal events and conditions (H1), b. expected events and conditions (H2), c. not expected events and conditions (H3), d. improbable events and conditions (H4A), e. special events and conditions (H4B), f. very improbable events and conditions (H5), g. extremely improbable events and conditions (H6), and 3. form the basis for specification of scenarios for radiological emergencies.
SE_SSMFS-A_010	The probabilistic safety analyses must take the events and conditions that are identified in accordance with 3 kap. 1 § SSMFS-K into account. The probabilistic safety analyses must refer to 1. the occurrence rate of damage to nuclear fuel assemblies (level 1), and 2. the occurrence rate of release of radiological substances to the environment as a consequence of the damage to the nuclear fuel assemblies (level 2). The probabilistic safety analyses do not have to take into account such events and conditions according to the first paragraph not considered relevant for the application of the analysis.
SK_UJDSR-106/2016_005	(2) The permit holder shall review it by periodic evaluation d) analyses of the response of a nuclear power plant to internal hazards and external hazards to a nuclear power plant, including an assessment of the mutual impact of several nuclear power plants located in the same territory,
SK_UJDSR-106/2016_006	(2) The permit holder shall review it by periodic evaluation e) the fulfillment of specified safety functions, the suitability of the required interventions of the nuclear power plant operator to prevent the development or mitigation of internal and external hazards to the nuclear power plant, the availability of selected equipment and other safety-relevant equipment, including the operation control room, emergency control room and emergency control center.
SK_UJDSR-430/2011_001	(1) The selected facility shall be designed so that when natural disasters or extreme natural conditions, which may be reasonably anticipated, such as, for example, earthquake, storm, flood, floods, extreme outdoor temperatures, extreme temperature of cooling water, rainfall all forms. humidity, icing, exposure to flora, fauna and the like, or in the event of human - caused events outside the nuclear installation or in a combination thereof, was possible a) safely shut down and maintain the nuclear installation in a subcritical state, b) dissipate residual heat from spent nuclear fuel or radioactive waste, c) keep leakages of radioactive substances below specified values.
CZ_BN-JB-2.5_004	Level-1 and Level-2 PSA model for both full power and shutdown should be available, which covers full spectrum of possible IEs, including those caused by hazards, when verification that the plant fulfills safety targets and criteria is carried out, with the exception when the safety targets/criteria are defined for the matters covered by reduced scope of PSA, or when alternative approaches are used to confirm that the risk related to the hazards is negligible from point of view of the safety targets and criteria under concern.
FI_A.6_001	717. The procedures and guidelines shall be systematically validated and verified. Validation shall also address the role of human factors in

BESEP id	Original requirement text
	the procedures. The validation of the procedures and guidelines shall be based on simulations or other suitable methods, primarily by using a training simulator.
FI_B.1_014	447. In events involving a combination of failures (DEC B) and in rare external events (DEC C), it shall be possible to shut down the reactor and keep it subcritical in a controlled state in such a way that the limits set forth for fuel integrity, radiological consequences and overpressure protection in design extension conditions are not exceeded.
FI_B.1_015	450a. It shall be possible to carry out the removal of residual heat from the reactor outside the containment in rare external events (DEC C) so that that the limit values set for fuel integrity, radiological consequences and overpressure protection are not exceeded under design extension conditions. Systems needed in the events shall be stationary and meet the self-sufficiency criterion. Measures related to the use of the systems and conducted at the plant site shall not require the use of vehicles during the first eight hours. Components designed for use shall be accessible even if any individual route or hatch were blocked by an external obstacle. It is not necessary to apply the single failure criterion to the arrangements.
FI_B.1_016	455a. It shall be possible to cool the reactor from a controlled state to a safe state and keep it in the safe state on a long-term basis in events involving a combination of failures (DEC B) and rare external events (DEC C). It is not necessary to apply the single failure criterion to the required systems.
FI_B.7_010	428. The licence applicant shall demonstrate that seismic category S1 and S2A structures and components meet the requirements for earthquake resistance established in chapter 4.2. Demonstration may be in the form of analyses, tests, up-to-date empirical assessments or combinations thereof. Such demonstrations or corresponding result documentation are to be presented in connection with STUK's inspections required for the types of structure or component in question before commissioning. The specification of a seismic category-dependent requirement level for the functionality and integrity of systems, structures and components is discussed in Guide YVL B.2. Analyses and experimental methods are addressed in more detail in the Guide IAEA SG NS-G-1.6 [9].
FI_B.7_011	428a. Earthquakes stronger than the design basis earthquake shall be considered design extension conditions (DEC C) in accordance with Guide YVL B.1. This can be done using the seismic fragility curves of equipment needed for bringing the plant to a safe state.
FI_B.7_013	438. The nuclear power plant's safe shutdown after an earthquake shall be based on unambiguous procedures. The pre-shutdown vibration acceleration level and the method of its establishment are presented in the procedures. Shutdown procedures shall be based on appropriately qualified category S1 systems, structures and components.

B.4.5 System modification and configuration management

For this requirement topic there are no high-level IAEA requirements.

The original national requirements related to system modification and configuration management are shown in the following table.

Table B.44 National requirements related to system modification and configuration management

BESEP id	Original requirement text
FI_B.1_001	305. The licensee shall maintain detailed design documentation to be able to ensure the design integrity and safety of the facility over its entire service life, including the planning of modifications and component replacements.
FI_B.1_002	324. Configuration management procedures shall be applied to configuration units and their documentation, including documentation related to verification and validation, throughout the configuration units' life cycle.

B.4.6 Validated modelling and simulation analysis tools

The IAEA high-level requirements related to validated modelling and simulation analysis tools are shown in the following table.

Table B.45 IAEA high-level requirements related to validated modelling and simulation analysis tools

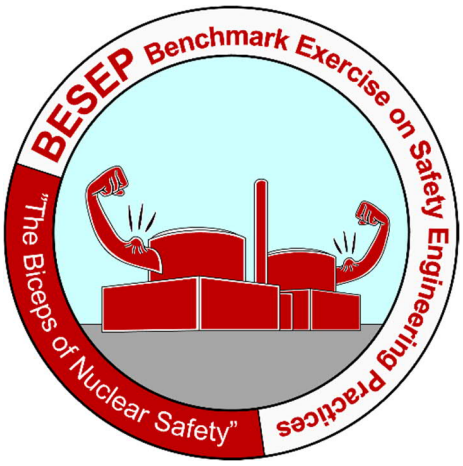
IAEA requirement	IAEA Requirement text
Requirement 42: Safety analysis of the plant design	A safety analysis of the design for the nuclear power plant shall be conducted in which methods of both deterministic analysis and probabilistic analysis shall be applied to enable the challenges to safety in the various categories of plant states to be evaluated and assessed. On the basis of a safety analysis, the design basis for items important to safety and their links to initiating events and event sequences shall be confirmed. It shall be demonstrated that the nuclear power plant as designed is capable of complying with authorized limits on discharges with regard to radioactive releases and with the dose limits in all operational states, and is capable of meeting acceptable limits for accident conditions. The safety analysis shall provide assurance that defence in depth has been implemented in the design of the plant. The safety analysis shall provide assurance that uncertainties have been given adequate consideration in the design of the plant and in particular that adequate margins are available to avoid cliff edge effects and early radioactive releases or large radioactive releases. The applicability of the analytical assumptions, methods and degree of conservatism used in the design of the plant shall be updated and verified for the current or as built design. […]

The original national requirements related to validated modelling and simulation analysis tools are shown in the following table.

Table B.46 National requirements related to validated modelling and simulation analysis tools

BESEP id	Original requirement text
SK_UJDSR-106/2016_003	(2) The permit holder shall review it by periodic evaluation b) determination of the characteristics of probable internal hazards and external hazards to the nuclear power plant, including analytical

BESEP id	Original requirement text
	methods, models, assumptions, criteria and data used for their determination,
FI_B.3_001	404. A description of the models and calculation methods employed in the analyses shall be presented. The models shall be described to a level of precision that allows for verifying the correctness of the model in relation to the plant design as well as assessing the applicability of the selected modelling solutions. The information presented in the description shall include an analysis model that describes the facility or a part thereof (such as the nodal distribution used in the model), a justification for the model parameters selected and the plant data used in the analyses or a reference to a source from where the plant data is available.
FI_B.3_002	405. The validation of the physical models and computer code used for the analyses shall be substantiated by comparing their calculation results to separate effects tests or tests carried out on entire systems, or to disturbances that have occurred at nuclear power plants. Comparison with models that have already been validated may also be utilised.



BESEP

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 945138.