Deliverable 2.1
Results on the assignment of safety requirement topics
February 2021
Version 1.2

Public

Z. Kovacs
RELKO spol. s r.o
Račianska 75, P.O.Box 98, 830 08 Bratislava
Slovak Republic
kovacs@relko.sk
Abstract
WP2 establishes a common starting point for the benchmark exercise in frame of BESEP project. It defines the external hazards, safety analysis methods, SSCs and a set of requirements involved in the comparison and evaluation of safety engineering processes used by the project partners.

The subtask WP2.1 is focused on identification of the external hazards and important safety requirement topics of interest in the benchmark exercise.

In the beginning, the report briefly describes the deterministic and probabilistic safety analyses for external hazards. The human factors engineering is also described. The described methods can be used to demonstrate that the plant is able to withstand the loading of external hazards. The safety margin is calculated. It is the level of a hazard that compromises the safety of a nuclear power plant. The compromising of safety means that the plant is rendered incapable of achieving safety objectives under the impact of the hazard.

At first, an overview of external hazards and their combinations is given which are involved in the safety assessment of BESEP partner countries. Then, the outlines of case studies, collected to the preliminary pool of case studies in preparing phase of the project, are used for the identification of external hazards. Several safety requirement topics were assigned to each external hazard using the recommended list of IAEA safety requirements.
**HISTORY OF CHANGES**

<table>
<thead>
<tr>
<th>Date</th>
<th>Version</th>
<th>Author</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.2.2021</td>
<td>1.0</td>
<td>Z. Kovacs</td>
<td>Original version</td>
</tr>
<tr>
<td>11.2.2021</td>
<td>1.1</td>
<td>J. Linnosmaa</td>
<td>Updated document template</td>
</tr>
<tr>
<td>24.2.2021</td>
<td>1.2</td>
<td>Z. Kovacs</td>
<td>Implementation of DRF comments</td>
</tr>
</tbody>
</table>
# List of Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ALARA</td>
<td>As Low As Reasonably Achievable</td>
</tr>
<tr>
<td>APC</td>
<td>Atmospheric Pressure Change</td>
</tr>
<tr>
<td>BESEP</td>
<td>Benchmark Exercise on Safety Engineering Practices</td>
</tr>
<tr>
<td>CDF</td>
<td>Core Damage Frequency</td>
</tr>
<tr>
<td>DID</td>
<td>Defence-in-Depth</td>
</tr>
<tr>
<td>DSA</td>
<td>Deterministic Safety Analyses</td>
</tr>
<tr>
<td>DSHA</td>
<td>Deterministic Seismic Hazard Analyses</td>
</tr>
<tr>
<td>EPRI</td>
<td>Electric Power Research Institute</td>
</tr>
<tr>
<td>EME</td>
<td>Emergency Management Equipment Guidance</td>
</tr>
<tr>
<td>EU</td>
<td>European Union</td>
</tr>
<tr>
<td>FLEX</td>
<td>Flexible Mitigation Strategies</td>
</tr>
<tr>
<td>HCLPF</td>
<td>High Confidence of Low Probability of Failure</td>
</tr>
<tr>
<td>HFE</td>
<td>Human Factors Engineering</td>
</tr>
<tr>
<td>HRA</td>
<td>Human reliability analysis</td>
</tr>
<tr>
<td>IAEA</td>
<td>International Atomic Energy Agency</td>
</tr>
<tr>
<td>IRS</td>
<td>Incident Reporting System</td>
</tr>
<tr>
<td>LERF</td>
<td>Large Early Release Frequency</td>
</tr>
<tr>
<td>LRF</td>
<td>Large Release Frequency</td>
</tr>
<tr>
<td>NEA</td>
<td>Nuclear Energy Agency</td>
</tr>
<tr>
<td>NPP</td>
<td>Nuclear Power Plant</td>
</tr>
<tr>
<td>NRC</td>
<td>U.S. Nuclear Regulatory Commission</td>
</tr>
<tr>
<td>OECD</td>
<td>Organization for Economic Cooperation and Development</td>
</tr>
<tr>
<td>PGA</td>
<td>Peak Ground Acceleration</td>
</tr>
<tr>
<td>PSA</td>
<td>Probabilistic Safety Assessment</td>
</tr>
<tr>
<td>PSHA</td>
<td>Probabilistic Seismic Hazard Analyses</td>
</tr>
<tr>
<td>QA</td>
<td>Quality Assurance</td>
</tr>
<tr>
<td>RLE</td>
<td>Review Level Earthquake</td>
</tr>
<tr>
<td>SEP</td>
<td>Safety Engineering Process</td>
</tr>
<tr>
<td>SMA</td>
<td>Safety (Seismic) Margin Analyses</td>
</tr>
<tr>
<td>SSC</td>
<td>Structure, System and Component</td>
</tr>
<tr>
<td>UHS</td>
<td>Ultimate Heat Sink</td>
</tr>
<tr>
<td>WP</td>
<td>Work Package</td>
</tr>
</tbody>
</table>
# Table of Contents

**History of Changes** .......................................................................................................................... 3

**List of Abbreviations** .......................................................................................................................... 4

**List of Figures** ..................................................................................................................................... 7

**List of Tables** ....................................................................................................................................... 7

1 **Introduction** ..................................................................................................................................... 8

2 **Deterministic Safety Analyses for External Hazards** ..................................................................... 9
   2.1 Deterministic safety analyses of seismic hazard .............................................................................. 9
      2.1.1 Deterministic seismic hazard analyses ......................................................................................... 9
      2.1.2 Deterministic seismic fragility analyses ....................................................................................... 10
      2.1.3 Deterministic seismic margin analyses ....................................................................................... 10
   2.2 Deterministic analyses of non-seismic natural hazards ................................................................. 11
      2.2.1 Deterministic non-seismic natural hazard analyses .................................................................... 12
      2.2.2 Deterministic non-seismic fragility analyses ............................................................................... 12
      2.2.3 Deterministic non-seismic safety margin analyses ..................................................................... 13
   2.3 Deterministic analyses of human-induced external hazards ....................................................... 13

3 **Probabilistic Safety Analyses for External Hazards** .................................................................... 13
   3.1 Key elements of PSA for external hazards ....................................................................................... 14
   3.2 Seismic PSA .................................................................................................................................... 14
      3.2.1 Probabilistic seismic hazard analyses ......................................................................................... 14
      3.2.2 Probabilistic seismic fragility analyses ....................................................................................... 15
      3.2.3 Plant response and accident sequence analyses for seismic hazard ........................................... 16
   3.3 PSA of non-seismic natural hazards ................................................................................................ 18
      3.3.1 Probabilistic non-seismic hazard analyses ................................................................................. 18
      3.3.2 Probabilistic non-seismic fragility analyses ............................................................................... 19
      3.3.3 Plant response and accident sequence analyses for non-seismic hazards ............................... 20
   3.4 PSA of human-induced hazards ....................................................................................................... 20
   3.5 Evaluation of consequences ............................................................................................................ 21

4 **Human Factors Engineering** ......................................................................................................... 24
   4.1 Human factors engineering applied for plant design and operation ............................................ 24
   4.2 Plant procedures ............................................................................................................................... 25
   4.3 Education and training .................................................................................................................... 26
   4.4 Experience with simulator training .................................................................................................. 26
   4.5 Human error data collection ............................................................................................................ 26
   4.6 Information feedback ....................................................................................................................... 27
   4.7 Operator support systems ............................................................................................................... 27
   4.8 PSA information for safety decisions ............................................................................................ 27
   4.9 International co-operation .............................................................................................................. 28
5 SELECTED EXTERNAL HAZARDS FOR BESEP .......................................................... 28
  5.1 External hazards in the safety assessments of BESEP partner countries ..........29
  5.2 External hazards in the preliminary case studies .......................................... 32
  5.3 External hazards not involved in the case studies ........................................... 33
6 COMBINATIONS OF EXTERNAL HAZARDS ................................................................. 33
  6.1 Combinations of external hazards in the safety assessments of partner countries ...34
  6.2 Selection of external hazard combinations from the preliminary case studies ...... 36
7 ASSIGNMENT OF SAFETY REQUIREMENT TOPICS TO EXTERNAL HAZARDS .... 37
  7.1 Overview of the IAEA safety requirements .................................................... 40
      7.1.1 Management of safety in design ................................................................. 40
      7.1.2 Principal technical safety requirements ...................................................... 40
      7.1.3 General plant design ................................................................................ 41
      7.1.4 Design of specific plant systems ............................................................... 42
  7.2 Assignment of safety requirement topics ....................................................... 43
  7.3 Extreme winds ............................................................................................... 46
      7.3.1 Extreme wind hazard analyses ................................................................. 46
      7.3.2 Extreme wind fragility analyses ............................................................... 47
      7.3.3 Plant response analyses to extreme wind ............................................... 47
  7.4 Tornado ........................................................................................................... 47
      7.4.1 Tornado hazard analyses ......................................................................... 48
      7.4.2 Tornado fragility analyses ...................................................................... 48
      7.4.3 Plant response analyses to tornado ......................................................... 49
  7.5 Extreme snow ............................................................................................... 49
      7.5.1 Extreme snow hazard analyses ............................................................... 49
      7.5.2 Extreme snow fragility analyses .............................................................. 49
      7.5.3 Plant response analyses to extreme snow .............................................. 50
  7.6 Extreme rain ................................................................................................ 50
      7.6.1 Extreme rain hazard analyses ............................................................... 51
      7.6.2 Extreme rain fragility analyses ............................................................... 51
      7.6.3 Plant response analyses to extreme rain ................................................. 51
  7.7 Extremely high/low temperature ................................................................. 52
      7.7.1 Extremely high/low temperature hazard analyses .................................. 52
      7.7.2 Extremely high/low temperature fragility analyses ................................. 52
      7.7.3 Plant response analyses to extremely high/low temperature .................. 53
  7.8 Extreme icing on the overhead power line .................................................. 53
      7.8.1 Extreme icing hazard analyses ............................................................... 53
      7.8.2 Extreme icing fragility analyses .............................................................. 53
      7.8.3 Plant response analyses to extreme icing .............................................. 54
  7.9 High sea level ................................................................................................ 54
  7.10 Low water level in river .............................................................................. 54
7.10.1 Low water level hazard analyses ................................................................. 54
7.10.2 Low water level fragility analyses ................................................................. 54
7.10.3 Plant response analyses to low water level .................................................. 55

7.11 Earthquake ...................................................................................................... 55
7.11.1 Seismic hazard analyses ............................................................................... 55
7.11.2 Seismic fragility analyses ............................................................................. 55
7.11.3 Plant response analyses to earthquake ......................................................... 56

7.12 Aircraft crash .................................................................................................. 56
7.12.1 Aircraft crash hazard analyses ..................................................................... 56
7.12.2 Aircraft crash fragility analyses ................................................................. 57
7.12.3 Plant response analyses to aircraft crash ................................................... 57

7.13 Malicious attack ............................................................................................. 58

8 CONCLUSION .................................................................................................. 59
9 ACKNOWLEDGMENT ................................................................................. 59
REFERENCES ................................................................................................. 59
APPENDIX A: CASE STUDIES .......................................................................... 61
APPENDIX B: IAEA SAFETY REQUIREMENTS, PROTECTION AGAINST EXTERNAL
HAZARDS AND DESIGN FOR EXTERNAL HAZARDS ......................................... 73

LIST OF FIGURES

Figure 3.1. The sample of seismic hazard curves ...................................................... 15
Figure 3.2. The sample of seismic fragility curves .................................................... 16
Figure 3.3. Probabilistic hazard curves for extreme winds - Gumbel distribution. 19
Figure 3.4. Probabilistic hazard curves for extreme winds - GEV distribution. 19
Figure 3.5. The fragility curves of the emergency feedwater pump suction .... 20
Figure 3.6. Generic event tree for accident sequence analysis. 20
Figure 3.7. Overview of the Level 1, 2 and 3 PSA .............................................. 22
Figure 7.1. The overall structure of benchmark exercise ...................................... 39

LIST OF TABLES

Table 3.1. Safety goals of countries and agencies around the world ..................... 23
Table 7.1 The connection of safety requirements and the means to ensure plant safety 44
Table 7.2. The most important hazard category for each safety requirement .... 45
1 Introduction

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 EU member countries have different nuclear safety requirements. It 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 several EU countries. This will help find the most efficient safety engineering processes to support the operation and licensing of nuclear power plants within EU.

The nuclear safety requirements are intended to ensure the highest standards of safety. However, it is recognized that technology and scientific knowledge are making progress, and that nuclear safety and the adequacy of protection against radiation risks need to be considered in the context of the present state of knowledge. Safety requirements will be changed over time. The benchmark exercise should reflect the present consensus.

The benchmark baseline of BESEP is defined within the Work Package 2 (WP2 - Benchmark baseline). WP2 has 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
- T2.3 Specification of key features of efficient and integrated Safety Engineering Process
- T2.4 Identification of general risk significance thresholds of external hazards

The objective of this report is to prepare output for the task T2.1. After the introduction, the second part of the report briefly describes the deterministic safety analyses of external hazards. The hazard analyses and fragility analyses of structures, systems and components (SSCs) are described. In addition, the safety margin analysis is described to demonstrate the plant response evaluation. The safety margin is the level of a hazard that compromises the safety of a nuclear power plant. The compromising of safety means that the plant is rendered incapable of achieving safety objectives under the impact of the hazard.

The third part of the report is focused on probabilistic safety analyses (PSA) for external hazards. This is the way how to seek answers to the following basic questions:

1. What type and how often external hazards occur in the vicinity of the plant?
2. What is the plant response?
3. What is the consequence of the adverse response?

Human factors engineering is discussed in fourth part of the report. Human factor can be understood as a qualitative as well as a quantitative term. Qualitatively it can be described as the aim for successful human performance of activities necessary for system availability and interactions. Quantitatively, it refers to data on failure rates or error probabilities that can be used in PSAs.

Parts two, three and four of the report are added to be familiar with evaluation and for better understanding the impact of external hazards on safety of nuclear power plants. The described methods can be used to demonstrate that the plant is able to withstand the loading of external hazards.

The fifth part of the report is focused on the selection of single external hazards for a site to support the benchmark exercise. The selection is based on the list of external hazards involved in the safety assessments of the BESEP partner countries and preliminary case studies prepared in the preparatory phase of the project.

The sixth part of the report describes selection of combinations of external hazards for the benchmark exercise. It means simultaneous occurrence of two or more external hazards on the site. At the present time,
there is no preliminary case study for combinations of external hazards from the BESEP partners. Therefore, the combinations of external hazards for the benchmark can be selected in a later phase of the project.

The IAEA high-level requirements are used as a starting point to identify the safety requirement topics which should be assigned to external hazards involved in the BESEP preliminary case studies. The assignment of these topics to external hazards is described in part seven of the report.

Conclusions are presented in the eighth part of the report. The preliminary case studies are included in Appendix A of the report. Appendix B of the report is focused on the plant safety requirements. An overview of IAEA safety requirements is provided, the protection against external hazards and design for external hazards are described

2 Deterministic safety analyses for external hazards

Deterministic safety analyses are an essential element of the safety analyses for external hazards. External hazards can be categorized as natural hazards and human-induced hazards. The natural hazards can be further subdivided to seismic hazard and non-seismic hazards.

Different 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 SSCs, while deterministic safety margin analyses, such as seismic margin analyses – SMA, are typically performed on the plant level. The objective of margin assessment of a nuclear power plant against external hazard is to determine the level of the hazard at which the safety objectives of the plant would be compromised. That is, the plant will cease to perform the basic safety functions. The margin assessment process also covers the work of identifying the weak points and areas of improvement for engineering the upgrades to ensure that the safety of the plant is in line with current requirements. So, the overall objective of the different approaches is to support the evaluation of the plant response against the external hazards.

Below, the deterministic safety analyses are described for seismic, non-seismic and human-induced external hazards.

2.1 Deterministic safety analyses of seismic hazard

2.1.1 Deterministic seismic hazard analyses

Deterministic seismic hazard analyses (abbreviated as DSHA) estimate the level of a ground-motion intensity parameter (i.e., peak ground acceleration - PGA and spectral acceleration at different vibration periods, etc.) that would be produced by future earthquakes. When design or seismic performance of structures is of concern, one of the major objectives is to describe ground-motion intensities of design level earthquakes.

DSHA can be considered as the special case of PSHA in which a particular earthquake scenario (i.e., a magnitude and source-to-site distance pair) is specified for the controlling earthquake. To this end, DSHA focuses on the maximum ground motion that can be generated by the seismic sources in the study area. The earthquake producing the maximum ground motion is the controlling earthquake and it describes the seismic hazard in the project site. The ground-motion intensity parameter of interest (i.e., PGA at a given vibration period, etc.) computed from the controlling earthquake scenario is used either for design or seismic performance assessment of structures. DSHA specifies the level of controlling-earthquake ground motion either as median or median + sigma. Specification of ground motions as median or median + sigma resembles the consideration of inherent uncertainty in ground-motion amplitudes.

Since the entire DSHA methodology is based on the controlling earthquake scenario, there is no return period concept at the end of the calculations. In other words, no information is provided on the occurrence probability of the controlling earthquake at the end of DSHA. To this end, DSHA always focuses on the worst-case scenario without quantifying its likelihood during the operation of the plant. However, the decision on the worst-case scenario is still subjective as the choices made for the controlling earthquake or the corresponding ground motion are strongly dependent on the hazard expert. Essentially, the deterministic earthquake or the ground motion identified at the end of DSHA may not be the “true” worst-case as the possibility of having larger earthquakes or ground motions always exists in this approach.
The following steps summarize DSHA [16]:

1. Define the seismic sources, if possible, with style-of-faulting information, in the study area (i.e., the active faults that are likely to affect the hazard in the plant site).
2. Estimate the magnitudes of maximum probable events that can occur on the identified seismic sources. This information can be obtained from the compiled earthquake catalogues. The alternative can be the use of empirical magnitude (M) versus fault rupture length relationships. The latter option assumes the rupture of entire fault length (or a significant portion of it) during the controlling earthquake. The hazard expert can consider an additional 0.5 magnitude units or can include the standard deviation in estimating the maximum magnitude to account for the uncertainty in the largest possible future earthquake.
3. Determine the shortest source-to-site distance between the identified sources and the site.
4. Determine the soil conditions at the site through in situ geotechnical studies (refer to the previous section about identification of soil conditions).
5. Use a proper ground-motion prediction equation to estimate the ground-motion parameter of interest using the magnitude, source-to-site distance, site class and style-of-faulting information obtained in the previous steps. In general, the ground motion parameter of interest is computed either as the median or median + sigma level using the chosen Ground Motion Prediction Equations. Some analysts prefer using the median values of ground motions whereas others chose the latter level. This choice can be specific to the project conditions.
6. Compare the ground motion parameter of interest computed from each source and chose the largest one to be used in the design (or seismic performance assessment). The corresponding scenario is the controlling earthquake specific to the considered design or performance assessment project. Note, that if the median ground motion is chosen, the ground motion has 50 % chance of exceedance whereas upon the choice of the median + sigma ground motion, it has 16 % chance of being exceeded provided that the controlling event hits the project site from the location where the shortest source-to-site distance is calculated.

2.1.2 Deterministic seismic fragility analyses

The plant components and buildings are designed to withstand the design basis earthquake where safe shutdown and cooling down of the reactor can be achieved. Conservatism is introduced into the buildings and component projects by applying conservative design rules.

Therefore, there is a high degree of certainty that even in the event of an earthquake slightly larger than the design basis earthquake, components and buildings will not fail and will perform the safety functions. Their real seismic capacity is therefore usually much higher than the acceleration in case of design basis earthquake with safe shutdown of the reactor.

The seismic resistance of the components and buildings of the nuclear power plant is determined using the boundary seismic resistance in the form of high confidence of low probability of failure (HCLPF). The Conservative Deterministic Failure Margin (CDFM) methodology is used to calculate this value. The safety factor $F_S$ is calculated. It corresponds with the resulting seismic response determined as PGA. The critical acceptance criteria are verified for the evaluated SSCs. The parameter $F_S$ is calculated using different analytical methods and finite element models [15].

The following relationship is applied for calculation of the boundary seismic resistance parameter HCLPF for SSCs:

$$HCLPF = F_S \cdot PGA$$

The parameter HCLPF is required to perform a seismic assessment on the plant level for all safety important components and buildings.

2.1.3 Deterministic seismic margin analyses

The objective of the seismic margin analyses (SMA) of a plant is to determine, if the plant can safely withstand the review level earthquake (RLE). It is a plant response analyses to earthquake.

In the literature two SMA methods are described. One methodology was developed by Electric Power Research Institute (EPRI) and another was developed by the U.S. Nuclear Regulatory Commission (NRC)
The discussion presented in the following is primarily applicable to the EPRI SMA methodology. The EPRI methodology is based on a "success paths" approach. Two success paths must be identified. Each success path consists of a selected group of safety functions capable of bringing the nuclear power plant to a safe state (hot or cold shutdown) after an RLE and of maintaining it there at least for 72 hr.

The SSCs needed to accomplish each of the success paths are then identified and become the basis for the rest of the SMA analysis. When such SMA has been completed, the principal results and insights are reported by findings such as "SSC number X has an HCLPF capacity of 0.2 g," or "has an HCLPF capacity of at least 0.25 g." Using combinatorial rules that are intended to be conservative, the individual SSC capacities can then be combined to provide results such as "the service-water system has an HCLPF capacity of 0.2 g," or "the residual heat removal safety function has an HCLPF capacity of 0.2 g," or ultimately that "the plant as a whole has an HCLPF capacity of 0.2 g," or of course perhaps has an HCLPF capacity of at least 0.25 g.

The main steps of SMA are the following [11]:

- **Selection of the RLE**
- **Selection of assessment team.** The assessment team is made up of systems engineers and seismic capability engineers, it should also incorporate utility personnel, to the maximum extent possible. So, that results, and insights obtained during the SMA can be utilized in plant operation, seismic upgrading, and accident management.
- **Preparatory work prior to walkdowns.** The preparatory work prior to walkdowns consists of gathering and reviewing information about the plant design and operation. During this step, the systems engineers define the candidate success paths and the associated frontline and support systems and components. Preliminary or final estimates of realistic floor response spectra to the RLE are also developed in this step. The potential for soil liquefaction and slope instability is assessed considering the seismic sources in the site region and soil conditions. The objective is to assess if soil failures are likely at the RLE and to estimate the potential consequences on buildings, buried piping, and ground-mounted tanks.
- **Success paths selection walkdown.** The primary objective of this step is a preliminary assessment of the relative seismic ruggedness of the major equipment in the candidate success paths and the selection of a preferred success path and an alternate success path.
- **Seismic capability walkdown.** This step involves the identification of any potential weak links in the SSCs required for the selected success paths. SSCs in the systems are screened in this step from further evaluation based on the EPRI screening criteria. Weak links to be considered include the potential for seismic spatial systems interactions, equipment anchorage, etc. Systems include all frontline safety systems and support systems, e.g., all fluid, electrical power, and instrumentation systems in the success paths.
- **Seismic Margin Assessment.** This step carries out the SMA to demonstrate structural capacity or operability of those structures and equipment that are not screened out in steps 4 and 5. Seismic HCLPF capacity calculations are done to verify if sufficient margin over the RLE exists in the components selected in the success paths.
- **Documentation.** The documentation of the SMA, including information gathered in walkdowns, is completed in this step.
- **Treatment of non-seismic failures and human actions.** This step involves the identification of non-seismic failures and human actions in the success paths. The success paths are chosen based on a screening criterion applied to non-seismic failures and needed human actions. It is important that the non-seismic failures and human actions identified have low enough failure probabilities so as not to affect the seismic capabilities of the success paths.
- **Evaluation of containment and containment systems.** This step is intended to identify vulnerabilities that involve early failure of containment functions including containment integrity, containment isolation, prevention of bypass functions, and some specific systems that are included in the success paths.
- **Relay chatter review.** This step is intended to identify any vulnerabilities that might result from the seismic-caused chatter of relays and contactors.

### 2.2 Deterministic analyses of non-seismic natural hazards

Natural external hazards other than earthquakes may be categorised into one of two categories for the site:

1. hazards that can be screened out from detailed analysis and
2. hazards that need detailed analysis.

Natural external hazards can be evaluated and screened out based on the following criteria:

- A phenomenon that occurs slowly or with adequate warning with respect to the time required to take appropriate protective action.
- A phenomenon which has no significant impact on the operation of a plant and its design basis.
- An individual phenomenon which has an extremely low probability of occurrence.
- The plant is located sufficiently distant from or above the postulated phenomenon (e.g., fire, flooding).
- A phenomenon that is already included or enveloped by design in another phenomenon (e.g., storm-surge included in flooding or accidental small aircraft crash enveloped by tornado loads).

Deterministic screening is usually dictated by standard practice, judgment, or regulatory requirement. The plant must be designed to withstand the not screened out external hazards with an exceedance frequency of $10^{-4}$ per year.

For example, the design against extreme wind and snow loads follows European engineering standards for conventional buildings, i.e., the Eurocodes. For wind, EN 1990:2002 and EN 1991-1-4:2005 are the standards to be applied. For snow, EN 1990:2002 and EN 1991-1-3:2003 are the standards to be applied.

2.2.1 Deterministic non-seismic natural hazard analyses

The analyses of the non-seismic natural hazard are based on a site-specific evaluation that uses recent available data and site-specific information. The analysis can be based on either historical data or a phenomenological model, or a mixture of the two.

Although a site-specific and plant-specific hazard analysis is always desirable, it is often acceptable to characterise a hazard on some other basis (for example, a regional or even generic basis), provided that the uncertainties introduced are acceptable for the applications contemplated. It is allowed to the extent necessary. This requirement is intended to allow approximations provided that the error or uncertainty introduced is not dominant in the analysis. Model uncertainties are especially difficult to quantify in some cases.

Little to no literature is known on establishing physical upper boundaries to phenomena such as meteorological processes. In some cases, extreme values might provide information on possible upper limits, however, for many hazards the recorded periods for which observational data are available are limited.

Whenever a statistical analysis is feasible (when observational data is sufficient), the output of the probabilistic hazard analysis is a so-called family of hazard curves accounting for uncertainties (exceedance frequency versus hazard intensity– the uncertainties allowing to identify a threshold beyond which it is not legitimate to use the hazard curve). However, such curves in the deterministic hazard analyses are not constructed. Normally the upper limit of the hazard size or the design basis external hazard is taken into consideration.

It is necessary to document the processes used to define and quantify the hazard. For example, this documentation typically includes a description of the specific methods used for determining the upper limit or design basis external hazard, including the technical interpretations that are the basis for the inputs and results.

2.2.2 Deterministic non-seismic fragility analyses

The objective of fragility analyses is to justify that the SSCs, performing the required safety functions, and the plant as a whole can withstand the design basis loads with sufficient safety margin. In addition, plant-specific HCLPF values in terms of the intensity of the hazard can be calculated. Note, that in this context, the plant operators are included as components of the system, since some hazards (e.g., toxic gas) may affect operators rather than equipment.
The fragility of an SSC is estimated from the actual capacity of the SSC for a given failure mode. Thus, a failure mode identification is a crucial aspect of this work. Another crucial aspect is an engineering evaluation of how the effect of the hazard is transmitted to the SSC, what force or effect leads to the specified failure mode. Analytical and full three-dimensional finite element analyses are performed.

Margin or fragility could be quantified as a best estimate value or a conservative value (e.g. the HCLPF value), depending on the selected hazard level. The best estimate plant margin is calculated using the best estimate capacities of relevant SSCs. The best estimate (mean or median) capacity of the SSCs is derived from realistic models (i.e. load characterization, failure modes and material properties) for a postulated hazard.

It is necessary to document the processes used to define and quantify the hazard fragilities. For example, this documentation typically includes:

- the methodologies used to quantify the fragilities (capacities) of SSCs, together with key assumptions
- the basis for the screening out of any generic high-capacity SSCs
- a detailed list of SSC fragility values that includes the method of analysis
- the dominant failure modes, the sources of information, and the location of each SSC.

### 2.2.3 Deterministic non-seismic safety margin analyses

The objective of the deterministic non-seismic safety margin analyses of a plant is to determine, if the plant can safely withstand the external hazard. It is a plant response analyses to non-seismic external hazard.

The approach is similar as in case of SMA for earthquake. For example, the wind fragility is evaluated using the same general methodology as for seismic fragilities. The result of a non-seismic margin analyses can be that the plant as a whole has a wind HCLPF capacity of 50 m/s.

### 2.3 Deterministic analyses of human-induced external hazards

The main steps of the analyses are the same as in case of non-seismic natural external hazard.

More detailed description of the methodology for aircraft crash, detonations and deflagrations is in [13].

### 3 Probabilistic safety analyses for external hazards

The accident that took place at the Fukushima Daiichi Nuclear Power Plant as a result of the 2011 Great East Japan earthquake and consequent tsunami raised awareness of the risks associated with external hazards. To achieve high level of safety for nuclear power plants, in addition to SMA the probabilistic safety assessment (PSA) is considered useful because it provides insight into the plant weaknesses by identifying as many accident sequences as possible.

Risk is defined as combination of consequence of an accident and its associated likelihood, i.e., occurrence probability. When a severe accident happens at a nuclear power plant, leading to core damage and containment damage, large amount of radioactive material is released into the environment, exposing the public in the vicinity of the plant and causing environmental contamination.

As a result of PSA, contributors to accident risk can be quantitatively assessed, which are potential causes of an accident. Moreover, PSA can estimate quantitatively the effectiveness of countermeasures to be taken to reduce the risk.

Quantitative safety goal and subsidiary objectives, so-called performance goals, are referred to the criteria that represent the societal acceptability of the risks, see Table 3.1 below.

Safety goals usually concern the radiation risk of the public as well as environmental contamination, while performance goals concern, for example, equivalent plant condition such as core damage frequency (CDF) as well as large early release frequency (LERF).
Events that initiate accidents are classified into:

- random failure of the plant components (internal events),
- internal hazards such as internal flooding and internal fire, and
- external hazards (seismic hazard, non-seismic natural hazards such as strong wind, and human-induced hazards such as an airplane crash and impact of neighbouring industry).

This part of the report is focused only on external hazards.

### 3.1 Key elements of PSA for external hazards

In external hazard PSA, attention is focused on seismic, non-seismic natural hazards and human-induced hazards that may happen in the future and affect the safety of the nuclear power plant. The failure probabilities of structures (e.g., buildings) and components are assessed. Uncertainty 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 can be identified as:

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

The key elements of PSA are described below for seismic, non-seismic and human-induced external hazards.

### 3.2 Seismic PSA

#### 3.2.1 Probabilistic seismic hazard analyses

A seismic hazard curve is a relationship between the earthquake ground motion intensity and its annual exceedance frequency. The main steps of the PSHA are the following [6,16]:

1. Identification of the seismic source model. In seismic hazard analysis, a probabilistic model is employed to model the possibilities of earthquake occurrence that may affect the target site. The magnitudes and occurrence of such earthquakes are considered probabilistically and statistically.
2. Ground motion prediction model. A ground motion prediction model, i.e., attenuation formula, is used to estimate the probability distribution of earthquake ground motion at the target site for each seismic source identified in step 1.
3. Construction of a logic tree. For the source model and ground motion prediction model, a logic tree is employed to account for epistemic uncertainty, i.e., knowledge-oriented uncertainty, in parameters that differ in assumptions concerning, for example, the fault length and the earthquake magnitude.
4. Seismic hazard analysis. As a result of analysis, the seismic hazard curve, i.e., the relationship between the earthquake ground motion intensity and the annual exceedance frequency, is obtained. Uncertainties in the estimated hazard curve are analysed using the logic tree.
5. Generation of artificial earthquake ground motion for fragility analysis. A seismic hazard curve is calculated for response spectra of the ground motion for different vibration periods. A value representing a specified level of exceedance probability is selected at each vibration period for the response spectrum. Then, a uniform hazard spectrum is obtained by connecting these points. From the uniform hazard spectrum simulated ground motion for use in dynamic response analysis is generated.

If the model and the data that produce this seismic hazard curve resulted from perfect knowledge, there would be no uncertainty in the curve. But the knowledge of seismic parameters or even how to model and interpret them is not perfect. In fact, there are generally a number of equally plausible models and interpretations supported by different seismology and geology experts. Each such model produces a different seismic hazard curve. Thus, there is uncertainty about any given result. But the compilation of all such curves would fully represent the state of knowledge about the seismic hazard at the site (Figure. 3.1). To
quantify this uncertainty, it is standard practice to assign weights to these curves based on the degrees of belief that each curve represents the true hazard at the site. These weights are up to 100%.

The seismic hazard curves should cover with sufficiently low and sufficiently high levels of field movement so that it can be shown that the resulting risks are either negligible or have a significant contribution to the frequency of core damage or the frequency of large early release to the environment.

3.2.2 Probabilistic seismic fragility analyses

The fragility curve shows conditional failure probabilities for different ground motion intensity levels. On the basis of information concerning the dynamic response and strength of structures and components, a fragility curve is developed. The fragility curve is estimated for structures and components that are significant in assessing the nuclear power plant risks.

For earthquake-resistant design, a deterministic approach is employed and structural components are designed to have an enough safety margin for the deformation and stress produced by the design basis external forces. On the other hand, the actual external forces from an earthquake and the actual material strength inherently exhibit scatter. In other words, the external forces and the strength of structures and components are random variables and the failure probability of structures and components is represented by a fragility curve.

The main steps of fragility analyses are the following [6,16]:

1. Selection of target structures and components, and the determination of their failure modes. After selecting target structures and components, their failure and associated response parameters to be used for determining their failure are defined.
2. Selection of an analysis method. The analysis method is chosen in view of required accuracy and the objectives of the analysis.
3. Assessment of realistic strength. For each of the target structures and components, the limit beyond which it will fail (i.e., the strength of the structures or components) is assessed probabilistically. The
assessment method that may be employed is either an empirical method using experiments, a numerical method based on analysis, or a method that makes use of engineering judgments integrating both empirical and numerical methods.

4. Analysis of realistic seismic response. For each of the target structures and components, the dynamic response is estimated stochastically, i.e., as a random variable. Conventionally, the input ground motion for this analysis is that derived from the uniform hazard spectrum.

5. Fragility analysis. On the basis of the result of the assessment of the probabilistically estimated strength and response, the fragility curves for the structures and components are obtained.

The fragility curves are typically done by treating the median capacity $A_m$ as a log-normally distributed variable with uncertainty parameters $\beta_R$ and $\beta_U$. Typically, the SSC strength can be represented according to the high confidence and low probability of failure (HCLPF) value derived from the fragility curve and then compared with the design basis ground motion. The HCLPF value is the strength at which failure probability of 5% can be assured with 95% confidence level.

Dependency between HCLPF and fragility parameters is given by the formula:

$$HCLPF = A_m \exp\{-1.65(\beta_R + \beta_U)\}$$

If we know HCLPF the $A_m$ is calculated from the formula:

$$A_m = HCLPF \exp\{1.65(\beta_R + \beta_U)\}$$

![Figure 3.2. The sample of seismic fragility curves.](image)

3.2.3 Plant response and accident sequence analyses for seismic hazard

On the basis of the seismic hazard analysis and SSC fragility analyses, the probability of failure is determined to enable the modelling of accident sequences leading to core damage. The probabilities are calculated by convolution of the hazard curves and fragility curves. The accident sequence analysis starts with the analysis of accident scenarios to calculate core damage frequency.

The main steps of the accident sequence analysis [6,16]:

1. Definition of accident sequences. Accident sequences are defined using event trees and fault trees as a systematic representation of scenarios leading to core damage. The event tree shows how progressive failures of safety functions may lead to an accident including core damage, while the fault tree shows how the combinations of component failures may be a cause of a safety function failure.

2. Calculation of core damage frequency. This is the result of the level 1 PSA. Dominant accident sequences leading to core damage are identified for all operating modes of the plant and the spent fuel pool, and the SSCs with significant contribution to the risk are also identified.

3. Calculation of large early release frequency. This is the result of the level 2 PSA. The level 2 PSA model is developed on the basis of the level 1 PSA model for all operating modes of the plant and
the spent fuel pool. Dominant accident sequences leading to large early release are identified, and the SSCs with significant contribution to the release are also identified.

So, the seismic event is materialized in initiating events. Each of the events may directly, or indirectly, generate event sequences within the plant that have the potential to lead to core damage, containment failure and radioactive material release. Two aspects of plant response are of interest - plant system behaviour and the behaviour of SSCs to the imposed loading conditions. Plant systems are typically modelled by a combination of event trees and fault trees. The seismic event is the initiator of the accident sequences. Plant accident sequences are initiated by a faulted condition, such as a loss of coolant accident, and are modelled by event trees. The ability of the plant systems to mitigate the consequences of the faulted condition depends on the degradation or failure of those safety systems. For example, assuming a coincidental loss of off-site power, a seismic event causes a loss of coolant accident, and the tertiary effect is a fire in the yard that damages the emergency power system.

The fragility analysis is performed on fragility functions of SSCs. Fragility is defined as the probability of failure as a function of the size of the input load. Generally, the fragility function is in terms of a single load parameter. This single parameter could integrate a number of factors into the single parameter. For simplified evaluations, fragility functions for SSCs may be assumed to be binary (i.e. zero or one), leading to screening of SSCs based on seismic capacity.

In the PSA for internal events and internal hazards, event trees are developed to model accident sequences and fault trees are developed to model failures of elements within the event trees, such as systems and structures. For the applications of PSA modelling for seismic event, existing systems models for internal initiators provide a valuable starting point. Modifications to these systems models are required to include failures normally not considered credible for previously modelled internal events. One example is underground cable chases, which may be assumed to be robust against internal events. However, a seismic event may cause their failure. Hence, for specific events, previously screened out components need to be revisited for potential inclusion.

Accident sequences lead to core damage or core melt end points to which containment performance trees need to be added. The analyst needs to recognize that containment performance may be directly, or indirectly, affected by the loading conditions of the containment systems. Containment performance criteria vary among member states of EU. In some member states, containment damage and failure may be allowed if core damage failure does not occur. In addition, emergency management equipment as specified in emergency management equipment guidance and diverse and flexible coping strategies (FLEX) are important elements in containment performance achievement. Off-site release may or may not be considered depending on the risk acceptance criteria.

In using the plant specific PSA approach, each event is in theory modelled by a set of event trees and fault trees similar in structure but with significant differences in loading conditions and consequently plant failure probabilities. To improve efficiencies of the analyses, the enveloping of loading conditions needs to be considered to the extent possible, assuming this does not cause excessively conservative results.

The plant specific PSA can be adapted to perform an in depth safety analysis for external hazards. The adaptation of the PSA for this analysis has some advantages, including:

- The existing plant logic models are available, can be adapted and used, and these models are the most accurate description of plant behaviour.
- End metrics consistent with high level acceptance criteria can be modified and used (e.g. core damage frequency and large release frequency can be calculated). Relative risk ranking of events can be made.
- Risk ranking of overall effectiveness of existing and proposed SSCs is possible.
- Effects of human error and unavailability of systems can be included.

On the other hand, the PSA approach also has some disadvantages. Unless a very simplified PSA approach is used, such as a simplified event tree method, it is only cost effective to use the PSA approach if an internal event PSA has been performed. It is preferable that internal events, internal hazards and external hazards are modelled using PSA techniques. Then, it is only necessary to modify the systems models to include those basic events that were screened out for previous studies but are potentially relevant to the external
hazard. In addition, fragility functions are required for a large number of components, depending on the detail of the systems models and the number of events. The total number of SSCs may require significant effort even after grouping and screening components according to similar behaviour and capacities. Furthermore, specialized expertise is required of the engineering team that develops these fragility functions.

More detailed description is available in EPRI guideline [3].

3.3 PSA of non-seismic natural hazards

3.3.1 Probabilistic non-seismic hazard analyses

The hazard analysis estimates the frequency of occurrence of external hazard loads on the site using a family of hazard curves. The results of analyses are the external hazard curves, i.e., the relationship between the external hazard loads and the annual exceedance frequency, is obtained.

The hazard curves of the site for extreme weather hazards (extreme winds, extreme snow, extreme rain, extremely high and extremely low temperatures, etc.) are generally constructed using the extreme value theory (when sufficient observational data is available, in some countries, observational data can be lacking for infrequent hazards that still have to be considered in the plant safety demonstration). Statistical theory of extreme values is used to analyse observed extremes and to forecast further extremes. For most natural hazards, when available, observational data range from 30 to 100 years, which can then lead to legitimate extrapolations between 100 and 1000-year return level events estimations. The objective of construction of the curves is the analyses of expected loads and determination of occurrence frequency of parameter, characterizing the load. To achieve this objective data collection is performed and evaluated from the site, important for the determination of connection between the load and the occurrence frequency.

The load parameter is known for each external hazard for which the occurrence frequency is calculated from the return period. Each external hazard due to the hazard load can potentially initiate initiating event of accident from the list of initiating events developed for internal event PSA of the plant.

The calculation of occurrence frequency is based on the specific probabilistic hazard analysis of the site which reflects the current available regional and plant specific information. Uncertainties in the model and in the values of parameters have to be correctly considered and propagated to achieve the family of curves used to calculate the hazard curve representing the mean value of the load. For illustration the hazard curves are presented for extreme winds in Figure. 3.3 [7]. The Gumbel distribution is used to construct the family of hazard curves. There is no physical limit on the curves. The generalized extreme value (GEV) models also have been used for these types of predictions. It is possible to include physical limitations (such as maximums and minimums) within this approach, see Figure.3.4 [18].
3.3.2 Probabilistic non-seismic fragility analyses

Fragility of an SSC is the conditional probability of its failure for a given level of external hazard input parameter. Fragilities are needed to estimate the frequency of occurrence of initiating events and to quantify the fault trees for obtaining the external hazard induced accident sequence frequencies.

For failure estimation the philosophy of boundary value with HCLPF (High Confidence of Low Probability of Failure) parameter is used. This parameter is also used in evaluation of seismic capacity of structures and components. The HCLPF value is the strength at which failure probability of 5 % can be assured with 95 % confidence level. For example, in case of extreme wind load it is presented in m/s.

The results of fragility analyses are the fragility curves. The fragility curves of the emergency feedwater pump suction are presented in Figure 3.5 for extremely low temperatures [7].

Some fragility curves can also be shaped as staircase (for instance for flooding, the failure of the SSCs will be associated with probability equal to 1 to an exceeding water level). The definition of relevant fragility curves requires a significant knowledge about design margins and uncertainties associated to the failure characterization.
3.3.3 Plant response and accident sequence analyses for non-seismic hazards

The plant response and accident sequence analyses have the same steps as in case of seismic hazard. The approach of accident sequence analysis is shown in Figure 3.6. A generic event tree for extreme wind is presented. The tree has 22 accident sequences, leading to OK state (accident sequence 1), a single initiating event (accident sequences 2, 3, 4, 5, 9, 13), combination of initiating events (accident sequences 6-8, 10-12, 14-20) or core damage (21 and 22).

3.4 PSA of human-induced hazards

The main steps of the analyses are the same as in case of non-seismic natural external hazards. More detailed description of the methodology for aircraft crash, detonations and deflagrations is in [13].
3.5 Evaluation of consequences

PSA is a method for analysing and assessing events (i.e., accidents and failures) that can happen for SSCs at a plant in a comprehensive and systematic manner, and it enables the quantitative assessment of the probability of occurrence of each event as well as the magnitude of consequence for each event.

The output of external hazard PSA includes the following:

- frequencies of occurrence of accidents with different consequences (e.g., core damage, large early radioactive release, potential health effects, and property damage), and
- identification of dominant risk contributors; if the risk is not acceptable, the structures, systems and components may be upgraded to reduce the risk.

In addition, the achievement of safety goals is verified. The IAEA (INSAG12) [4] and US NRC [5] safety and performance goals are presented in Table 3.1. The safety goals and performance goals are technology-neutral. It means, that they are valid for all nuclear power plants with any type of reactor technology.

PSA estimates three levels of risk, depending on different stages in accident progression:

- Level 1 PSA develops events up to the occurrence of core damage and the core damage frequency is estimated.
- Level 2 PSA further develops events leading to a release of radioactive material and the frequency of occurrence for such release is obtained.
- Level 3 PSA consists of assessing the societal risk including the health risks to the public in the nearby area, including its occurrence frequency based on the results of Level 2 PSA.

External hazard Level 2 PSA can be implemented using the Level 2 PSA procedures for internal events.

External hazard Level 2 PSA identifies and estimates accident scenarios leading to release of radioactive materials. Attention is given not only to the damage possibility of containment by external hazard, but also to possible damage of SSCs which support the capacity of the containment. The accident scenarios leading to core damage are classified into several groups according to their types. Attention is paid to the particularities and similarities among different scenarios. Representative plant damage states are assigned to each group of accident sequences. The frequency and magnitude of the release (source terms) are quantified.

After determination of the source terms the external hazard Level 3 PSA can be implemented using Level 3 PSA procedures for internal events.

Overview of the Level 1, 2 and 3 PSA are in Figure 3.7 [6].

Typical considerations about consequences include both deterministic and probabilistic approaches what can be summarized in the following way:

1. Safety of the public: To control the radiation exposure to people during operational and accidental states, which is the overarching metric, within intermediate metrics such as:
   - Core damage frequency;
   - Containment and containment systems failure;
   - Large early release frequency;
   - Release of radioactive material to the environment (dispersion in air, water and ground);
   - Collateral effects (e.g. release of radioactive materials and received radiation doses).
2. Environmental consequences: Short, medium and long term effects on the environment (air, water and ground).
3. Safety of plant personnel: Short, medium and long term health and welfare of plant personnel.
4. Energy security of the country: The need for the power generated by the nuclear power plant for country welfare.
5. Economic considerations: Short, medium and long term effects on the country economy.
Figure 3.7. Overview of the Level 1, 2 and 3 PSA.
<table>
<thead>
<tr>
<th>Country/agency</th>
<th>Safety goals</th>
<th>Performance goals</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General nuclear safety objective</strong></td>
<td>- To protect individuals, society and the environment by establishing and maintaining in nuclear power plants an effective defence against radiological hazard. <strong>Radiation protection objective</strong> - To ensure in normal operation that radiation exposure within the plant and due to any release of radioactive material from the plant is as low as reasonably achievable, economic and social factors being taken into account, and below prescribed limits. - To ensure mitigation of the extent of radiation exposure due to accidents. <strong>Technical safety objective</strong> - To prevent with high confidence accidents in nuclear plants - To ensure that, for all accidents taken into account in the design of the plant, even those of very low probability, radiological consequences, if any, would be minor. - To ensure that the likelihood of severe accidents with serious radiological consequences is extremely small.</td>
<td>Existing plants core damage frequency &lt; 1.0E-4/plant operating year New plants core damage frequency &lt; 1.0E-5/plant operating year Practical elimination of large early releases Severe accident management and mitigation measures should reduce by a factor of at least ten the probability of large off-site releases requiring short term off-site response</td>
</tr>
<tr>
<td><strong>Quality safety goals</strong></td>
<td>- Individual members of the public should be provided a level of protection from the consequences of nuclear power plant operation such that individuals bear no significant additional risk to life and health. - Societal risks to life and health from nuclear power plant operation should be comparable to or less than the risks of generating electricity by viable competing technologies and should not be a significant addition to other societal risks <strong>Quantitative safety goal</strong> - The risk, to an average individual in the vicinity of a nuclear power plant, of prompt fatalities that might result from reactor accidents should not exceed 0.1 % of the sum of prompt fatalities risks resulting from other accidents to which members of the US population are exposed - The risk to the population, in the area near a nuclear power plant, of cancer fatalities that might result from nuclear power plant operation should not exceed 0.1 % of the sum of cancer fatality risks resulting from all other causes.</td>
<td>Core damage frequency (existing plant, new plant) &lt; 1.0E-4/reactor year Large early release frequency (existing plant) &lt; 1.0E-5/reactor year Large release frequency (new plant) &lt; 1.0E-6/reactor year</td>
</tr>
</tbody>
</table>

Table 3.1. Safety goals of countries and agencies around the world.
4 Human factors engineering

Human error can contribute substantially to system failures. At nuclear power plants, operational experience demonstrates that human error accounts for a considerable proportion of safety-related incidents. However, experience also shows that human intervention can be very effective if there is a thorough understanding of the situation in the plant. Thus, an efficient interface of man and machine is important not only to prevent human errors but also to assist the operator in plant operation, accident scenarios and coping with unforeseen events.

Human reliability can be understood as a qualitative as well as a quantitative term. Qualitatively it can be described as the aim for successful human performance of activities necessary for plant safety, system reliability and availability. Quantitatively, it refers to data on failure rates or error probabilities that can be used, for example, for PSA.

This part of the report is prepared based on [19,20].

4.1 Human factors engineering applied for plant design and operation

For the design and construction of new nuclear power plants as well as for maintenance and operation of the existing one’s new man-machine interface designs and modifications are been produced. For these new designs Human Factors Engineering (HFE) must be applied the same as for any other traditional engineering discipline.

Advantages of implementing adequate HFE techniques in the design and operation of nuclear reactors have become not only a fact recognized by the majority of engineers and operators but also an explicit requirement regulated and mandatory for the new designs of the so-called advanced reactors. Additionally, the big saving achieved by a nuclear power plant having an operating methodology which significantly decreases the risk of operating errors makes it necessary and almost vital its implementation.

The first step for this is preparing a plan to incorporate all the HFE principles and developing an integral design of the instrumentation and control and man-machine interface systems.

Such a plan should state activities to be performed. It is required to develop several methodologies to screen those design features that meet the general requirements and objectives of the facility and of the systems which make it up as well as for performing design evaluations from a human factor standpoint. Implementation of those methodologies is needed in the system design.

Creation of an HFE team adequately qualified is also needed. The HFE team is an integral part of the design team and is strongly linked to the engineering organizations but simultaneously has independence to act and is free to evaluate designs and propose changes in order to enhance human behaviour.

Finally, the verification confirms that the product of each step in the development of design specifications, fulfils all requirements imposed by the previous step of the design. Using identified user tasks, verification processes are used to evaluate the availability of the correct information and controls. Verification is a check of the individual control room components against the plant engineering criteria, human engineering criteria, and operating and functional requirements. The verification includes:

- Instruments and displays provided in the control room represents relevant process parameters.
- Controls and displays, whether computer generated or hardware, are arranged in a consistent and orderly pattern.
- Failed instruments and displays are easily recognizable as failed.
- Workstations are arranged so that access to the control boards is not impeded.
- Adequate controls for air temperature, humidity, and ventilation are provided.
- Controls are located so that related displays can be used to provide feedback.
- Maintenance, test, and inspection activities can be performed as planned.

Following integration of the human system interface hardware and software, validation is the test and evaluation of the product to determine the user's ability to perform the assigned tasks in accordance with defined acceptance criteria. Thus, the validation process measures the ability of the user to perform the
allocated tasks using the product that has been provided the specific task. Due to its position in the design process, the validation process identifies deficiencies in the preparation of user procedures and training. The control room configuration design is validated against the functional requirements established from operations analysis. This process is achieved by simulating operations with a control room mock-up. Time dependent characteristics are evaluated using a full-scope simulator.

4.2 Plant procedures

The plant procedures are all the procedures that are used in the operation of a nuclear power plant. There are four categories:

- administrative procedures,
- operating procedures (normal, alarm response, pre-hazard, abnormal and emergency procedures - SB EOPs, SAMGs, EME, FLEX),
- maintenance and technical support procedures, and
- testing and surveillance procedures.

Administrative procedures describe how administrative aspects of plant activities are carried out, such as review and approval of documents, training and qualification of plant personnel, and maintenance and retention of plant records. Operating procedures are self-defined. Maintenance and technical support procedures relate to activities such as the conduct of preventive and corrective maintenance, radiation protection, and chemistry control. Testing and surveillance procedures relate to activities such as: functional tests of safety systems, post-maintenance test procedures, and post modification procedures. The principal plant documentation excluded from this definition of plant procedures is design documents including vendor manuals.

Following the Three Mile Island accident in 1979, symptom-based emergency operating procedures (SB EOPs) have been implemented in preventing or mitigating core damage as a result of unplanned transients. The operator actions result from the monitoring of plant symptoms. All the symptom-based procedures prioritize operator actions based on the potential threat to the three barriers (fuel cladding, primary coolant system boundary, and containment) and allows the operator to respond to these threats prior to event diagnosis. This is the way how to improve human reliability.

Most recently, it has been recognized that the operator needs additional guidance for those conditions beyond the design basis accidents where core damage exists or is imminent; hence the evolution of severe accident management guidelines (SAMGs). Due to the wide variety of conditions that may exist, these guidelines have been written in a symptom-based format and offer greater latitude in determining the appropriate success path. This approach also improves human reliability.

Given that, for example due to an external hazard, no success path is available to perform safety functions, the EME and FLEX equipment and procedures are used. To take into account these strategies several issues must be verified. If there is no redundancy, diversity and separation (i.e. a single train system is considered), then verification is required of the following [24]:

- There will be no damage to EME or FLEX equipment from the external hazards (no damage from impact, collateral damage from debris, damage from fire, or from smoke from aircraft crash; and no damage from an explosion);
- There will be no damage in the yard to impede the personnel from performing their required function to implement the equipment;
- There will be no missing equipment or inoperative equipment;
- There will be no human error, so the single train system is 100% operative (zero failure).

If EME or FLEX is a single train system, the likelihood, potentially a small likelihood based on evaluations as described above, that a single train system does not perform its function needs to be considered.
4.3 Education and training

Qualified personnel are central to ensuring safe and reliable operation of a nuclear power plant. Their continuing education is necessary so that required performance levels are achieved and maintained. It includes initial training, retraining, and the updating and broadening of knowledge and skills. While each country has certainly developed its own educational system depending on national conditions, the particular skills required of nuclear power plant personnel anywhere are common, the safe operation of the plant cannot be compromised.

Thus, each country’s nuclear power training programme has to attain the same level. One primary skill, particularly in the future, will be adaptability, that is, the ability to cope with unforeseen circumstances, for example generated by external hazards. It means being able to find, to recognize, and to formulate a problem and deciding if the problem ought to be solved, as well as how to solve it. While education refers mainly to formal studies and continued competence, training is oriented towards job specific tasks. Apart from training performed in classrooms or on the job, the utilization of simulators for this purpose has attracted particular attention. Most countries with nuclear power plants have simulator training programmes, generally well developed. But their value can be limited by the simulator's age, type, size, and capability. However, simulator training and retraining is indispensable for improving safe plant operation and providing the knowledge and skills for plant control under normal and abnormal conditions. Furthermore, benefits of simulator training can be seen for three aspects. One refers to PSAs, where the insights gained can be used to select scenarios for training. Simulation experiences also can be used to update and improve PSAs. The other aspect relates to the possibility of evaluating plant modifications from the standpoint of human factors. This includes new equipment, the correctness and practicability of normal and emergency operating procedures, and the adjustment and updating of training programmes. The last aspect is to improve the reliability of operator in accident scenarios induced for example by external hazards.

4.4 Experience with simulator training

Review of experience with simulator training for emergency conditions showed that safety-significant incidents often present operators with a situation that evolves and develops quite differently from the scenarios on the simulator. In addition, since emergency conditions are rare events, prediction and analysis of human performance presents certain difficulties. However, the overall usefulness and importance of simulator training for severe plant conditions is generally recognized, especially if accident scenarios are designed in such a way that sequences can be started at different power levels and the simulation can proceed until degraded core conditions are reached. Furthermore, if an error is committed by the trainee in handling a particular situation, the simulation can be stopped, and the error can be pointed out and discussed. Subsequently, the scenario can be resumed, thus providing a valuable feedback for both the instructor and the trainee. In a systematic manner, data can be collected by means of automatic systems monitoring trainee performance or the establishment of a scheme that reports errors for the instructor. PSAs are making increasing use of data on human performance collected from simulator sessions. In the future, such activities should be concentrated also on external hazards.

4.5 Human error data collection

Analysis of abnormal events and insights from PSAs have demonstrated that a large proportion of cases have their origin in erroneous human performance. The main source of information on human behaviour or error is the operational experience at nuclear power plants. Apart from the national reporting practices of safety-related events to the regulatory authorities also international reporting schemes exist: Incident Reporting System (IRS) of NEA/OECD and IRS IAEA

Analysis methods are developed to single out the human performance contribution to the accident. Utilities also started systems dedicated to identifying the role of human errors in incidents. Following examples can be presented to address the topic:

- Activities such as testing and maintenance are a common cause of errors. Implementation of automatic procedures may alleviate some problems.
- Human errors are more frequent in systems having low levels of availability or redundancy, or those not sufficiently automated.
- Human errors in abnormal conditions are more frequent just after alarms have been initiated.
- Bad design (from viewpoint of system engineering, control-room layout, and ergonomic principles) is a major cause of human error.
- The transfer of information during shift changes of personnel is a general cause of error.
- Internal and external hazards have significant impact on the key performance factors of the plant personnel.

PSAs provide valuable insights for determining the plant systems which are subject to human interaction and for aggregating these interactions in terms of similar tasks or common causes.

4.6 Information feedback

Accident analysis provides the possibility of understanding human errors to some extent. The operator has to get feedback, but the question is how to establish specifications for assessing it. In solving problems related to human error and the implications of operational experience, some countries seem to focus on databases, others on simulators. Research has to continue in this area, in different directions, and co-ordination seems to be necessary, in the view of many experts. Feedback on the role of human factors in significant events is being analysed nowadays in several research centres. One objective is to assure that operational events are investigated in a systematically and technically sound way. Significant attention is paid to impacts of external hazards.

The most common types of errors included omissions and delayed operations. As for mechanisms of errors, the most common are forgetting to perform an operation and the failure to identify the correct operation, together with a bad diagnosis of the state of the system.

4.7 Operator support systems

Operator support systems refer to a class of devices designed to be added to a nuclear power plant control room to assist the operator in performing his job and thereby decrease the probability of human error. They encompass a wide range of devices from the simple, such as colour coding a display to distinguish it from a group of similar displays, to the complex, such as a computer-generated video display that concentrates a number of scattered indicator readings located around a control room into a concise display in front of the operator.

Major efforts have been devoted to the development of computerized operator information and support systems. Depending on the pre-defined purpose, different systems have been conceptualized. While early systems were primarily devoted to monitoring critical safety functions and the detection and location of disturbances, later systems surpassed this limited scope by additionally providing information on the normal plant configuration as a function of the mode of operation and predictive plant behaviour. This increasing reliance on computerized operator support systems should be examined in the light of tasks to be performed, thus emphasizing the relative strengths of humans and computers. Support systems are being developed for monitoring the size of external hazards, for example the peak ground acceleration in case of earthquake.

4.8 PSA information for safety decisions

PSA has become an important tool for evaluating reactor safety. The results have brought invaluable insights for plant design and operation. Some works allow for a more immediate and interactive use of the information contained in a PSA. The objective of these efforts is to create a "living PSA model", readily available for operational safety management.

Applications of PSA information for operational safety management are based on the effect that changes in plant configuration may have on overall plant safety. They include control and assessment of the status of the essential safety systems; modifications in operational procedures; changes in technical specifications (in particular those regarding test and maintenance and allowable outage times); prioritization of items for repair; evaluation of design changes considering the interactions between plant systems; prioritization of inspection activities.
Current developments are aimed at providing information for decision-making under normal plant operation conditions. Software packages (risk monitors) include a PSA model of the plant based on results from fault tree and event tree analyses. Utility personnel and regulators are the main users of these software packages. At the present time the risk monitors are being extended from internal event and internal hazard PSA also to external hazard PSA.

4.9 International co-operation

Many possibilities exist to strengthen the human factor in nuclear power plant operation. This can be achieved by engineering measures to improve equipment or by measures to improve operator behaviour. Topics included analyses of human behaviour in plant operation, reviews of human engineering measures to improve human performance, and the importance of providing the operator with more and better information. The international cooperation is extremely important in this area because the particular skills required of nuclear power plant personnel anywhere are common since there can be no compromise for the safe and reliable operation of a nuclear power plant. Exchange of information is the best way for transfer of know-how. Now the activities are focused mainly on external hazards.

5 Selected external hazards for BESEP

External hazards can occur as single hazards or as combinations of two or more external hazards. The single hazards are described in this chapter of the report. Chapter six is focused on combinations of external hazards.

The vast variety of the characteristics of external hazards themselves and of their interaction between each other and with the plant makes the analysis a challenging task. Given the multitude of possible external hazards on the site, efficient identification methods, screening criteria, and analyses methods are extremely important in order to make it possible to perform relevant and credible analyses with reasonable results.

External hazard analyses are largely site and plant specific. However, many basic features of the analyses are common. This applies to the identification of potentially relevant single external hazards, development of screening procedures and analysis methods. The methodology of external hazard identification for a site is described in [1].

The engineering safety evaluation process of protection against single external hazards is composed of five phases [25]:

- Phase 1: Hazard identification;
- Phase 2: Hazard evaluation and load characterization;
- Phase 3: Design and evaluation approaches to SSCs;
- Phase 4: Plant performance assessment and acceptance criteria;
- Phase 5: Operator response.

This part of the report is focused on the first phase which is the first and highest level of screening implemented in the process. In this phase, single external hazards with the potential to cause unacceptable consequences are identified for further evaluation.

Phase 1 comprises three steps: 1) general assessment of potential hazards, 2) consequence evaluation, and 3) screening and categorization of hazards. These steps are described below.

Event assessment means a complete identification and evaluation of previously and newly defined hazards, categorizing them for inclusion in the evaluation. A hazard assessment comprises: identification of the hazard, definition of the loading conditions associated with the hazard and selection of the evaluation process (including methodologies of evaluation and parameters to be considered), consequence identification and acceptance criteria. Comprehensive and well organized external hazard assessment programmes need to be conducted by the operator of the nuclear power plant and reviewed, as appropriate, by national, state and local government organizations, as these organizations are the source of much of the information on the hazards evaluated (human-induced external hazard).
Consequence evaluation identifies the consequences of interest to be taken into account for external hazards. Typical considerations of consequences are described in part 3.5 of this report.

Screening and categorization of the hazards is a decision step. Experts perform screening and categorization of the identified hazards from step 1, and apply the consequence criteria from step 2 to define the events to be considered for the nuclear power plant of interest. Categories include:

- Not to be considered: This includes those events that are not applicable owing to reasons such as:
  - Physical conditions of the nuclear power plant.
  - Events that remain the government responsibility to ensure no impact on the nuclear power plant (e.g. a state owned dam whose water should be systematically released to prevent overtopping or dam failure under extreme flooding conditions).

- Design basis external hazards: Generally, these are events considered in the design.

- Design extension external hazards: These are rare and extreme events for which realistic, rather than conservative assumptions and acceptance criteria, can be used. They are the principal subject of the design, evaluation process and methodology. In existing plants, these events were generally not considered in the design.

The phase 1 end products are the following:
- A comprehensive list of identified external hazards that may be applicable to the nuclear power plant (step 1);
- Documentation of the government defined consequence criteria, which will be the basis for screening in, or out, external hazards (step 2);
- The disposition of the identified external hazards into categories (step 3)

It is important to consider external hazards at all stages of the nuclear power plant: sitting, design, construction, operation and decommissioning.

In addition, it is necessary to emphasize the link between the site characteristics and the ultimate heat sink and the need to consider external hazards that could cause a loss of function of systems required for the long term removal of heat from the core, such as ship collisions, oil spills and fires.

It is important to note that consideration of external hazards goes far beyond the site selection stage, since human activities around a selected site can change considerably during the life of the nuclear power plant. Hence, the set of external hazards considered applicable to the plant is not to be frozen at the site selection stage. The site needs to be periodically assessed for the potential new or increased external hazards derived mainly from the updated human activities in the site vicinity (human-induced external hazards).

The objective of BESEP project is to show applications of the above described approaches for single external hazards. At first, the single external hazards in the safety assessment of BESEP partner countries are described. Then, the external hazards of interest in the BESEP benchmark exercise are identified on the basis of available case studies from the preparing stage of the project. In addition, a supplementary list has been developed for additional external hazards not involved in the case studies but based on the available experience are recommended to be involved in the project.

5.1 External hazards in the safety assessments of BESEP partner countries

The external hazards described below are involved in the safety assessments of BESEP partner countries.

**Czech Republic**

The external hazards are presented for Dukovany NPP and Temelin NPP [21]:

<table>
<thead>
<tr>
<th>Event definition</th>
<th>Type of analysis in Dukovany PSA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Volcanic activity</td>
<td>Qualitative analysis</td>
</tr>
<tr>
<td>Ground changes</td>
<td>Qualitative analysis</td>
</tr>
<tr>
<td>Abrasive storm</td>
<td>Modelled in PSA</td>
</tr>
<tr>
<td>External floods (river)</td>
<td>Qualitative analysis</td>
</tr>
</tbody>
</table>
Extremely high temperature: Modelled in PSA
Extremely low temperature: Modelled in PSA
Extreme rain: Modelled in PSA
Extreme snow: Modelled in PSA, important
Frost: Qualitative analysis
Hail: Qualitative analysis
Extreme wind: Modelled in PSA, important
Hurricanes, cyclones: Qualitative analysis
Lightning: Modelled in PSA
Earthquake: Modelled in PSA, separate project on seismic PSA
Meteorite impact: Qualitative analysis
Man-made external events: Qualitative analysis
Aircraft crash: Detailed analysis and estimation of frequency
Tornado: Modelled in PSA

**Event definition**
**Type of analysis in Temelin PSA**

<table>
<thead>
<tr>
<th>ID</th>
<th>Description</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>A01</td>
<td>Strong wind</td>
<td>X</td>
</tr>
<tr>
<td>A02</td>
<td>Tornado</td>
<td></td>
</tr>
<tr>
<td>A03</td>
<td>High air temperature</td>
<td></td>
</tr>
<tr>
<td>A04</td>
<td>Low air temperature</td>
<td></td>
</tr>
<tr>
<td>A06</td>
<td>Extreme rain</td>
<td></td>
</tr>
<tr>
<td>A07</td>
<td>Extreme snow</td>
<td>X</td>
</tr>
<tr>
<td>A10</td>
<td>White frost</td>
<td></td>
</tr>
<tr>
<td>A14</td>
<td>Lightning</td>
<td>X</td>
</tr>
<tr>
<td>A26</td>
<td>Ice storm</td>
<td></td>
</tr>
<tr>
<td>A30</td>
<td>Downburst</td>
<td></td>
</tr>
<tr>
<td>A31</td>
<td>Freezing rain</td>
<td></td>
</tr>
<tr>
<td>G07</td>
<td>External fire</td>
<td></td>
</tr>
<tr>
<td>G14</td>
<td>Earthquake</td>
<td></td>
</tr>
<tr>
<td>W02</td>
<td>Low sea (river) water level</td>
<td></td>
</tr>
<tr>
<td>W03</td>
<td>High sea (river) water level</td>
<td>X</td>
</tr>
<tr>
<td>W04</td>
<td>High sea (river) water temperature</td>
<td>X</td>
</tr>
<tr>
<td>W07</td>
<td>Surface ice (sea)</td>
<td></td>
</tr>
<tr>
<td>W08</td>
<td>Frazil ice (sea)</td>
<td></td>
</tr>
<tr>
<td>W09</td>
<td>Ice ridge/pack (sea)</td>
<td>X</td>
</tr>
<tr>
<td>W10</td>
<td>Organic material in sea water</td>
<td>X</td>
</tr>
<tr>
<td>W12</td>
<td>Solid or liquid water pollution (from ships)</td>
<td>X</td>
</tr>
<tr>
<td>W13</td>
<td>Chemical water releases</td>
<td></td>
</tr>
</tbody>
</table>

**Finland and Sweden**

The external hazards considered in PSA in Sweden and Finland after initial screening process (X = dominating for level 1 PSA incidents) [22]:

**France**

The French regulation (Order of 7 February 2012 setting the general rules relative to basic nuclear installations) requires that plausible external hazard and plausible combinations of external hazards be taken into consideration in the demonstration of nuclear safety of basic nuclear installations (BNI).
In France, the nuclear safety demonstration shall include deterministic and probabilistic analyses of accidents and their consequences.

**Deterministic Hazard Analysis**: Natural hazards assessed by EDF for the PWR French fleet are (some hazard can be site-dependent): earthquake, external flood, lightning, snow, wind and associated missiles, warm and cold temperatures, tornado and heat sink specific hazards (lowest safety water level, icing, frazil ice, clogging and silting).

External hazards assessment is completed with human-induced external hazards: risks induced by the industrial activities and communication routes, including explosion, hazardous substance emission and airplane crash.

**Hazard PSA**: In the regulatory context, the probabilistic analyses shall also include external hazards for each nuclear site, unless the licensee demonstrates that this is irrelevant. In practice, external hazards “screening” is expected to be performed by licensees, in order to identify the hazards and combinations of hazards which may need detailed probabilistic assessment to evaluate the associated risk. EDF provided an external hazard screening guide which was reviewed by IRSN. EDF already applied external hazards screening for 900 MWe and N4 sites but limited to single hazards. In France there are no methodology documents in place for the development of hazards PSA or PSA for hazard combinations. Only screened in external hazard or combinations of external hazards which are judged relevant will be explicitly modelled in PSA models. Relevance depends on state of the art, available data for hazards characterization and safety issues.

For the 900 MWe NPPs, 12 single external hazards were screened in and only 7 single external hazards were explicitly considered:

- Airplane crash;
- Air pressure wave;
- Earthquake;
- Rupture of retaining structure (excluding dam) – the only NPP concerned is Tricastin (site under hydraulic load due to a dike existence). This analysis was conducted within the seismic PSA;
- River flooding;
- Sea Site flooding;
- Capacity failure on site.

Regarding the 1300MWe series, 8 single external hazards were screened in. These 8 external hazards will be explicitly modelled in PSA models if feasible:

- Airplane crash;
- Air pressure wave;
- Earthquake;
- River flooding;
- Capacity failure on site;
- Extreme high temperature;
- Wind;
- Tornado.

These PSAs have not been performed yet. EDF also wants to point out that these lists are site dependent and cannot be directly applicable for other sites and other designs.

**Hungary**

The following single external hazards were considered in the design basis of the Paks NPP [23]:

- natural external hazards:
  - hazards belonging to the domain of geosciences:
    - geological and tectonic hazards,
    - seismological hazards,
    - geotechnical hazards,
    - hydrogeological hazards,
o meteorological hazards:
  • extreme wind,
  • extreme rainfall,
  • extreme snow,
  • extreme frost and ice formation,
  • extremely high and low air temperature,
  • lightning,
  • tornado,

o hydrological hazards:
  • extremely high water level,
  • extremely low water level,
  • riverine events endangering water intake from the river Danube as ultimate heat sink due to contamination or debris,

o biological hazards,

• human-induced external hazards, related to the following activities:
  o road transport,
  o transport by inland waterways,
  o rail transport,
  o aviation,
  o usage of parking lots (parking lot fire),
  o forest use and management (forest fire),
  o construction and operation of nearby industrial facilities (including nuclear as well as non-nuclear accidents),
  o military activities.

After screening and hazard analyses, PSA models have been developed for the following single external hazards:

• extreme wind,
• extreme snow,
• extreme frost and ice formation,
• extremely high and low air temperature,
• tornado,
• river events endangering water intake from the Danube.

Slovak Republic

After a screening process based on methodology described in [1,8] the following external hazards are involved in PSA [7]:

• Earthquake
• Extreme wind
• Tornado
• Extremely high outside temperatures
• Extremely low outside temperatures
• Extreme rain
• Extreme snow
• Icing
• Lightning
• Human induced accidents (explosion after transportation accident, chemical release after transportation accident near the plant and aircraft crash)

Only the impact of earthquake, extreme wind and tornado is important from the risk point of view.

5.2 External hazards in the preliminary case studies

As a preliminary step, a review has been made of the case studies, prepared during the project proposal phase, with focus on the needs of task T2.1. Based on the review, the external hazards addressed in the initial case studies have been identified.

The following external hazards are identified on the basis of the preliminary case studies:
• Seismic hazard (Earthquake)
• Natural non-seismic hazards:
  o extreme weather conditions:
    ▪ extreme wind;
    ▪ tornado;
    ▪ extreme snow;
    ▪ extreme rain;
    ▪ extremely high or extremely low air temperature;
    ▪ icing (glaze ice and rime);
  o hydrological hazards:
    ▪ low water level in river;
    ▪ high sea level;
• Human-induced hazards:
  o aircraft crash;
  o malicious attacks.

5.3 External hazards not involved in the case studies

In addition to the external hazards addressed in the preliminary case studies, a supplementary list has also been developed for additional external hazards. Additional hazards are considered as important based on experience. Moreover, these hazards are, to a greater or lesser extent, in the focus of safety assessment and evaluation worldwide. Accordingly, it is suggested that efforts should be made to cover some of these additional hazards, as seen feasible and manageable within the project:

• Non-seismic natural hazards:
  o extreme weather conditions:
    ▪ lightning;
  o external events endangering water intake from the ultimate heat sink (these may be partly human-induced hazards too);
  o geomagnetic currents (highly energetic particles ejected from the sun - solar wind);
  o biological hazards:
    ▪ pandemic;
  o hydrological hazards
    ▪ extremes of cooling water (sea, lake or river) temperature (low/high)
• Seismic hazard
  o seismological hazard
  ▪ liquefaction
• Human-induced hazards:
  o accidents during handling chemical substances (explosion, fire and release of toxic gases);
  o missiles from rotating equipment;
  o transportation accidents (explosion, fire and release of toxic gases);
  o electromagnetic interference, radiofrequency interference or disturbance from off-site sources.

Now, it can be stated that some most relevant external hazards are addressed in the preliminary case studies. However, the extension of the case study pool with a few additional external hazards could usefully serve the objectives of the project. It should also be emphasised that even if some case studies address a certain external hazard, it does not mean that all the aspects relevant to the given hazard and the corresponding safety assessment and evaluation are covered within and among the case studies. A systematic review is seen necessary from this respect when the case studies are finalised.

6 Combinations of external hazards

The potential combined hazards are two or more external hazards having a conditional probability occurring simultaneously, e.g., strong wind occurring at the same time with extreme rain or snow. Combined hazards which may contribute significantly to the plant risk need to be identified during the risk assessment of the plant.
After identification of the relevant single hazards, the possible combinations of hazards are analysed. In the first step exclusion of combinations with two events is performed. High number of combinations can be screened out using the criteria described in [1,8]: 1) independent events, 2) seasonal variations, 3) exclusive preconditions and 4) similar or same effects.

1) Independent events: The selected events that have no dependency with other events are excluded from further evaluation. However, an event combination may be considered relevant if it exceeds the general cut-off value frequency (for example 1.0E-7/y) normally applied in the PSA.

2) Seasonal variation: The events occurring in different seasons cannot form a relevant combination, for example extremely low and extremely high temperatures.

3) Exclusive preconditions: Some events require the same specific preconditions related to weather conditions. The events that have opposite preconditions cannot form a relevant combination. Natural events related to atmosphere and sea typically require certain simple preconditions. The preconditions normally analysed are: air temperature (at ground level) above or below zero, wet/rainy or dry conditions and open sea or sea covered by an ice sheet. For example, lightning needs air temperature > 0 °C and wet or rainy weather. Low air temperature is below 0 °C. These two events cannot create a combination of external hazards.

4) Similar or same effects: The effects of two events are the same or very similar, for example, the same initiating events are initiated from the list of internal event PSA. Given the first event occurred, no further consequences are caused by the second event. These event combinations are not considered. However, the event combination is relevant if the combined effect is significantly greater than the effect of a single event.

Many times there are dependencies between external hazards. There are two types of dependencies: 1) fundamental and 2) cascade-type dependency. In the first case the occurrence of external hazard is related to the same basic phenomenon or the hazards are created by the same mechanism. Given the cascade-type dependency the first hazard strengthens the second hazard, it means that its probability is increased or its effect is worsened.

The qualitative and quantitative assessment is performed for the identified relevant combinations of two events. If after a qualitative assessment a combination is still considered relevant, the frequency of the event combination is calculated by using the frequencies of occurrence of the single events. These frequencies are usually estimated using the extreme value theory [9].

The combinations with more than two events are also identified. The approach is that the two-events combinations are evaluated whether there is additional event which has a dependency with both events.

The objective of BESEP project is to show applications of the above described approaches for combinations of external hazards. At first, the combinations of external hazards in the safety assessment of BESEP partner countries are described. Then, the combinations of external hazards for the BESEP benchmark should be identified. However, this task is not done because there is no case study for detailed analyses of safety impact caused by combinations of external hazards.

6.1 Combinations of external hazards in the safety assessments of partner countries

The combinations of external hazards involved in the safety assessments of BESEP partner countries are described below.

Czech Republic

The analyses are in progress. For Dukovany NPP, 1954 combinations were selected finally, 1613 classified as independent, 292 as correlated, 49 as consequential (very similar numbers are valid for Temelin NPP).

The preliminary results of comparison of CDF and LERF caused by various external hazards treated just as single ones with the updated results, where the impact of each external hazard includes also its occurrence in combination with other external hazards, is available for NPP Dukovany PSA. These results show that:
• the effect of the hazard “extreme air temperature (both low and high)” highly increased when the combinations of this hazard with other hazards was considered in the new analysis, the original CDF related to the scenario with extreme temperature as single hazard was of order of $10^9$, whereas the new result addressing also combinations with other hazards was of order of $10^7$;

• in a similar comparison, the effect of the external hazard extreme wind, measured by CDF, increased from $8.1 \times 10^{-6}$ up to $8.7 \times 10^{-6}$ – the relative increasing of CDF was much lower than for extreme temperature hazard, but the effect on the absolute CDF value was almost the same as for extreme temperatures;

• no other significant increasing of CDF (or LERF) for the other external hazards due to addressing combinations of them was identified, i.e., the risk impact is dominated by the single hazards in all other cases (however, this view can change in future after more detailed analysis of the impact of hazards combinations).

**Finland and Sweden**

Combinations of external hazards considered in PSA ($X = \text{considered at more than one plant}$) [22]:

<table>
<thead>
<tr>
<th>Combination</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A01-A04</td>
<td>Strong wind - Low air temperature</td>
</tr>
<tr>
<td>A01-A06</td>
<td>Strong wind - Extreme rain</td>
</tr>
<tr>
<td>A01-A07</td>
<td>Strong wind - Extreme snow</td>
</tr>
<tr>
<td>A01-G07</td>
<td>Strong wind - External fire</td>
</tr>
<tr>
<td>A01-W02</td>
<td>Strong wind - Low sea (river) water level</td>
</tr>
<tr>
<td>A01-W03</td>
<td>Strong wind - High sea (river) water level</td>
</tr>
<tr>
<td>A01-W07</td>
<td>Strong wind - Surface ice (sea)</td>
</tr>
<tr>
<td>A01-W08</td>
<td>Strong wind - Frazil ice (sea)</td>
</tr>
<tr>
<td>A01-W09</td>
<td>Strong wind - Ice ridge/pack (sea)</td>
</tr>
<tr>
<td>A01-W10</td>
<td>Strong wind - Organic material in sea water</td>
</tr>
<tr>
<td>A01-W12</td>
<td>Strong wind - Solid or liquid water pollution (from ships)</td>
</tr>
<tr>
<td>A01-W13</td>
<td>Strong wind - Chemical water releases</td>
</tr>
<tr>
<td>A02-A06</td>
<td>Tornado - Extreme rain</td>
</tr>
<tr>
<td>A02-A14</td>
<td>Tornado - Lightning</td>
</tr>
<tr>
<td>A03-W04</td>
<td>High air temperature - High sea (river) water temperature</td>
</tr>
<tr>
<td>A04-A07</td>
<td>Low air temperature - Extreme snow</td>
</tr>
<tr>
<td>A06-A14</td>
<td>Extreme rain - Lightning</td>
</tr>
<tr>
<td>A07-W08</td>
<td>Extreme snow - Frazil ice (sea)</td>
</tr>
<tr>
<td>A14-W04</td>
<td>Lightning - High sea (river) water temperature</td>
</tr>
</tbody>
</table>

**France**

The regulatory context is the same as for single external hazards.

**Deterministic Hazard Analysis:** The deterministic approach used for defining hazard combinations consists, firstly in identifying the different types of combination (consequential, correlated or independent hazards) and then to identify those of each type, on the basis of a pragmatic approach based on expertise and feedback. The site-specific list of single external hazards constitutes a basis for defining hazard combinations.

**Hazard PSA:** The first screening of combinations of hazards is done in the frame of the 4th PSR of 1300 MWe NPPs. In France there are no methodology documents in place for the development of hazards PSA or PSA for hazard combinations. Only screened in external hazard or combinations of external hazards which are judged relevant will be explicitly modeled in PSA models. Relevance depends on state of the art, available data for hazards characterization and safety issues. Simplified probabilistic analysis are currently underway regarding these relevant combinations.

Regarding the 1300MWe series, 15 external hazards combinations were screened in. Only 8 combination of external hazards will be explicitly modeled in PSA models if feasible:

- Airplane crash and air pressure wave ;
- Air pressure wave and toxic flammable or asphyxiating gas or liquid discharges ;
- Riverine flooding and waves induced by local wind ;
- Seaside overtopping (waves, wind, surge) ;
- Capacity failure on site and earthquake;
- Wind and intake clogging;
- Tornado and hail;
- Tornado and lightning.

These PSA has not been performed yet. EDF also wants to point out that this list is site dependent and cannot be directly applicable for other sites and other designs.

**Hungary**

The following combinations of external hazards need detailed assessment in relation to both the design basis as well as the PSA of the Paks NPP:

- storm: high wind and extreme precipitation and thunder,
- snowstorm: high wind and extreme snow,
- extremely high temperature conditions: extremely high air temperature and high Danube water temperature,
- extremely low temperature conditions: extremely low air temperature and surface ice on the Danube (and icing and snow),
- earthquake and soil liquefaction,
- earthquake and extremely high or low air temperature (independent),
- simultaneous accidents in nearby industrial facilities that handle dangerous chemical substances (due to a common root cause, e.g., earthquake, tornado),
- extreme meteorological conditions and handling of dangerous substances (the meteorological conditions may have a significant impact on the spread and dispersion of dangerous substances).

**Slovak Republic**

Combinations of external hazards in the focus of safety assessments [7]:

- Tornado - Lightning
- Tornado - Extreme rain
- Icing - Extreme snow
- Lightning - Extreme rain
- Lightning - Extreme wind
- Low air temperature - Extreme wind
- Low air temperature - Icing
- Extreme rain - Extreme wind
- Extreme snow - Extreme wind
- Extreme wind - Icing
- Extreme wind - Extreme snow - Icing

The contribution of combinations of external hazards to the risk is negligible.

6.2 Selection of external hazard combinations from the preliminary case studies

There is no case study for detailed analyses of safety impact caused by combinations of external hazards. The case study A.9 from Appendix A of this report is limited to the screening process of combinations. In the case study A.8 is no intention to perform analyses of safety impact for simultaneous occurrence of earthquake and extreme weather. The suggestion of the authors of the report is that this issue can be finalized after all project partners provide their contributions to case studies in the later phase of the project.
7 Assignment of safety requirement topics to external hazards

The overall plant specific evaluations are utilizing the concept of defence in depth. In a full scope safety evaluation against external hazards all layers of defence in depth are assessed. These layers may be intrinsic or extrinsic, on-site or off-site, and related to safety, security or a combination. Some layers are related to prevention (prevention of external hazards from adversely impacting the nuclear power plant) and others to mitigation when, for example, core damage is considered the consequence of external hazards.

There are five levels of defence in depth, described in Appendix B of this report: 1) normal operation, 2) anticipated operational occurrences, 3) design basis accidents, 4) design extensions conditions without significant core degradation, 5) design extensions conditions with core melting.

The government and the plant operator share the responsibility of the defence in depth as a whole. At level 1, external hazards are occurring or initiated outside the plant boundary. Consequently, there is a shared responsibility between the government organizations to prevent external hazard (mainly human-induced hazards) from occurring. At levels 2 - 4, if external hazards are occurring, the operator has the majority of responsibility. However, there is an understanding of approach between government organizations and the responsible plant personnel. At level 5, emergency response activities clearly involve the government, not only the operator. Hence, the related activities are also interdependent. A coordination plan is the key element to ensure coordination of off-site and on-site activities. A coordination plan is to be established for the integration of on-site and off-site action plans. The coordination plan needs to define roles and responsibilities, communication (including command and control, alarms, responsible government organizations, media, public) and emergency response coordination with existing procedures.

Two modelling and evaluation approaches are the tools in the plant specific evaluation process: safety margin assessment (SMA) and probabilistic safety assessment (PSA). Human factors engineering (HFE) is used to increase reliability of plant personnel. These methods are discussed in detail in chapter 2, 3 and 4 of this report.

The methodologies for existing and for new nuclear power plants are basically the same. The differences are that new plants have a focus on explicitly considering some external hazards in the design process. Such external hazards may not have been recognized at the time of the design of existing plants. In other words, beyond design external hazards were not taken into account in the design process of most existing plants.

There are distinct differences between the evaluation of existing plants for beyond design external hazards and the design of new plants when these external hazards are subjected. The obvious difference is that the physical existence of the existing plant limits the physical modifications that can be implemented easily or at all. Hence, management of external hazard induced scenarios for existing plants will rely on the robustness of the existing designs, relatively small physical modifications (if deemed necessary and cost effective), operational or procedural changes, and emergency management (e.g. EME and FLEX). These modifications are part of the safety engineering process (SEP) for implementing safety requirements to the plant for fulfilling the defence in depth principle.

There are many events for which area dependent evaluations are performed for design basis external hazards and for design extension external hazards. Three examples are security events: 1) design basis threats and beyond design basis threats, 2) internal and external fires, and 3) internal and external floods. In the case of physical protection systems, security evaluations are based on identifying vital areas and protecting those vital areas. A vital area is an area within the protected area containing safety related equipment, systems, devices or nuclear material, the damage of which could directly or indirectly lead to unacceptable radiological consequences.

Depending on the safety philosophy of the nuclear power plant (and the government), the set of vital areas could include all designated safety systems or a subset of safety systems and equipment. The number of vital areas and their extent depend on the physical protection philosophy of the government. In some countries all safety related items are to be protected. This translates into a small number of vital areas, but with very large areal extent (e.g. an entire building might be defined as one vital area). Alternatively, a minimum set of equipment may be a subset. This latter philosophy would be parallel to the SMA approach to external hazards.

In the case of fire and flood, location dependent evaluations are also implemented and can be used to assess the survivability of a minimum subset of SSCs. Location dependency is especially true when one assumes items in a compartment fail when fire or flood engulf the compartment. In that case, survivability is
100% dependent on location. It is important to note that existing models and results can be used in the development of the elements of the evaluation methodology. These models could be probabilistic or deterministic (i.e. event or fault tree or success path based).

The three fundamental safety functions to be maintained for external hazards imposed on the nuclear reactor are control of reactivity, fuel cooling and confinement of radioactive material. To achieve these safety functions, front line and support systems are required to perform their functions. As part of the front line and support systems, essential monitoring and control capabilities are required. Additional conditions to be met are integrity of the spent fuel pool and availability of spent fuel pool cooling under the loading conditions of external hazards.

External plant conditions are conditions which exist in the surrounding areas of the nuclear power plant that may be a help in preventing the consequences of the external hazards. Typical conditions that would be helpful in preventing an external hazard from having a significant effect on the nuclear power plant and the surrounding area are administrative controls on potential sources of these events implemented by the government:
- Buffer zones in the air, land and water, for example maintaining hazardous material boundaries outside the plant boundary and so preventing vehicles from entering areas where explosions or hazardous material releases could affect the nuclear power plant;
- Maintaining no-fly zones around the nuclear power plant;
- Maintaining a buffer zone of no combustibles on the land around the plant boundary.

A typical condition that would be a hindrance to preventing an external hazard from having a significant effect on the nuclear power plant and the surrounding area is high population density in the vicinity of the nuclear power plant.

The overall methodology deals with acceptance criteria, which may be in the form of end metrics:
- Risk oriented, for example core damage frequency, large early release frequency, total effective dose equivalent to personnel and total effective dose equivalent to the public.
- Capacity oriented, for example conservative containment capacity when subjected to specified aircraft impact loads, best estimate capacity (only slightly conservatively biased).

Acceptance criteria may expand on to the SSC level:
- Systems requirements: The number of safety trains to be protected or demonstrated to be available, including capacities of SSCs in the safety trains.
- SSC capacity values: treating the loading environment as best estimate and the resistance of SSC in the same manner, or conservatively defining the loading environment and conservatively defining the systems acceptance criteria, for example demonstrate one or two trains of safety systems to be verified to perform (redundancy).

In summary, the general procedure for plant specific evaluation consists of:
- Event and load characterization: This is the input to the plant specific evaluation.
- Systems analysis: Depending on the selected approach (SMA or PSA), success paths or failure paths are identified for each event given as input.
- SSC: Using the results of the systems analysis and the area review, a list of SSCs required to perform the selected safety functions under the plant conditions generated by the considered external hazards is compiled for capacity assessment.
- Area dependent event evaluation: Areas of influence corresponding to external hazards are assessed in order to identify the portions of the plant at which SSCs will likely not be available to perform their intended safety functions.
- Assessment of SSCs: Performance of selected SSCs for the loading conditions given as input is assessed. As a result of the assessment, SSCs not able to perform their intended safety functions are identified.
- Assessment of plant performance: Using the results of the systems analysis and the assessment of SSCs carried out in the previous step, the overall performance of the plant to keep the fundamental safety functions under the external hazards is assessed.
- Acceptability of plant performance: Plant performance is assessed against the acceptance criteria.

A very important element to emphasize is that the evaluation of safety against external hazards is very much a multidisciplinary activity. It involves specialists with expertise in safety engineering, operations, engineering (e.g. civil, structural, mechanical, electrical, instrumentation and control, and geotechnical) and emergency response. The interaction of these disciplines is essential to obtaining a holistic approach to dealing with design extension external hazards [24].
The objective of BESEP project is to develop best practices for safety requirements verification against external hazards. The project will support this objective by using efficient and integrated set of safety engineering practices and PSA.

For the benchmark exercise, case study descriptions are collected from the project partners. In the case studies different safety analyses on plant SSCs against external hazards have been conducted previously by the project partners. The case studies are grouped to case study groups using a set of requirements that will be determined in accordance with a benchmark baseline. These requirements will include the major attributes that will form the basis of grouping, such as safety requirements to be met, types of safety analyses, similarity of the external hazards and the SSCs, etc.

During the benchmark exercise two comparisons are carried out: 1) comparison of individual case studies within a case study group; and 2) comparison of different case study groups. The comparison between individual case studies evaluates the efficiency and integration of different safety analysis methods. The comparison between different case study groups evaluates the number and depth of analyses performed taking the risk significance of external hazards to plant safety into consideration. Both comparisons are done to support the project objective to support safety margins determination and safety requirements verification against external hazards using efficient and integrated set of safety engineering practices and probabilistic safety assessment. The overall structure of the benchmark exercise is illustrated in Figure 7.1. The figure shows an example of three case study groups. For each case study group it is defined a set of safety requirements on specific topic of interest (marked in blue boxes), specific SSCs (marked in green boxes) and specific external hazard (marked in red boxes). The notations of Figure 7.1 are only for demonstration purposes and the actual set of safety requirements, SSC and external hazards are determined during the project [14].

Several safety requirement topics were assigned to each external hazard from the case studies using the recommended list of IAEA safety requirements, see chapter 7.3 – 7.13 below.

All countries, involved in BESEP, have safety requirements and safety goals, but these are expressed in many different ways. The differences in the requirements from different countries are difficult to resolve as the goals are derived using different principles and assumptions and are given for a specific reactor technology.

To achieve the above mentioned objective, it is necessary to have a degree of convergence on the safety requirements and safety goals that are required to be met by plant designers and operators.

The following natural and human induced hazards are involved in preliminary case studies of BESEP (this list of external hazards can be modified in a later stage of the project):

- Natural non-seismic and seismic hazards:
  - extreme wind;
  - tornado;
  - extreme snow;
At the present time the combinations of external hazards for the site are not involved in the preliminary case studies. This issue can be implemented into the project in its later phase.

7.1 Overview of the IAEA safety requirements

The IAEA safety requirements are described in Appendix B [2,10] of this report. In addition, the principles of protection against external hazards and design for external hazards are described in this Appendix [13].

This part of the report provides condensed overview of the IAEA safety requirements. The overarching safety requirements for nuclear power plants are the following [2]:

- **Management of safety in design.** General requirements to be satisfied by the design organization in the management of safety in the design process.
- **Principal technical requirements.** Requirements for principal technical design criteria for safety, including requirements for the fundamental safety functions, the application of defence in depth and provision for construction; requirements for interfaces of safety with nuclear security and with the State system of accounting for, and control of, nuclear material; and requirements for ensuring that radiation risks arising from the plant are maintained as low as reasonably achievable.
- **General plant design.** Requirements for general plant design that supplement the requirements for principal technical design criteria to ensure that safety objectives are met, and the safety principles are applied. The requirements for general plant design apply to all SSCs important to safety.
- **Design of specific plant systems.** Requirements for the design of specific plant systems such as the reactor core, reactor coolant systems, containment system, and instrumentation and control systems.

7.1.1 Management of safety in design

The following requirements are involved:

Requirement 1: Responsibilities in the management of safety in plant design
Requirement 2: Management system for plant design
Requirement 3: Safety of the plant design throughout the lifetime of the plant

7.1.2 Principal technical safety requirements

The following requirements are involved:

Requirement 4: Fundamental safety functions
Requirement 5: Radiation protection in design
Requirement 6: Design for a nuclear power plant
Requirement 7: Application of defence in depth
Requirement 8: Interfaces of safety with security and safeguards
Requirement 9: Proven engineering practices
Requirement 10: Safety assessment
Requirement 11: Provision for construction
Requirement 12: Features to facilitate radioactive waste management and decommissioning
7.1.3 General plant design

7.1.3.1 Design basis

The following requirements are involved:

Requirement 13: Categories of plant states
Requirement 14: Design basis for items important to safety
Requirement 15: Design limits
Requirement 16: Postulated initiating events
Requirement 17: Internal and external hazards
Requirement 18: Engineering design rules
Requirement 19: Design basis accidents
Requirement 20: Design extension conditions
Requirement 21: Physical separation and independence of safety systems
Requirement 22: Safety classification
Requirement 23: Reliability of items important to safety
Requirement 24: Common cause failures
Requirement 25: Single failure criterion
Requirement 26: Fail-safe design
Requirement 27: Support service systems
Requirement 28: Operational limits and conditions for safe operation

7.1.3.2 Design for safe operation over the lifetime of the plant

The following requirements are involved:

Requirement 29: Calibration, testing, maintenance, repair, replacement, inspection and monitoring of items important to safety
Requirement 30: Qualification of items important to safety
Requirement 31: Ageing management

7.1.3.3 Human factors

The only requirement involved is Requirement 32: Design for optimal operator performance

7.1.3.4 Other design consideration

The following requirements are involved:

Requirement 33: Safety systems, and safety features for design extension conditions, of units of a multiple unit nuclear power plant
Requirement 34: Systems containing fissile material or radioactive material
Requirement 35: Nuclear power plants used for cogeneration of heat and power, heat generation or desalination
Requirement 36: Escape routes from the plant
Requirement 37: Communication systems at the plant
Requirement 38: Control of access to the plant
Requirement 39: Prevention of unauthorized access to, or interference with items important to safety
Requirement 40: Prevention of harmful interactions of systems important to safety
Requirement 41: Interactions between the electrical power grid and the plant

7.1.3.5 Safety analyses

The only requirement involved is Requirement 42: Safety analysis of the plant design
7.1.4 Design of specific plant systems

7.1.4.1 Reactor core and associated features

The following requirements are involved:

Requirement 43: Performance of fuel elements and assemblies  
Requirement 44: Structural capability of the reactor core  
Requirement 45: Control of the reactor core  
Requirement 46: Reactor shutdown

7.1.4.2 Reactor coolant system

The following requirements are involved:

Requirement 47: Design of reactor coolant systems  
Requirement 48: Overpressure protection of the reactor coolant pressure boundary  
Requirement 49: Inventory of reactor coolant  
Requirement 50: Clean up of reactor coolant  
Requirement 51: Removal of residual heat from the reactor core  
Requirement 52: Emergency cooling of the reactor core  
Requirement 53: Heat transfer to an ultimate heat sink

7.1.4.3 Containment structure and containment system

The following requirements are involved:

Requirement 54: Containment system for the reactor  
Requirement 55: Control of radioactive releases from the containment  
Requirement 56: Isolation of the containment  
Requirement 57: Access to the containment  
Requirement 58: Control of containment conditions

7.1.4.4 Instrumentation and control system

The following requirements are involved:

Requirement 59: Provision of instrumentation  
Requirement 60: Control systems  
Requirement 61: Protection system  
Requirement 62: Reliability and testability of instrumentation and control systems  
Requirement 63: Use of computer-based equipment in systems important to safety  
Requirement 64: Separation of protection systems and control systems  
Requirement 65: Control room  
Requirement 66: Supplementary control room  
Requirement 67: Emergency response facilities on the site

7.1.4.5 Emergency power supply

The only requirement involved is Requirement 68: Design for withstanding the loss of off-site power

7.1.4.6 Supporting systems and auxiliary systems

The following requirements are involved:

Requirement 69: Performance of supporting systems and auxiliary systems  
Requirement 70: Heat transport systems  
Requirement 71: Process sampling systems and post-accident sampling systems  
Requirement 72: Compressed air systems  
Requirement 73: Air conditioning systems and ventilation systems.
Requirement 74: Fire protection systems
Requirement 75: Lighting systems
Requirement 76: Overhead lifting equipment

7.1.4.7 Power conversion systems

The only requirement involved is Requirement 77: Steam supply system, feedwater system and turbine generators

7.1.4.8 Treatment of radioactive waste

The following requirements are involved:

Requirement 78: Systems for treatment and control of waste
Requirement 79: Systems for treatment and control of effluents

7.1.4.9 Fuel handling system

The only requirement involved is Requirement 80: Fuel handling and storage systems

7.1.4.10 Radiation protection

The following requirements are involved:

Requirement 81: Design for radiation protection
Requirement 82: Means of radiation monitoring

7.2 Assignment of safety requirement topics

Postulated initiating events of the plant can occur after SSCs failures arising from an external hazard in full power, low power or shutdown states. Initiating events of the spent fuel pool also can occur. Therefore, safety assessments (Requirement 10: Safety assessment) and safety analysis (Requirement 42: Safety analysis of the plant design) are to be undertaken as a means of evaluating compliance with safety requirements for the plant and to determine the safety measures that need to be taken to ensure safety. In addition, to improve the plant safety also human factors engineering and safety engineering processes can be implemented into the plant design.

The following safety analyses and safety engineering processes 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, see chapter 2
2. Probabilistic safety analyses (PSA) – modelling of accident sequences, quantification of their risk significance, see chapter 3
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, SAMGs, procedures EME and FLEX, see chapter 4
4. Safety engineering process (SEP) – implementation of safety requirements to existing plant design for fulfilling the Defence in Depth principle.

A subjective view on the relation of relevant safety requirements with the safety analyses, safety engineering processes and the different external hazard categories is given in Tables 7.1 and 7.2. The tables are created solely to support the safety requirements allocation in the BESEP benchmark exercise. Therefore, the interpretations from the tables should not be extended outside the project.

Table 7.1 identifies the relevant requirements to each of four categories (DSA, PSA, HFE, SEP). It means that the given type of analyses and engineering application have been the traditional and primary ways to show how the safety requirements are met.
Table 7.2 identifies the relation of three hazard categories (defined as seismic hazard, non-seismic hazard and human-induced hazard) for each safety requirement. It means that the hazards have been the traditional and primary categories when considering for the fulfilment of the requirements.

The information from Tables 7.1 and 7.2 can be used to identify the safety requirement topics for the individual external hazards relevant for the BESEP benchmark exercise.

Table 7.1 The connection of safety requirements and the means to ensure plant safety.

<table>
<thead>
<tr>
<th>SAFETY REQUIREMENTS</th>
<th>DSA</th>
<th>PSA</th>
<th>HFE</th>
<th>SEP</th>
</tr>
</thead>
<tbody>
<tr>
<td>PRINCIPAL TECHNICAL SAFETY REQUIREMENTS</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Requirement 4: Fundamental safety functions</td>
<td>x</td>
<td></td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Requirement 7: Application of defence in depth</td>
<td></td>
<td></td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Requirement 8: Interfaces of safety with security and safeguards</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>DESIGN BASIS</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Requirement 16: Postulated initiating events</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Requirement 17: Internal and external hazards</td>
<td></td>
<td></td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Requirement 21: Physical separation and independence of safety systems</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Requirement 23: Reliability of items important to safety</td>
<td></td>
<td></td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Requirement 24: Common cause failures</td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Requirement 25: Single failure criterion</td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>HUMAN FACTORS</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Requirement 32: Design for optimal operator performance</td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>OTHER DESIGN CONSIDERATIONS</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Requirement 40: Prevention of harmful interactions of systems important to safety</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Requirement 41: Interactions between the electric grid and the plant</td>
<td>x</td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>SAFETY ANALYSIS</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Requirement 42: Safety analysis of the plant design</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>REACTOR COOLANT SYSTEM</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Requirement 51: Removal of residual heat from the reactor core</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Requirement 52: Emergency cooling of the reactor core</td>
<td></td>
<td></td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Requirement 53: Heat transfer to an ultimate heat sink</td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>CONTAINMENT</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Requirement 54: Containment system for the reactor</td>
<td></td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Requirement 55: Control of radioactive releases from the containment</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Requirement 56: Isolation of the containment</td>
<td></td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>INSTRUMENTATION AND CONTROL SYSTEM</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Requirement 62: Reliability and testability of instrumentation and control systems</td>
<td>x</td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Requirement 63: Use of computer-based equipment in systems important to safety</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Requirement 65: Control room</td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Requirement 66: Supplementary control room</td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Requirement 67: Emergency response facilities on the site</td>
<td></td>
<td></td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>EMERGENCY POWER SUPPLY</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Requirement 68: Design for withstanding the loss of off-site power</td>
<td>x</td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>SUPPORTING AND AUXILIARY SYSTEM</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Requirement 69: Performance of supporting systems and auxiliary systems</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
</tr>
</tbody>
</table>
Table 7.2. The most important hazard category for each safety requirement.

<table>
<thead>
<tr>
<th>Requirements</th>
<th>Seismic hazard</th>
<th>Non-seismic natural hazard</th>
<th>Human – induced hazard</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requirement 70: Heat transport systems</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Requirement 73: Air conditioning systems and ventilation systems</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
</tbody>
</table>

PRINCIPAL TECHNICAL REQUIREMENTS

| Requirement 4: Fundamental safety functions | x | (x) | (x) |
| Requirement 7: Application of defence in depth | x |     | x   |
| Requirement 8: Interfaces of safety with security and safeguards |     |     | x   |

DESIGN BASIS

| Requirement 16: Postulated initiating events | (x) |
| Requirement 17: Internal and external hazards | (x) |
| Requirement 21: Physical separation and independence of safety systems | x |
| Requirement 23: Reliability of items important to safety | (x) |
| Requirement 24: Common cause failures | x |
| Requirement 25: Single failure criterion | (x) |

HUMAN FACTORS

| Requirement 32: Design for optimal operator performance | (x) |

OTHER DESIGN CONSIDERATIONS

| Requirement 40: Prevention of harmful interactions of systems important to safety | (x) |
| Requirement 41: Interactions between the electrical power grid and the plant | x |

SAFETY ANALYSIS

| Requirement 42: Safety analysis of the plant design | (x) | x | (x) |

REACTOR COOLANT SYSTEMS

| Requirement 51: Removal of residual heat from the reactor core | x |
| Requirement 52: Emergency cooling of the reactor core | x |
| Requirement 53: Heat transfer to an ultimate heat sink | x |

CONTAINMENT STRUCTURE AND CONTAINMENT SYSTEM

| Requirement 54: Containment system for the reactor | x |
| Requirement 55: Control of radioactive releases from the containment | x |
| Requirement 56: Isolation of the containment | x |

INSTRUMENTATION AND CONTROL SYSTEMS

| Requirement 62: Reliability and testability of instrumentation and control systems | x |
| Requirement 63: Use of computer based equipment in systems important to safety | x |
| Requirement 65: Control room | x |
| Requirement 66: Supplementary control room | x |
| Requirement 67: Emergency response facilities on the site | x |

EMERGENCY POWER SUPPLY

| Requirement 68: Design for withstanding the loss of off-site power | x |

SUPPORTING SYSTEMS AND AUXILIARY SYSTEMS

| Requirement 69: Performance of supporting systems and auxiliary systems | x |
Requirements 70: Heat transport systems
Requirements 73: Air conditioning systems and ventilation systems

x = primary determining hazard; (x) = partially determining hazard

7.3 Extreme winds

Extreme winds constitute an important loading condition to all types of above-ground structures of the nuclear power plant. Extreme winds produce loads on structures as a result of the induced pressures, wind-propelled missiles, atmospheric pressure change, and storm surge effects.

Based on Table 7.2 the following safety requirements are considered to be the most important against extreme wind:

- Requirement 41: Interactions between the electrical power grid and the plant (DSA)
- Requirement 42: Safety analysis of the plant design (DSA, PSA, HFE, SEP)
- Requirement 51: Removal of residual heat from the reactor core (DSA)
- Requirement 52: Emergency cooling of the reactor core (DSA)
- Requirement 53: Heat transfer to an ultimate heat sink (DSA)
- Requirement 68: Design for withstanding the loss of off-site power (DSA, PSA)
- Requirement 69: Performance of supporting systems and auxiliary systems (DSA, PSA, SEP)
- Requirement 70: Heat transport systems (DSA)
- Requirement 73: Air conditioning systems and ventilation systems (DSA, PSA)

Type of analyses and engineering applications from Table 7.1 are presented in parentheses to show the adequate way for achievement the safety requirements.

7.3.1 Extreme wind hazard analyses

Deterministic and probabilistic wind hazard analyses are needed for the site of the plant.

Wind hazard analysis consists of the development of probabilistic statements on the long-term windspeeds. These statements can be represented by probability distribution functions or expressed as discrete probabilities for specified windspeeds. The results are generally given as windspeed exceedance probabilities for a specified time period, usually 1 year. A plot of windspeed versus annual frequency of exceedance (called the wind hazard curve) is developed.

Uncertainties in the mean hazard functions or curve are generally ignored in deterministic hazard analyses. However, in PSAs, the uncertainties are often represented through a family of curves, accounting for uncertainties and modelling errors. (This concept is discussed in more detail in chapter 3 of this report.) It is important to note that, for wind-sensitive structures, the wind hazard analysis requires the development of joint probability functions of windspeed and direction.

The development of the wind hazard function begins with the analysis of available wind data, generally in the form of windspeed measurements at the site. All windspeed versus probability of exceedance curves correspond to a specific averaging time, height above ground, and terrain roughness.

Hazard curves are needed for the plants whose failure has significant economic or public health consequences (used in the plant PSA). For plant buildings the design windspeeds are generally based on 10 000-year mean return period winds.

After the windspeeds are converted to the 10 m level the windspeed exceedance frequencies are predicted using extreme value theory (see chapter 3).

The following analyses are needed to confirm that the plant fulfils the safety requirements identified above:

DSA: deterministic wind hazard analyses
PSA: probabilistic wind hazards analyses
7.3.2 Extreme wind fragility analyses

Extreme wind loading effects include wind pressures which are a principal loading mechanism for all windstorm types. Wind loads on structures can be divided broadly into two classes:

1. Wind loads are due to the action of wind only and can be determined assuming the structure behaves as a rigid body. Structures that fall into this class are typically low-rise buildings.
2. Wind loads are associated with a combination of the direct action of the wind on the structure and the dynamic response of the structure itself. These dynamically sensitive structures can be further divided into categories: structures where forces induced by the motion of the structure can be ignored (most tall buildings), and structures where the motion of the structure strongly influences the wind loads. The latter category includes tall slender buildings and venting stacks.

The wind fragility analyses estimate structural failure probability due to wind effects. The wind capacity of the SSCs is calculated using deterministic fragility analyses. Failure probabilities are computed using fragility curves for SSCs in the PSA.

The following analyses are needed to confirm that the plant fulfils the safety requirements identified above:

DSA: deterministic wind fragility analyses
PSA: probabilistic wind fragility analyses

7.3.3 Plant response analyses to extreme wind

The plant response analyses to extreme wind involves hazard and fragility analyses, analyses of interactions between the structures and plant model development.

Deterministic and probabilistic response analyses are performed (see chapter 2 and 3). Within the deterministic response analyses the wind capacity is calculated for the plant. PSAs calculate the contribution of extreme wind to CDF and LERF.

The following analyses are needed to confirm that the plant fulfils the safety requirements:

DSA: deterministic plant response analyses for extreme wind
PSA: probabilistic plant response analyses for extreme wind

7.4 Tornado

Tornado loading effects include, principally, the aerodynamic forces produced by the dynamic pressure component of the wind flow and impact forces produced by objects picked up and accelerated by the wind field. The other load effect is the atmospheric pressure change associated with the low central pressure region within tornadoes. The wind pressure is also a relevant impact of tornado.

Based on Table 7.2 the following safety requirements are considered to be the most important against tornado:

- Requirement 41: Interactions between the electrical power grid and the plant (DSA)
- Requirement 42: Safety analysis of the plant design (DSA, PSA, HFE, SEP)
- Requirement 51: Removal of residual heat from the reactor core (DSA)
- Requirement 52: Emergency cooling of the reactor core (DSA)
- Requirement 53: Heat transfer to an ultimate heat sink (DSA)
- Requirement 68: Design for withstanding the loss of off-site power (DSA, PSA)
- Requirement 69: Performance of supporting systems and auxiliary systems (DSA, PSA, SEP)
- Requirement 70: Heat transport systems (DSA)
- Requirement 73: Air conditioning systems and ventilation systems (DSA, PSA)

Type of analyses and engineering applications from Table 7.1 are presented in parentheses to show the adequate way for achievement the safety requirements.
7.4.1 Tornado hazard analyses

A tornado is a violently rotating column of air whose circulation reaches the ground, and is often observable as a condensation funnel attached to the cloud base or as a rotating dust cloud rising from the ground. Key aspects of tornado hazard analysis include databases, windspeed transformations from observed damage, and the integration of these elements into a hazard model.

Tornado databases include position, time, size, and central pressure. Indirect databases including damage path parameters provide the main source of data for hazard analysis. Indirect wind data are used in the development of site-specific tornado hazard curves. Databases that include tornado occurrences, path dimensions, and damage intensity are coupled with relations of damage to windspeed to develop tornado hazard curves. Because of the limitations of these indirect databases, tornado hazard curves are subject to considerable uncertainty, particularly for gust windspeeds (2- to 3-sec averages).

Tornado hazard analyses have been performed by a number of investigators for a variety of purposes by deterministic and probabilistic methods.

The following analyses are needed to confirm that the plant fulfils the safety requirements:

DSA: deterministic tornado hazard analyses
PSA: probabilistic tornado hazards analyses

7.4.2 Tornado fragility analyses

Tornado loading effects include missiles, wind pressure and atmospheric pressure change. Wind-borne missiles are generally considered only in tornado-resistant design. Atmospheric pressure change loads are limited also to tornadoes.

Two basic approaches have been used in tornado missile analysis. The traditional deterministic approach uses a spectrum of several missile types and maximum velocities to be considered in design. Using a tornado windfield model and a missile trajectory model, maximum missile speeds are calculated for each missile type. A design spectrum is developed that is intended to envelope the missile impact effects conservatively from a broad class of missiles. These analyses use simplified three-degrees-of-freedom (3-D) trajectory models and an average drag coefficient.

The second approach is based on a probabilistic analysis covering a much broader class of potential missiles. Probabilities of missile impact and damage are estimated for each structure or component. These results can be used directly in PSAs.

Both deterministic and probabilistic methods to evaluate missile effects require tornado windfield and trajectory models to predict the characteristic velocities of missiles. The impact effects are generally evaluated using empirically-based penetration, perforation, or spall equations. For certain types of missile, overall dynamic response analysis may also be required.

Atmospheric pressure change (APC) loads are of practical engineering significance only for tornadoes, with the combination of relatively high translational storm speed and maximum pressure drop in the centre of a rapidly rotating vortex. For a perfectly sealed structure, the APC produces outward-acting pressures across all surfaces of the structure. The estimation of APC loads requires a model of the tornado windfield and knowledge of the rate at which the structure may vent. Because most buildings are not perfectly sealed, the actual pressures resulting from APC may be much less and are often negligible for structures with typical venting features.

The tornado fragility analyses estimate structural failure probability due to tornado effects. Tornado capacity of the SSCs is calculated using deterministic fragility analyses. Failure probabilities are computed using fragility curves for SSCs in the PSA. Adequate protection of SSCs against tornado using safety engineering processes must be taken into consideration.

The following analyses and safety engineering process are needed to confirm that the plant fulfils the safety requirements:
**7.4.3 Plant response analyses to tornado**

The plant response analysis to tornado involves hazard and fragility analyses, analyses of interactions between the structures and plant model development.

Deterministic and probabilistic response analyses are performed (see chapter 2 and 3). Within the deterministic response analyses the tornado capacity of the plant is calculated. PSAs calculate the contribution of tornado to CDF and LERF.

The following analyses are needed to confirm that the plant fulfils the safety requirements:

- **DSA:** deterministic plant response analyses to tornado
- **PSA:** probabilistic plant response analyses to tornado

**7.5 Extreme snow**

Snow induced damage is usually represented by the unavailability of the power supply or the electrical grid, but snow could also affect ventilation intakes and discharges, structural loading (water pressure in the snow), access by the operator to external safety related facilities and mobility of emergency vehicles.

Based on Table 7.2 the following safety requirements are considered to be the most important against extreme snow:

- Requirement 41: Interactions between the electrical power grid and the plant (DSA)
- Requirement 42: Safety analysis of the plant design (DSA, PSA, HFE, SEP)
- Requirement 51: Removal of residual heat from the reactor core (DSA)
- Requirement 52: Emergency cooling of the reactor core (DSA)
- Requirement 53: Heat transfer to an ultimate heat sink (DSA)
- Requirement 68: Design for withstanding the loss of off-site power (DSA, PSA)
- Requirement 69: Performance of supporting systems and auxiliary systems (DSA, PSA, SEP)
- Requirement 70: Heat transport systems (DSA)
- Requirement 73: Air conditioning systems and ventilation systems (DSA, PSA)

Type of analyses and engineering applications from Table 7.1 are presented in parentheses to show the adequate way for achievement the safety requirements.

**7.5.1 Extreme snow hazard analyses**

Deterministic and probabilistic extreme snow hazard analyses are normally performed using the extreme snow database of the site. Within the deterministic analyses a design basis extreme snow is considered. In probabilistic analyses the hazard curves are constructed using the extreme value theory.

The following analyses are needed to confirm that the plant fulfils the safety requirements:

- **DSA:** deterministic extreme snow hazard analyses
- **PSA:** probabilistic extreme snow hazards analyses

**7.5.2 Extreme snow fragility analyses**

The load derivation follows the evaluation of the extreme values for the quantities of interest, which define also the duration of such conditions, their periodicity and their reasonable combination with other load cases, such as wind.
The fragility analyses estimate structural failure probability due to extreme snow effects. Extreme snow capacity is calculated using deterministic fragility analyses for the plant. Failure probabilities are computed using fragility curves for SSCs in the PSA.

Human interactions have impact on the structural fragility, for example by removing the snow from roofs of the buildings on the basis of the pre-hazard procedures and implementation of safety engineering process.

The following analyses and safety engineering processes are needed to confirm that the plant fulfils the safety requirements:

DSA: deterministic extreme snow fragility analyses
PSA: probabilistic extreme snow fragility analyses
HFE: adequate use of procedures and adequate human interactions against extreme snow
SEP: availability of adequate equipment and installations against extreme snow

7.5.3 Plant response analyses to extreme snow

The plant response analysis to extreme snow involves hazard and fragility analyses, analyses of human factors engineering, safety engineering process and plant model development.

Deterministic and probabilistic response analyses are performed (see chapter 2 and 3). Within the deterministic response analyses the extreme snow capacity is calculated for the plant. PSAs calculate the contribution of extreme snow to CDF and LERF.

The following analyses and safety engineering processes are needed to confirm that the plant fulfils the safety requirements:

DSA: deterministic plant response analyses to extreme snow
PSA: probabilistic plant response analyses to extreme snow
HFE: adequate use of procedures and adequate human interactions against extreme snow
SEP: availability of adequate equipment and installations against extreme snow

7.6 Extreme rain

Extreme rain can induce external flooding of the site. In addition to rain precipitation at the site, the following sources of external flooding can be considered:

- Runoff of water from off-site precipitation;
- Snow melt — seasonal or due to volcanism;
- Failure of water retaining structures (hydrological, seismic and from faulty operation);
- Failure of natural obstruction created by landslides, ice, log or debris jams and volcanism (lava or ash);
- Sliding of avalanches and/or landslides into water bodies;
- Rising of upstream water level due to stream obstructions;
- Changes in the natural channel for a river;
- Storm surge due to tropical or extra-tropical cyclones;
- Tsunami;
- Seiche, also combined with high tides;
- Wind induced waves of the sea.

The usual methodologies for analyzing extreme local precipitation depend on modelling of intense local rain over very short time periods (a few minutes up to, say, an hour), coupled with computer-based stochastic studies, such as Monte Carlo-type analysis, to generate the likelihood of several severe rains or snows in a longer period such as an 8 h period. The limitations on these methods are principally that not enough is known about the correlations among extreme short-duration storms. Attempts have been made to develop correlations, either spatial over short distances or temporal over a few hours, based on the proposition that one can develop an understanding of how a severe storm might move (or not) in time, but these attempts have not generally been successful. This is an example of methodology. At the present time other methodologies are being developed to support this activity.
Based on Table 7.2 the following safety requirements are considered to be the most important against extreme rain:

- Requirement 42: Safety analysis of the plant design (DSA, PSA, HFE, SEP)
- Requirement 51: Removal of residual heat from the reactor core (DSA)
- Requirement 52: Emergency cooling of the reactor core (DSA)
- Requirement 53: Heat transfer to an ultimate heat sink (DSA)
- Requirement 69: Performance of supporting systems and auxiliary systems (DSA, PSA, SEP)
- Requirement 70: Heat transport systems (DSA)
- Requirement 73: Air conditioning systems and ventilation systems (DSA, PSA)

Type of analyses and engineering applications from Table 7.1 are presented in parentheses to show the adequate way for achievement the safety requirements.

7.6.1 Extreme rain hazard analyses

The frequency of external flooding at the site is based on a site-specific probabilistic hazard analysis (existing or new) that reflects recent available site-specific information. The external flooding hazard analysis uses up-to-date databases. Uncertainties in the models and parameter values are properly accounted for and fully propagated in order to obtain a family of hazard curves from which a mean hazard curve can be derived.

The following analyses are needed to confirm that the plant fulfils the safety requirements:

DSA: deterministic extreme rain hazard analyses
PSA: probabilistic extreme rain hazards analyses

7.6.2 Extreme rain fragility analyses

The objective of the fragility analysis is to identify those SSCs that are susceptible to the effects of external floods and to determine their plant-specific failure probabilities as a function of the severity of the external flood.

A flooding fragility evaluation is performed to estimate plant-specific, realistic flooding fragilities for those SSCs whose failure contributes to core damage or large early release. Human interactions have impact on the structural fragility, for example by preparing barriers against high water level on the basis of the pre-hazard procedures.

The following analyses and safety engineering processes are needed to confirm that the plant fulfils the safety requirements:

DSA: deterministic extreme rain fragility analyses
PSA: probabilistic extreme rain fragility analyses
HFE: adequate use of procedures and adequate human interactions against extreme rain
SEP: availability of adequate barriers against extreme rain

7.6.3 Plant response analyses to extreme rain

The plant response analysis to extreme rain involves hazard and fragility analyses, analyses of human factors engineering, safety engineering process and plant model development.

Deterministic and probabilistic response analyses are performed (see chapter 2 and 3). Within the deterministic response analyses the extreme rain capacity is calculated for the plant. PSAs calculate the contribution of extreme rain to CDF and LERF.

The following analyses and safety engineering processes are needed to confirm that the plant fulfils the safety requirements:

DSA: deterministic plant response analyses to extreme rain
PSA: probabilistic plant response analyses to extreme rain
7.7 Extremely high/low temperature

Extremely high temperature has been the root cause of many malfunctions in nuclear power plants, particularly affecting I&C systems, which on many occasions have generated spurious signals.

Extremely low temperatures have at times created moisture condensation in closed rooms, with consequent dropping of water onto electrical equipment causing short circuits and malfunctions. Low temperatures have also prevented the air ventilation system of some nuclear power plants from working properly, hindered proper operation of diesel generators where the fuel showed separation of paraffin, damaged the external power supply system and limited the availability of service water.

Based on Table 7.2 the following safety requirements are considered to be the most important against extremely high/low temperature:

- Requirement 42: Safety analysis of the plant design (DSA, PSA, HFE, SEP)
- Requirement 51: Removal of residual heat from the reactor core (DSA)
- Requirement 52: Emergency cooling of the reactor core (DSA)
- Requirement 53: Heat transfer to an ultimate heat sink (DSA)
- Requirement 69: Performance of supporting systems and auxiliary systems (DSA, PSA, SEP)
- Requirement 70: Heat transport systems (DSA)
- Requirement 73: Air conditioning systems and ventilation systems (DSA, PSA)

Type of analyses and engineering applications from Table 7.1 are presented in parentheses to show the adequate way for achievement the safety requirements.

7.7.1 Extremely high/low temperature hazard analyses

The frequency of extremely high/low temperature at the site is based on a site-specific probabilistic hazard analysis (existing or new) that reflects recent available site-specific information. The hazard analysis uses up-to-date databases. Uncertainties in the models and parameter values are properly accounted for and fully propagated in order to obtain a family of hazard curves from which a mean hazard curve can be derived.

The following analyses are needed to confirm that the plant fulfils the safety requirements:

DSA: deterministic extremely high/low temperature hazard analyses
PSA: probabilistic extremely high/low temperature hazards analyses

7.7.2 Extremely high/low temperature fragility analyses

The objective of the fragility analysis is to identify those SSCs that are susceptible to the effects of extremely high/low temperature and to determine their plant-specific failure probabilities as a function of the severity of the external air temperature.

A fragility evaluation related to temperature extremes is performed to estimate the vulnerability/capacity of plant-specific, real SSCs whose failures contribute to core damage or large early release.

Human interactions have impact on the SSCs fragility, for example by preparing cooling systems against high temperatures in the I&C rooms on the basis of the pre-hazard procedures.

The following analyses and safety engineering processes are needed to confirm that the plant fulfils the safety requirements:

DSA: deterministic extremely high/low temperature fragility analyses
PSA: probabilistic extremely high/low temperature fragility analyses
HFE: adequate use of procedures and adequate human interactions against high temperature
SEP: availability of adequate cooling equipment against high temperatures
7.7.3 Plant response analyses to extremely high/low temperature

The plant response analyses involve hazard and fragility analyses, analyses of human factors engineering, safety engineering process and plant model development.

Deterministic and probabilistic response analyses are performed (see chapter 2 and 3). Within the deterministic response analyses the extremely high/low temperature capacity is calculated for the plant. PSAs calculate the contribution of extremely high/low temperature to CDF and LERF.

The following analyses and safety engineering processes are needed to confirm that the plant fulfils the safety requirements:

- **DSA**: deterministic plant response analyses to extremely high/low temperature
- **PSA**: probabilistic plant response analyses to extremely high/low temperature
- **HFE**: adequate use of procedures and adequate human interactions against high temperature
- **SEP**: availability of adequate barriers against high temperature

7.8 Extreme icing on the overhead power line

Extreme icing on the overhead power line leads to loss of offsite power from the grid.

Based on Table 7.2 the following safety requirements are considered to be the most important against icing on the overhead power line:

- Requirement 41: Interactions between the electrical power grid and the plant (DSA)
- Requirement 42: Safety analysis of the plant design (DSA, PSA, HFE, SEP)
- Requirement 51: Removal of residual heat from the reactor core (DSA)
- Requirement 52: Emergency cooling of the reactor core (DSA)
- Requirement 53: Heat transfer to an ultimate heat sink (DSA)
- Requirement 68: Design for withstanding the loss of off-site power (DSA, PSA)
- Requirement 69: Performance of supporting systems and auxiliary systems (DSA, PSA, SEP)
- Requirement 70: Heat transport systems (DSA)
- Requirement 73: Air conditioning systems and ventilation systems (DSA, PSA)

Type of analyses and engineering applications from Table 7.1 are presented in parentheses to show the adequate way for achievement the safety requirements.

7.8.1 Extreme icing hazard analyses

The thickness of the ice is being measured (mm) and the weight (g) is calculated from it. The load of the ice on the conductor should be known in g/m for evaluation the impact of extreme loads.

The frequency of icing at the site is based on a site-specific probabilistic hazard analysis (existing or new) that reflects recent available site-specific information. The hazard analysis uses up-to-date databases. Uncertainties in the models and parameter values are properly accounted for and fully propagated in order to obtain a family of hazard curves from which a mean hazard curve can be derived.

The following analyses are needed to confirm that the plant fulfils the safety requirements:

- **DSA**: deterministic icing hazard analyses
- **PSA**: probabilistic icing hazards analyses

7.8.2 Extreme icing fragility analyses

A fragility evaluation is performed to estimate the capacity of plant-specific, real SSCs whose failure contributes to core damage or large early release.

The following analyses are needed to confirm that the plant fulfils the safety requirements:
7.8.3 Plant response analyses to extreme icing

The plant response analyses involve hazard and fragility analyses and plant model development.

Within the deterministic response analyses the icing capacity is calculated for the plant. PSAs calculate the contribution of icing to CDF and LERF.

The following analyses are needed to confirm that the plant fulfills the safety requirements:

DSA: deterministic plant response analyses to icing
PSA: probabilistic plant response analyses to icing

7.9 High sea level

Wind induced waves of the sea can be a source of external flooding due to high sea level. Analysis of impact is similar as in case of external flooding caused by extreme rain (see part 7.6 of the report).

7.10 Low water level in river

Intake structures for the heat transport systems directly associated with the UHS should be designed to provide an adequate flow of cooling water during seasonal water level fluctuations, as well as under credible drought conditions.

Based on Table 7.2 the following safety requirements are considered to be the most important against low water level in river:

- Requirement 42: Safety analysis of the plant design (DSA, PSA, HFE, SEP)
- Requirement 51: Removal of residual heat from the reactor core (DSA)
- Requirement 52: Emergency cooling of the reactor core (DSA)
- Requirement 53: Heat transfer to an ultimate heat sink (DSA)
- Requirement 69: Performance of supporting systems and auxiliary systems (DSA, PSA, SEP)
- Requirement 70: Heat transport systems (DSA)
- Requirement 73: Air conditioning systems and ventilation systems (DSA, PSA)

Type of analyses and engineering applications from Table 7.1 are presented in parentheses to show the adequate way for achievement the safety requirements.

7.10.1 Low water level hazard analyses

The frequency of low water level at the site is based on a site-specific probabilistic hazard analysis (existing or new) that reflects recent available site-specific information. The hazard analysis uses up-to-date databases. Uncertainties in the models and parameter values are properly accounted for and fully propagated in order to obtain a family of hazard curves from which a mean hazard curve can be derived.

The following analyses are needed to confirm that the plant fulfills the safety requirements:

DSA: deterministic low water level hazard analyses
PSA: probabilistic low water level hazard analyses

7.10.2 Low water level fragility analyses

The UHS is lost due to the external hazard. The plant safety is compromised by this event. Fragility analyses of SSCs are not required.
7.10.3 Plant response analyses to low water level

The plant response analyses involve hazard and plant response model development.

Within the deterministic response analyses the low water level capacity is calculated for the plant. PSAs calculate the contribution of low water level to CDF and LERF.

The following analyses are needed to confirm that the plant fulfils the safety requirements:

DSA: deterministic plant response analyses to low water level
PSA: probabilistic plant response analyses to low water level

7.11 Earthquake

Detailed deterministic and probabilistic hazard, fragility and plant response analyses are presented for illustration in chapter 2 and 3 for earthquake.

Based on Table 7.2 the following safety requirements are considered to be the most important against earthquake:

- Requirement 4: Fundamental safety functions (DSA, HFE)
- Requirement 7: Application of defence in depth (DSA)
- Requirement 24: Common cause failures (PSA)
- Requirement 41: Interactions between the electrical power grid and the plant (DSA)
- Requirement 42: Safety analysis of the plant design (DSA, PSA, HFE, SEP)
- Requirement 54: Containment system for the reactor (DSA, SEP)
- Requirement 55: Control of radioactive releases from the containment (DSA, PSA)
- Requirement 56: Isolation of the containment (DSA, PSA)
- Requirement 62: Reliability and testability of instrumentation and control systems (PSA)
- Requirement 68: Design for withstanding the loss of off-site power (DSA, PSA)
- Requirement 69: Performance of supporting systems and auxiliary systems (DSA, PSA, SEP)
- Requirement 70: Heat transport systems (DSA)
- Requirement 73: Air conditioning systems and ventilation systems (DSA, PSA)

Type of analyses and engineering applications from Table 7.1 are presented in parentheses to show the adequate way for achievement the safety requirements.

7.11.1 Seismic hazard analyses

Deterministic and probabilistic seismic hazard analyses are performed for earthquake (see chapter 2 and 3 of the report).

The following analyses are needed to confirm that the plant fulfils the safety requirements:

DSA: deterministic seismic hazard analyses
PSA: probabilistic seismic hazard analyses

7.11.2 Seismic fragility analyses

Deterministic and probabilistic seismic fragility analyses are performed for earthquake (see chapter 2 and 3 of the report).

The following analyses are needed to confirm that the plant fulfils the safety requirements:

DSA: deterministic seismic fragility analyses
PSA: probabilistic seismic fragility analyses
7.11.3 Plant response analyses to earthquake

The plant response analyses involve seismic hazard and fragility analyses and plant model development using the deterministic SMA approach and seismic PSA (see chapter 2 and 3 of the report).

Within the deterministic response analyses the seismic capacity is calculated for the plant. SPSAs calculate the contribution of earthquake to CDF and LERF.

The following analyses are needed to confirm that the plant fulfils the safety requirements:

DSA: deterministic plant response analyses to earthquake
PSA: probabilistic plant response analyses to earthquake

7.12 Aircraft crash

There is no experience of damage induced by aircraft falling on nuclear islands, although some crashes have been recorded in their vicinity, sometimes with long skidding (300 m) of the engines far from the impact areas, with damage to residential and industrial facilities.

Based on Table 7.2 the following safety requirements are considered to be the most important against aircraft crash:

- Requirement 7: Application of defence in depth (DSA)
- Requirement 8: Interfaces of safety with security and safeguards (DSA)
- Requirement 21: Physical separation and independence of safety systems (DSA, HFE, SEP)
- Requirement 42: Safety analysis of the plant design (DSA, PSA, HFE, SEP)
- Requirement 63: Use of computer based equipment in systems important to safety (DSA, HFE, SEP)
- Requirement 65: Control room (HFE)
- Requirement 66: Supplementary control room (HFE)
- Requirement 67: Emergency response facilities on the site (HFE)
- Requirement 68: Design for withstanding the loss of off-site power (DSA, PSA)
- Requirement 69: Performance of supporting systems and auxiliary systems (DSA, PSA, SEP)
- Requirement 70: Heat transport systems (DSA)
- Requirement 73: Air conditioning systems and ventilation systems (DSA, PSA)

Type of analyses and engineering applications from Table 7.1 are presented in parentheses to show the adequate way for achievement the safety requirements.

7.12.1 Aircraft crash hazard analyses

Depending on the location of the airport or airways with respect to the nuclear power plant, the type and size of aircraft accidently impacting the plant is selected. It is assumed that a probabilistic analysis of the aircraft hazard for accidental crash in the vicinity has been conducted and a specific aircraft is chosen to perform the margin assessment. This margin assessment could also be part of the overall probabilistic analysis. For a postulated aircraft crash, it is expected that the competent authority of the country will specify the hazard. It could be in terms of a forcing function or the type of aircraft and its impact velocity.

The frequency of aircraft crash is calculated from the frequency of aircraft transport in the vicinity of the plant and generic values of aircraft crash of given type.

The following analyses are needed to confirm that the plant fulfils the safety requirements:

DSA: deterministic aircraft crash hazard analyses
PSA: probabilistic aircraft crash hazard analyses
7.12.2 Aircraft crash fragility analyses

The prevention of penetration of the impacted outer shell or wall of a structure against the load applied by an aircraft crash represents the main goal of the protection of the nuclear power plant. The maximum impact load per unit surface provides the indication for the possibility of local overstressing of the structure and initiation of the penetration processes. An assessment of the danger of penetration needs to be therefore performed not only for the maximum loads related to the whole aircraft but also for their parts impacting with the same velocity but acting on a much smaller surface. The effect of an aircraft crash on a building mainly depends on the type of aircraft, the design concept of the structure and the thickness of the outer shell of the structure as well as the location of the impact region on the building. In order to assess the effectiveness of the overall protection concept of a nuclear plant subjected to impacts, fires and other concomitant events, the following need to be checked:

- The global stability (overturning) of the safety related structure;
- Major structural damage, such as the collapse of large portions of the building;
- The penetration resistance of the impacted outer walls and shells;
- The integrity and functionality of the safety relevant SSCs;
- Fire resistance.

The stability checks are to be performed for the loads applied by the aircraft acting on the corresponding building at its upper regions, considering the local soil conditions. The zone of influence concept is identified for the purposes of preliminary screening. The concept is applied to an aircraft crash by imposing the damage and debris triangles on a scaled representation of a nuclear plant, aligned along each or all determined approach paths. An approximation of the areas of damage likely to occur to the relevant building could be obtained. The footprint of the fire and smoke damage can be obtained by extending the zone of influence until met by a fire barrier that has not been damaged by the initial impact or subsequent debris. Assuming a loss of all SSCs contained within the zone of influence, and using the defined success criteria (i.e. the redundancy and survivability requirements), an estimation of the effect of the aircraft crash on the plant could be obtained. Margin assessment would then determine whether successful shutdown of the nuclear power plant is feasible using the SSCs outside the zone of influence.

The following analyses are needed to confirm that the plant fulfils the safety requirements:

DSA: deterministic plant response analyses to aircraft crash
PSA: probabilistic plant response analyses to aircraft crash

7.12.3 Plant response analyses to aircraft crash

In summary, the major steps for margin assessment for an aircraft crash are the following [25]:

1. To review the aircraft to be considered by type, size, impact angle and amount of jet fuel or the loading parameters defined.
2. To choose the reference parameter for fragility or margin evaluation (e.g. the impact velocity).
3. To construct the zone of influence for a specific location of impact, which comprises an impact zone, a debris zone and a fire and smoke zone and to identify the SSCs that are in this zone. Depending on the structure impacted, there may or may not be any damage or breach (e.g. the containment may withstand the aircraft impact, including engines, without damage, whereas the auxiliary building may be breached). Therefore, some SSCs may be affected by the aircraft impact, while others may be affected by secondary missiles and/or heat generated by the jet fuel fire. The empirical formulas for local behaviour and the global response procedures are used to determine whether or not the structure is damaged for this aircraft crash.
4. To determine the fire and smoke zone for the amount of jet fuel available at impact: The zone is also dependent on the resistance of the structure impacted. Depending on the type of aircraft, the mass at impact (including fuel) and other parameters, there is a strong correlation between the amount of jet fuel flowing and ignited and the impact loadings. The joint probability distributions for impact and heat loading conditions are difficult to derive. Instead, the probabilities of failure for impact and heat are defined as independent variables, but in fact the jet fuel fire and the size of the impact are coupled. Hence, the governing failure mode is defined to be either impact or fire, whichever is more critical. A conservative approximation is to assume that all equipment, including piping and cabling, within the zone of influence is lost.
5. To calculate the median (best estimate) aircraft velocity for breach, or instability (i.e. overturning or sliding) of the building, and to estimate the uncertainty $\beta_c$ for this velocity.
6. To calculate the median and uncertainty $\beta_c$ for other SSCs due to secondary missiles and heat loading.
7. To perform a systems analysis to develop the accident sequences and, with the SSC fragilities appearing in these sequences, to calculate the plant level fragility. The aircraft velocity for which the probability of failure is 1% is also to be calculated.
8. To use, as an alternative, the systems analysis to derive success paths.
9. To assess the SSC capacities on these success paths (in terms of reference parameters) to safely withstand the impact of aircraft, secondary missiles and heat loading. The lowest SSC capacity on the success path determines the margin of the path. This procedure could be repeated for selected impact locations and the plant margin against aircraft crashes is the lowest of margins so calculated.

The following analyses are needed to confirm that the plant fulfils the safety requirements:

- DSA: deterministic plant response analyses to aircraft crash
- PSA: probabilistic plant response analyses to aircraft crash
- HFE: human factors engineering
- SEP: safety engineering processes

7.13 Malicious attack

Safety measures and nuclear security measures and arrangements for a nuclear power plant shall be designed and implemented in an integrated manner so that they do not compromise one another (IAEA Requirement 8).

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 (IAEA Requirement 63).

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.

Based on Table 2.2 the following safety requirements are considered to be the most important against malicious attack:

- Requirement 7: Application of defence in depth (DSA)
- Requirement 8: Interfaces of safety with security and safeguards (DSA)
- Requirement 21: Physical separation and independence of safety systems (DSA, HFE, SEP)
- Requirement 42: Safety analysis of the plant design (DSA, PSA, HFE, SEP)
- Requirement 63: Use of computer based equipment in systems important to safety (DSA, HFE, SEP)
- Requirement 65: Control room (HFE)
- Requirement 66: Supplementary control room (HFE)
- Requirement 67: Emergency response facilities on the site (HFE)
Type of analyses and engineering applications from Table 7.1 are presented in parentheses to show the best way for achievement of safety requirements.

The following analyses are needed to confirm that the plant fulfils the safety requirements:

DSA: deterministic plant response analyses  
PSA: probabilistic plant response analyses  
HFE: Human interaction within the nuclear security measures prevents the postulated malicious attacks.  
SEP: Safety engineering processes to show that adequate safety measures are implemented

8 Conclusion

This report summarized the works performed within Task 2.1 of the BESEP project. The external hazards of interest are identified from the preliminary case studies to support the benchmark exercise within BESEP. IAEA safety requirements have been identified and assigned for the single external hazards. Only the single hazards are evaluated. No combinations of external hazards are involved in the preliminary case studies. It can be a task in the future, mainly in WP3.

In Task 2.2 the safety requirements, identified in Task 2.1, will be 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 will be involved in Task 2.3. Task 2.4 focuses on identification of general risk-significance thresholds of external hazards.

Important conclusion of the Task 2.1 is that the description of case studies should be improved. The role of deterministic safety analyses (DSA), probabilistic safety analyses (PSA), human factors engineering (HFE) and safety engineering processes (SEP) should be implemented and detailed descriptions provided. To support this activity a template should be developed with examples for seismic event, non-seismic natural event and human induced-event.

9 Acknowledgment

The authors would like to express their sincere gratitude to partner organizations within BESEP for their contributions to the report.

REFERENCES

[7] Probabilistic safety assessment for full power operation of unit 1 of Mochovce NPP – non-seismic external events, main report, RELKO report, No. 6R0218, Bratislava, October 2018


[15] Level 1 probabilistic safety assessment for unit 3 of Mochovce NPP - PSA study of non-seismic external events – Fragility analyses of components and buildings for seismic event, RELKO report No. 5R0118, Bratislava, 2018


[21] Email from J. Holy, UJV: External events for WP2, dated 11.1.2021

[22] Email from E. Bradenmark, RISK PILOT: Task 2.1 BESEP, dated 13.1.2021

[23] JORF (Official Journal of the French Republic) No. 0033 of 8 February 2012, page 2231 Text No. 12 ORDER, "Order of 7 February 2012 setting the general rules relative to basic nuclear installations" or in French : Arrêté du 7 février 2012 fixant les règles générales relatives aux installations nucléaires de base


APPENDIX A: CASE STUDIES

CONTENTS

A. Introduction 61
A.1 Cybersecurity of an overall I&C architecture 61
A.2 The flood protection of the Auxiliary Emergency Feed Water (AEFW) building against extreme flood 62
A.3 The freezing of instrumentation at reactor building and turbine building during extreme cold weather 63
A.4 Collapse of venting stack due to high wind 63
A.5 Safety margin assessment of human-induced external event 64
A.6 Evaluation of protective measures in case of low water level in river or water body providing ultimate heat sink 66
A.7 Icing events of the overhead power lines 67
A.8 Formal verification of I&C systems' tolerance for consequential failures 68
A.9 Screening process for combinations of natural external hazards 69
A.10 Estimation of extreme values of external hazards for very low frequencies of occurrence 69
A.11 Safety margin assessment of the diesel generator building for tornado 70
A.12 Safety margin assessment of the reactor hall for extreme snow 71

A. INTRODUCTION

In this appendix the case studies are described which were prepared during the project proposal phase with focus on the needs of Task 2.1.

A.1 Cybersecurity of an overall I&C architecture

Description of the Case Study:

The instrumentation and control (I&C) systems of nuclear facilities shall have, and shall be operated with, appropriate defences against malicious cyber-attacks. Such defences include physical security measures, technical measures in the I&C design, procedural measures in the installation and operation of the I&C, and overall organisational measures. The French SMR project (to which EDF is a party) has designed an overall I&C architecture that include a number of cybersecurity measures, at the level of the overall I&C architecture, and also at the level of individual I&C systems or devices. The measures at the level of the architecture follow the requirements of IEC 62645, but also include a Cybersecurity Management System. The measures at the level of an individual I&C system or device depend on the level of defence in depth to which it belongs, and also on its safety class. The case study is concerned with applying a claim-argument-evidence approach to justify that the set of measures taken ensure that no malicious attacks (whether from outside of a plant or from an insider) can adversely affect safety. However, cybersecurity is also concerned with availability and production. In the case of the French SMR project, which aims at building a fleet of relatively low power units that are geographically distributed, the case study is also concerned with applying a claim-argument-evidence approach to justify that the set of measures taken ensure that no malicious attacks can significantly affect the production of a fleet.

Related Safety requirement set:

- The set of postulated malicious attacks adequately covers the possible attacks that could affect safety or production.
- No postulated malicious attack shall be able to adversely affect the safety of any individual unit.
- No postulated malicious attacks shall be able to affect the production of a fleet.

Plant SSC(s) involved:

- I&C system cabinets & rooms
- Digital I&C devices
- Digital support systems (HVAC, power supplies)
Corresponding External Hazard(s):

- Malicious attacks

Safety analyses involved:

- Multi-level vulnerability analysis: individual unit, plant, fleet
- Claim-argument justification
- Functional Failure modes, effects and criticality analysis (f-FMECA)

A.2 The flood protection of the Auxiliary Emergency Feed Water (AEFW) building against extreme flood

Description of the Case Study:

After Fukushima accident high sea level and external flooding have been widely recognised issue at many nuclear power plants (NPP). At Loviisa NPP some studies and plant modifications have been implemented to prepare for extreme sea level and flooding at the plant area. The strategy of the protection against flood is to secure the reactor core residual heat removal and prevent core damage and severe accident. This has been carried out by establishing flood protection for the most important buildings and rooms at the plant. Flood protection is implemented by removable equipment like door covers and walls that can be quickly installed at the places like doors and sewer openings. Because the extreme high sea level can be foreseen there is time to prepare and install flood protection equipment when needed. Some permanent flood protection covers have been installed, for example ventilation vents. Removable protection has been made for two most important targets:

- auxiliary emergency feed water building that is used for removing residual heat from reactor by secondary circuit and has an own diesel generator and
- reserve residual heat removal system (RRHRS) that removes the heat to ultimate heat sink (sea or cooling towers).

Flood protection has been established so that doors are still available for passage even though it means climbing over the flood protection walls.

PSA studies show that the protection implemented is greatly affected at CDF. Procedures are important for the situation management and give the sea level values and guidance how and when flood protection needs to be done. Strategy for flood protection is proven by APROS® analysis of complete station black out and loss of ultimate heat sink.

Related Safety requirement set:

- Prevent severe accident by ensuring residual heat removal.
- Probabilistic safety goals/criteria shall be met for level 1 and level 2 PSA with consideration to all relevant external hazards.

Plant SSC(s) involved:

- AEFW
- RRHRS

Corresponding External Hazard(s):

- Extreme sea level

Safety analyses involved:

- Extreme values on sea level
- Extreme values on rainfall and capacity of drainages
- Studies on leak tightness of buildings
A.3 The freezing of instrumentation at reactor building and turbine building during extreme cold weather

Description of the Case Study:

Usually, the volume of the buildings and structures give good prevention against rapid temperature changes. However, there are several places where extreme cold temperature may cause process equipment failure if temperature falls inside the plant. At Loviisa power plant there are some cases where some impulse piping has frozen. Other possible targets for freezing are diesel tanks that are located outside the buildings. There is also equipment that are placed next to doors and may get affected by cold air if doors are opened. Some rooms at the lowest parts of reactor building have equipment that could be affected if temperature falls enough. These rooms had previously air conditioning that had air intake directly outside of the building and risk of freezing temperatures inside these rooms at extremely low temperatures was real. These are problems that Loviisa power plant has faced during the years. Following correcting actions have been done: Most of the tanks that are located outside are warmed and stirred so that freezing is unlike. Also, most of the tanks have such volume that it itself prevents fast temperature changes. Plant has some movable heaters that can be used. Rooms that contain important instrumentation have temperature measurements and if room temperature falls too much an alarm is given. Some studies have also been carried out. Example the risk of cooling of certain instrumentation rooms at the lowest parts of the reactor building have been studied and found out that there are some water tanks that keep the temperature high enough for several hours which gives time to provide extra heating for the rooms if needed. Also building, structures and operating equipment produce heat that keeps rooms warm. Air conditioning has been modified so that the air is warmed before blowing it into the instrumentation rooms. Effects of freezing and cold temperatures have been prevented by installing heaters at some rooms. Cold weather itself doesn't directly cause significant risk for core damage according to PSA. Keeping plant at power operation is probably the most effective way to prevent equipment failures caused by low temperature.

Related Safety requirement set:

- Ensuring warming for the rooms that contain instrumentation of safety systems.
- Keeping plant on power when temperature lowers and prevent cold to get inside the buildings.

Plant SSC(s) involved:

- Instrumentation in turbine building
- Air conditioning of instrumentation room under reactor building

Corresponding External Hazard(s):

- Extreme cold weather

Safety analyses involved:

- Extreme values about cold temperatures
- COCOSYS analyse about cold air usage for instrumentation rooms cooling at low temperature.
- Probabilistic Safety Assessment;
- Studies about heat capacities of some tanks at reactor building

A.4 Collapse of venting stack due to high wind

Description of the Case Study:

High-wind is strongly moving air flow that arises as a result of pressure equalization between areas of different atmospheric pressure. It is a ground horizontal flow of air flowing from the pressure up to the pressure below. In its description, the wind direction, speed and cooling effect are significant. In general, only
the horizontal component of the wind load is taken into account because its vertical component is very small compared to the horizontal one. A similar situation is in the case of an earthquake. The wind speed varies greatly over time, so the average wind speed (for 10 minutes) and wind speed (maximum velocity in a gust) are often reported. The wind direction is indicated by the direction from which the wind blows - either by azimuth (0 - 360 °) or by meteorology using world directions. Direction and wind speed are accurately measured at meteorological stations by anemometer or anemograph, usually at a height of 10 m above the earth's surface. The more precise name of the wind measured in this way is the ground wind. The wind speed may change rapidly, and it will be seen as a wind impact of varying intensity (gusts). High-wind may affect critical SSCs of the plant. Wind forces exceeding the load bearing capacity of SSCs can cause the walls or frame to collapse or overturning the structure and component. A very strong wind can also be capable of lifting the materials and throwing them as objects to objects (buildings) and devices could be damaged if they are not adequately constructed. Most nuclear power plant structures have excellent wind resistance. However, major vulnerabilities have been identified for non-safety structures due to their potential for collapsing on safety related structures or equipment. An example is the venting stack. Collapse of the venting stack may damage the safety-related buildings (reactor building, DG station and auxiliary building) in case of VVER440/V213 type reactors. The case study describes the construction of the hazard curves for the high-wind and construction of the fragility curves for the different plant structures. Implementation into the PSA study is presented. Contribution to the total risk is quantified and uncertainty sources are identified.

**Related Safety requirement set:**

- Prevent spatial interactions of the structures during high-wind.
- Probabilistic safety goals for level 1 and level 2 PSA with consideration of all relevant internal events, internal and external hazards.

**Plant SSC(s) involved:**

- Venting stack
- Reactor building
- DG station
- Auxiliary building

**Corresponding External Hazard(s):**

- High wind

**Safety analyses involved:**

- High-wind hazard analyses
- Fragility analyses of the structures
- High-wind plant response PSA model

**A.5 Safety margin assessment of human-induced external event**

**Description of the Case Study:**

The case study aims to investigate a human induced external event, which would exceed the design basis for the nuclear power plant in question. The postulated event will be analysed from structural assessment to the component performance to the effect of the impact and fire to the plant safety. The assessment process includes the following phases: 1) Event identification, 2) Assessment of structures, 3) Plant performance assessment and acceptance criteria, 4) Operator response.

**Phase 1. Event identification:** Event consists of impact and consequent explosion and fire at nuclear power plant, e.g., an impact of heavy, fuel laden airplane. The aircraft will be specified to exceed the design basis for the nuclear power plant in question.

**Phase 2. Assessment of structures:** Load characterization for: a) Mechanical load, b) explosion, c) fire. In a) and b), the following analysis steps are included: i) Selection of representative impact locations, ii) Structural response analysis, iii) Assessment of performance: Penetration resistance, Induced vibrations, iv) Capacity
check for the technological systems installed in the structures to demonstrate their sufficient design functionality under the induced loads. In c), the analysis steps are illustrated in figure below.

**Phase 3. Plant performance assessment and acceptance criteria:** Based on Phase 2 assessment on the damages to the plant systems, plant performance with the given input will be analysed. This analysis will be performed with either plant system modelling or severe accident management tools, depending on the extent of the damage estimated. The results can also be used to indicate the probability of (and margin to) the core damage.

**Phase 4. Operator response:** Evaluation of operator responses to the accident progression and mitigation. Control room operators’ ability to detect, control, and extinguish fire, and to make sure that the performance of safe shutdown functions is not prevented, and the risk of radioactive release to the environment is minimized, will be analysed. Suitable risk analysis methods such as Functional Resonance Analysis Method (FRAM) and System-Theoretic Accident Model and Processes (STAMP) are applied.

**Related Safety requirement set:**
- Sufficiency of physical separation and structural integrity against external impacts
- Fire resistance of systems and components
- Sufficiency of failure tolerance and safety margins

**Plant SSC(s) involved:**
- Auxiliary buildings
- Power supply systems

**Corresponding External Hazard(s):**
- Impact of heavy, fuel laden airplane
Earthquake

Safety analyses involved:

- Structural response analysis
- Assessment of performance
- Fire analysis
- Functional resonance analysis and system-theoretic accident model and processes methods
- Human reliability analysis

A.6 Evaluation of protective measures in case of low water level in river or water body providing ultimate heat sink

Description of the Case Study:

Decrease of the water level in river or large water bodies that ensure ultimate heat sink by means of direct cooling in several nuclear power plants (hereinafter referred to as decrease of water level in the ultimate heat sink) is typically a slowly evolving phenomenon. Thus, protective measures can be taken if an appropriate alarm has been initiated in a timely manner, and the associated technical, organizational, administrative, etc. conditions can be ensured for successfully implementing the measures. Often, a high level strategy is available for coping with such situations; however, the details of the strategy and the exact planning of actions to be taken are not fully elaborated in advance. Consequently, various kinds of difficulties and challenges may well need to be faced with to actually implement the necessary measures when dangerously low water level actually occurs. As an example, it is noted that the water level in the river Danube providing direct cooling and ultimate heat sink for the Paks NPP was lower than ever before in 2018, and the plant experienced the challenges and problems that needed to be overcome to actually and successfully implement adequate protective measures. Appropriate defences against the effects of low water level in the ultimate heat sink should be ensured through defining preparatory measures in an action plan and/or in appropriate operating procedures to provide sufficient safety margin and, also, to reassuringly exclude potential cliff-edge effects due to such phenomena. The case study is concerned with the demonstration and evaluation of safety engineering practices aimed at the justification of sufficient protective measures in case of low water level in the ultimate heat sink. The approach to ensuring appropriate defences against low water level of the ultimate heat sink and to assessing the safety margin of the water intake system for such events in particular, the underlying engineering and analysis methods, the associated assumptions as well as the evaluation and interpretation of the results are to be provided within this case. The case study describes how quantitative safety margin assessment is incorporated into the PSA in case of low water level, and how a slowly evolving endangering phenomena and the associated arrangements in place for protective measures (including the lack of a sufficiently detailed action plan) can be considered in the PSA. As part of the case study, it is also to be discussed and evaluated how the safety engineering process should be improved, including implications on the protective measures and/or additional safety analyses, if the safety margin appears insufficient or the cliff-edge effects cannot be excluded with high confidence.

Related Safety Requirement Set:

- Adequate defences and sufficient safety margins shall be ensured against the effects of external events by appropriate design solutions and operating procedures;
- Cliff-edge effects shall be excluded by design with high level of confidence.

Plant SSC(s) involved:

- The water intake system, with focus on the essential service water system in particular as well as the portable equipment in low water level situations.

Corresponding External Hazard(s):

- Low water level of the ultimate heat sink.

Safety analyses involved:
A.7 Icing events of the overhead power lines

Description of the Case Study:

The 400 kV overhead power line is used to export electricity to the grid during plant operation. Given loss of 400 kV line due to external reason the turbogenerators reduce power to the level of self-consumption. Reactor trip occurs given loss of the 400 kV line due to internal reason. Then, the self-consumption of the plant is supplied from the reserve transformer which is fed from the 110 kV overhead power line from the electrical grid. Given simultaneous loss of both 400 kV and 110 kV lines the diesel generators (DG) are being started to supply the 6 kV busbars.

During reactor shutdown with available 400 kV line, the generator breakers are open and the power supply to the 6 kV busbars of the plant is provided from the grid using this line. After loss of 400 kV lines (due to planned or unplanned maintenance) the power supply for residual heat removal is ensured by the reserve transformer which is fed from the 110 kV overhead power line. After loss of 110 kV line the diesel generators are started and connected to the 6 kV busbars.

The ice load can damage the overhead power lines and cause partial loss of offsite power (loss of 400 kV or 110 kV lines) or total loss of offsite power (loss of both 400 kV and 110 kV lines) of the plant. There are different forms of ice loads of the overhead power lines.

Atmospheric icing is a general term for the processes where water in various forms freezes in the atmosphere and sticks to objects exposed to the air. In case of the overhead lines, there are two types of icing: precipitation icing and incloud icing. Ice accretion due to precipitation icing may occur in different forms, namely glaze due to freezing rain, wet snow accretion and dry snow accretion. The regional and local topography affects the ice accretion. Coastal mountains along the windward side of the continents act to force moist air upwards, leading to a cooling of the air with condensation of water vapour and droplet growth with the consequence of incloud icing. The most severe incloud icing occurs above the condensation level and the freezing level on openly exposed heights, where mountain valleys force the moist air through passes and thus both lift the air and strengthen the wind. On the leeward side of the mountains, however, the descent of air mass results in internal heating of the air and evaporation of droplets thus protecting overhead power lines routed there against high ice accretion.

The thickness of the ice is being measured (mm) and the weight (g) is calculated from it. The load of the ice on the conductor should be known in g/m for evaluation the impact of extreme loads.

The case study describes the construction of hazard curves for icing events of overhead power lines to support the external natural event PSA of VVER440/V213 type reactors. Ice loads are not measured in general by meteorological stations on the overhead power lines. Therefore, information on ice accretion needs to be recorded directly at correspondingly designed observation devices at the plant site. The measurement of ice accretion is performed on the observation device at the plant site which is a line with length of 1 m and diameter of 30 mm. The thickness of the ice is being measured (mm) and the weight (g) is calculated from it. An example is provided for illustration of weight calculation from the thickness of the ice. The hazard curves of icing loads for different confidence levels are constructed and presented in the case study using the Gumbel distribution (named also extreme value distribution). In addition, the fragility analyses of the overhead power lines are described and implementation of icing into the PSA model is presented. The contribution to the risk is quantified and the sources of uncertainties are identified.

Related Safety requirement set:

- Prevent partial or total loss of offsite power due to icing.
- Probabilistic safety goals for level 1 and level 2 PSA with consideration of all relevant internal events, internal and external hazards.

Plant SSC(s) involved:
400 kV line
110 kV line

**Corresponding External Hazard(s):**
- Icing

**Safety analyses involved:**
- Construction of the hazard curves for icing of the power lines
- Fragility analyses of the overhead power lines
- Icing plant response PSA model

### A.8 Formal verification of I&C systems’ tolerance for consequential failures

**Description of the Case Study:**

The instrumentation and control (I&C) systems of nuclear facilities shall tolerate single failure anywhere in the system, including consequential failure due to internal or external event, which may disable a crucial support system (power supply, HVAC, etc.). A formal verification method called model checking can be used to prove that the application logic (software or FPGA circuit) fulfils its functional requirements. A software tool (model checker) either proves that the system model meets formal properties, or outputs a counterexample demonstrating erroneous behaviour. Including the failure modes of the underlying hardware equipment in the analysis comes at a significant computational cost. However, it has been shown that by abstracting the failure model (purely non-deterministic failures), and limiting the analysis to single failure tolerance, it is possible to verify the N+1 or N+2 criterion. In other words, the model checker can prove that the I&C application logic will perform its function, despite a consequential failure. The case study is concerned with identifying a feasible approach for modelling consequential failures caused by internal or external events. A suitable abstraction is needed in modelling the hardware failure mechanisms, and it may be necessary to limit the analysis to failures occurring at specific locations in the overall I&C system architecture. Still, it is also necessary to verify that the I&C application logic deals with multiple failures in a resilient, pre-determined way.

**Related Safety requirement set:**
- Safety I&C application logic shall meet its functional requirements.
- The I&C system shall be able to perform its function even if any singled component fails, including consequential failure due to internal or external event (N+1, N+2 failure tolerance).
- The I&C logic shall handle the degraded state of redundant systems/equipment (multiple failures) in a pre-determined way.

**Plant SSC(s) involved:**
- I&C system cabinets & rooms
- Power supply equipment

**Corresponding External Hazard(s):**
- Extreme weather
- Earthquake

**Safety analyses involved:**
- Formal verification (model checking)
- Failure modes and effects analysis (FMEA)
A.9 Screening process for combinations of natural external hazards

Description of the Case Study:

External hazards analysis has become an important topic of NPP safety analysis at Czech NPPs after Fukushima accident. A comprehensive list of natural external hazards was developed and was a subject of several levels of screening reflecting specific features of locations of operated NPPs. The final product of this phase of analysis was a list of plant specific hazards sorted according to estimated safety impact. The most important hazards from the list have been subject of deterministic and probabilistic analysis and measures have been taken to improve plant safety related features regarding potential impact of external hazards. One of the general results of external hazards analysis was that not only the individual hazards, but combinations of them could have significant impact on plant safety. This conclusion led to new step in the analysis devoted to external hazards combinations. The basic idea was to repeat the whole process of screening and consequent analysis used for individual hazards for combinations of natural hazards. One impulse for such analysis was the regulatory body requirement made as a part of conditions defined for approval of long-term operation of NPP Dukovany so that the regulatory aspects had to be considered in the analysis.

It was found during the analysis that there is a lot of new specific features that must be solved (large scope / thousands of combinations of two or even more individual hazards, timing of hazards impacts to shift them from two or more independent to combination, independent versus dependent versus consequential hazards, impact of specific order of hazards in sequence defining combination, estimation of frequency of combination of hazards, other specific features connected with concrete levels of screening etc.). PSA formed one important step in the overall general scheme of the screening and analysis process proposed for treatment of combinations of natural external hazards, which was expected to take place in the case that previous levels of qualitative and quantitative screening would not lead to screening out the combination of hazards.

Related Safety requirement set:

- probabilistic safety goals/criteria shall be met for level 1 and level 2 PSA with consideration to all relevant external hazards
- sufficiency of physical separation and structural integrity against external impacts
- sufficiency of safety margins ensured by appropriate design solutions and operating procedures
- elimination of cliff-edge effects by high level of confidence
- elimination of possible impact of long-term operation features on NPP resistance to the impact of external hazards

Plant SSC(s) involved:

- in general, all SSC important for safety which could be subject of potential impact of natural external hazards

Corresponding External Hazard(s):

- all natural external hazards (in combinations)

Safety analyses involved:

- safety analyses on the impact of extreme wind on selected SSCs
- safety analyses on the impact of extreme snow on selected SSCs
- safety analyses on the impact of extreme rain on capacity of drainages
- safety analyses on the impact of extremely high/low temperature on selected SSCs
- probabilistic safety assessment (NPP Dukovany Living PSA project, NPP Temelin PSA project)

A.10 Estimation of extreme values of external hazards for very low frequencies of occurrence

Description of the Case Study:
External hazards analysis has become an important topic of NPP safety analysis at Czech NPPs after the Fukushima accident. A comprehensive list of natural external hazards was developed and was a subject of several levels of screening reflecting specific features of environment of the operated NPPs. The final product of this phase of analysis was a list of plant specific hazards sorted according to estimated safety impact. The most important hazards from the list have been subject of deterministic and probabilistic analysis and measures have been taken to improve plant safety related features regarding potential impact of external hazards.

An important part of the analysis was evaluation of the relationship between the parameters determining hazard intensity, and annual frequency of hazard occurrence. From theoretical point of view it was a problem of “long” extrapolation of the parameters based on plant/location specific data collected during several last decades (since the time, natural hazards parameters as temperature, windspeed, snow cover etc. started being measured and recorded) up to 10,000 years corresponding to the (initiating) event frequency of $10^{-4}$ postulated as the borderline for design basis. Due to relatively limited role, plant specific (as well as more generic) data may play in this case, a selection and the way of (correct) using of the mathematical method of data treatment had a big impact on the direct quantitative results of the analysis and, later, on the external hazards analysis and conclusions and measures carried on the base of them.

To limit the impact of lack of natural hazards related data usually presented in the format of extreme values per the given year, comparative analyses were made as a case study testing the impact of various methodological aspects. One part of the analysis was related to treatment of data (approach to the analysis when several data sets are available from plant vicinity, selection of the most suitable data set, removing of defective data points, applications for testing validity of data sets – normality etc.). Another part of analysis focused on a selection of most suitable probability distributions, testing of impact of using of various probability distributions on the results of analysis (extreme values of hazard parameters corresponding to $10^{-4}$ frequency). It was found out, for example, that there was no unique valid choice for the best fitting distribution for all major natural hazards (and even for different data sets related to the same hazard).

Later on, selected results of the case study in the format of relationships/curves frequencies versus extreme values were inverted and a set of specific frequencies corresponding to the key extreme values (usually with some specific impact on SSCs) were used for quantification of NPP Dukovany PSA model. This way, the impact of methodological solutions studied in the case study on the estimation of plant operation risk was determined.

**Related Safety requirement set:**
- probabilistic safety goals/criteria shall be met for level 1 and level 2 PSA with consideration to all relevant external hazards

**Plant SSC(s) involved:**
- in general, all SSC important for safety which could be subject of potential impact of natural external hazards

**Corresponding External Hazard(s):**
- selected most important natural external hazards for the NPPs in Czech Republic (extreme wind, extreme snow and rain, extremely high/low temperature)

**Safety analyses involved:**
- some conclusions made from the safety analyses on the impact of extreme wind, snow, rain, high/low temperature
- probabilistic safety assessment (NPP Dukovany Living PSA project, NPP Temelin PSA project)

A.11 Safety margin assessment of the diesel generator building for tornado

**Description of the Case Study:**
Nuclear facilities shall be designed to withstand loads induced by site and facility specific external and internal hazards. One source of external hazards is tornado. Tornado may be considered as a hazard that induces complex effects, i.e., direct wind pressure, atmospheric pressure drop and missile generation. Appropriate defences against these effects should be ensured through establishing and maintaining sufficient safety margins by design for design basis loads and beyond and, also, to reassuringly exclude potential cliff-edge effects due to such loads. The case study is concerned with the demonstration and evaluation of safety engineering practices aimed at the justification of the abovementioned requirements for the diesel generator building structure of a nuclear power plant considering tornado. The approach to ensuring appropriate defences against tornado and to assessing the safety margin of the diesel generator building for such loads in particular, the underlying engineering and analysis methods, the associated assumptions as well as the evaluation and interpretation of the results are to be provided within this case. Although qualitative as well as quantitative aspects of the relevant safety engineering practices are to be addressed in this case study, how quantitative safety margin assessment is incorporated into the PSA for tornado, and how PSA is applied to justify the fulfilment of probabilistic safety goal/criteria and to qualify the adequacy of protecting the diesel generator building against tornado at a higher, facility level will be in the focus of attention. As part of the case study, it is also to be discussed and evaluated how the safety engineering process should be improved, including implications on structural design and/or additional safety analyses, if the safety margin appears insufficient or the cliff-edge effects cannot be excluded with high confidence.

**Related Safety requirement set:**

- Adequate defences and sufficient safety margins shall be ensured for plant structures against the effects of external events by appropriate design solutions;
- Cliff-edge effects shall be excluded by design with high level of confidence;
- Probabilistic safety goals/criteria shall be met for level 1 and level 2 PSA with consideration to all relevant external hazards including tornado too.

**Plant SSC(s) involved:**

- The complete structure of the diesel generator building.

**Corresponding External Hazard(s):**

- Tornado.

**Safety analyses involved:**

- Structural strength analysis;
- Structural reliability analysis;
- Fragility analysis related to tornado;
- Probabilistic Safety Assessment.

A.12 Safety margin assessment of the reactor hall for extreme snow

**Description of the Case Study:**

Nuclear facilities shall be designed to withstand loads induced by site and facility specific external and internal hazards. One source of external hazards is extreme snow. Appropriate defences against the effects of extreme snow should be ensured through establishing and maintaining sufficient safety margins by design for design basis loads and beyond and, also, to reassuringly exclude potential cliff-edge effects due to such loads. The case study is concerned with the demonstration and evaluation of safety engineering practices aimed at the justification of the above mentioned requirements for the building structure of the reactor hall of a nuclear power plant considering extreme snow. The approach to ensuring appropriate defences against snow loads and to assessing the safety margin of the reactor hall for such loads in particular, the underlying engineering and analysis methods, the associated assumptions as well as the evaluation and interpretation of the results are to be provided within this case. Although qualitative as well as quantitative aspects of the relevant safety engineering practices are to be addressed in this case study, how quantitative safety margin assessment is incorporated into the PSA for extreme snow, and how PSA is applied to justify the fulfilment of
probabilistic safety goal/criteria and to qualify the adequacy of protecting the reactor hall against snow loads at a higher, facility level will be in the focus of attention. As part of the case study, it is also to be discussed and evaluated how the safety engineering process should be improved, including implications on structural design and/or additional safety analyses, if the safety margin appears insufficient or the cliff-edge effects cannot be excluded with high confidence.

*Related Safety requirement set:*

- Adequate defences and sufficient safety margins shall be ensured for plant structures against the effects of external events by appropriate design solutions;
- Cliff-edge effects shall be excluded by design with high level of confidence;
- Probabilistic safety goals/criteria shall be met for level 1 and level 2 PSA with consideration to all relevant external hazards including extreme snow too.

*Plant SSC(s) involved:*

- The complete structure of the reactor hall.

*Corresponding External Hazard(s):*

- Extreme snow.

*Safety analyses involved:*

- Structural strength analysis;
- Structural reliability analysis;
- Fragility analysis related to extreme snow;
- Probabilistic Safety Assessment;
APPENDIX B: IAEA SAFETY REQUIREMENTS, PROTECTION AGAINST EXTERNAL HAZARDS AND DESIGN FOR EXTERNAL HAZARDS

CONTENTS

B. Introduction 73
B.1 Overview of IAEA specific safety requirements 73
B.1.1 Application of fundamental safety objective, principles and concepts 74
B.1.1.1 Fundamental safety objective 74
B.1.1.2 Fundamental safety principles 74
B.1.1.3 Fundamental safety concepts 76
B.1.2 Management of safety in design 78
B.1.3 Principal technical requirements 78
B.1.4 General safety requirements for plant design 79
B.1.4.1 Design basis 79
B.1.4.2 Design for safe operation over the lifetime of the plant 81
B.1.4.3 Human factors 81
B.1.4.4 Other design consideration 82
B.1.4.5 Safety analyses 83
B.1.5 Design of specific plant systems 84
B.1.5.1 Reactor core and associated features 84
B.1.5.2 Reactor coolant system 85
B.1.5.3 Containment structure and containment system 85
B.1.5.4 Instrumentation and control system 86
B.1.5.5 Emergency power supply 88
B.1.5.6 Supporting systems and auxiliary systems 89
B.1.5.7 Power conversion systems 90
B.1.5.8 Treatment of radioactive waste 90
B.1.5.9 Fuel handling system 91
B.1.5.10 Radiation protection 92
B.2 Application of safety criteria to the design for protection against external hazards 93
B.3 Design basis for external hazards 95
B.3.1 Loading derivation 95
B.3.2 Load combinations and acceptance criteria 97
B.3.3 General guidance on the procedures for structural design 97
B.3.4 Interaction effects 99
B.3.5 Documentation and QA 99
B.3.6 Accident monitoring and post-accident procedures 99

B. Introduction

The IAEA safety requirements for nuclear power plants, protection against external hazards and design for external hazards are described in this Appendix on the basis of [2,10,13].

The term safety requirement is a requirement that is defined for the purpose of risk reduction. Like any other requirements, it may at first be specified at a high level, for example, simply as the need for the reduction of a given risk. The totality of the safety requirements for all risks forms the safety requirements specification. Any safety requirement is met by a combination of safety functions, and these are implemented in the safety systems.

The term safety goals are defined to cover all health and safety requirements which must be met: these may be deterministic rules or probabilistic targets. They should cover the safety of workers, public and the environment in line with the IAEA's Basic Safety Objective, encompassing safety in normal operation through to severe accidents [10].

B.1 Overview of IAEA specific safety requirements
The IAEA safety requirements are technology-neutral. It means that they are valid for all types of reactors.

Safety objective, safety principles and concepts form the basis for deriving the safety function requirements that must be met for the nuclear power plant, as well as the safety design criteria.

The overarching safety requirements for nuclear power plants are the following [2]:

- **Management of safety in design.** General requirements to be satisfied by the design organization in the management of safety in the design process.
- **Principal technical requirements.** Requirements for principal technical design criteria for safety, including requirements for the fundamental safety functions, the application of defence in depth and provision for construction; requirements for interfaces of safety with nuclear security and with the State system of accounting for, and control of, nuclear material; and requirements for ensuring that radiation risks arising from the plant are maintained as low as reasonably achievable.
- **General plant design.** Requirements for general plant design that supplement the requirements for principal technical design criteria to ensure that safety objectives are met and the safety principles are applied. The requirements for general plant design apply to all SSCs important to safety.
- **Design of specific plant systems.** Requirements for the design of specific plant systems such as the reactor core, reactor coolant systems, containment system, and instrumentation and control systems.

**B 1.1 Application of fundamental safety objective, principles and concepts**

**B.1.1.1 Fundamental safety objective**

The fundamental safety objective is to protect people and the environment from harmful effects of ionizing radiation.

**B.1.1.2 Fundamental safety principles**

The fundamental safety principles establish one fundamental safety objective (see above) and ten safety principles that provide the basis for requirements and measures for the protection of people and the environment against radiation risks and for the safety of the plant and activities that give rise to radiation risks.

The safety principles are the following [10]:

Principle 1: Responsibility for safety. The prime responsibility for safety must rest with the person or organization responsible for facilities and activities that give rise to radiation risks.

The licensee retains the prime responsibility for safety throughout the lifetime of plant and activities, and this responsibility cannot be delegated.

Principle 2: Role of government. An effective legal and governmental framework for safety, including an independent regulatory body, must be established and sustained.

Government authorities have to ensure that arrangements are made for preparing programmes of actions to reduce radiation risks, including actions in emergencies, for monitoring releases of radioactive substances to the environment and for disposing of radioactive waste. Government authorities have to provide for control over sources of radiation for which no other organization has responsibility, such as some natural sources, orphan sources and radioactive residues from some past facilities and activities.

Principle 3: Leadership and management for safety. Effective leadership and management for safety must be established and sustained in organizations concerned with, and facilities and activities that give rise to radiation risks.

Leadership in safety matters has to be demonstrated at the highest levels in an organization. Safety has to be achieved and maintained by means of an effective management system. This system has to integrate all
elements of management so that requirements for safety are established and applied coherently with other requirements, including those for human performance, quality and security, and so that safety is not compromised by other requirements or demands. The management system also has to ensure the promotion of a safety culture, the regular assessment of safety performance and the application of lessons learned from experience.

Principle 4: Justification of facilities and activities. Facilities and activities that give rise to radiation risks must yield an overall benefit.

For facilities and activities to be considered justified, the benefits that they yield must outweigh the radiation risks to which they give rise. For the purposes of assessing benefit and risk, all significant consequences of the operation of facilities and the conduct of activities have to be taken into account.

Principle 5: Optimization of protection. Protection must be optimized to provide the highest level of safety that can reasonably be achieved.

The safety measures that are applied to facilities and activities that give rise to radiation risks are considered optimized if they provide the highest level of safety that can reasonably be achieved throughout the lifetime of the facility or activity, without unduly limiting its utilization.

Principle 6: Limitation of risks to individuals. Measures for controlling radiation risks must ensure that no individual bears an unacceptable risk of harm.

Justification and optimization of protection do not in themselves guarantee that no individual bears an unacceptable risk of harm. Consequently, doses and radiation risks must be controlled within specified limits.


Radiation risks may transcend national borders and may persist for long periods of time. The possible consequences, now and in the future, of current actions have to be taken into account in judging the adequacy of measures to control radiation risks. In particular: Safety standards apply not only to local populations but also to populations remote from facilities and activities.

- Where effects could span generations, subsequent generations have to be adequately protected without any need for them to take significant protective actions.

Principle 8: Prevention of accidents. All practical efforts must be made to prevent and mitigate nuclear or radiation accidents.

The most harmful consequences arising from facilities and activities have come from the loss of control over a nuclear reactor core, nuclear chain reaction, radioactive source or other source of radiation. Consequently, to ensure that the likelihood of an accident having harmful consequences is extremely low, measures have to be taken: To prevent the occurrence of failures or abnormal conditions (including breaches of security) that could lead to such a loss of control;

- To prevent the escalation of any such failures or abnormal conditions that do occur;
- To prevent the loss of, or the loss of control over, a radioactive source or other source of radiation.

Principle 9: Emergency preparedness and response. Arrangements must be made for emergency preparedness and response for nuclear or radiation incidents.

The primary goals of preparedness and response for a nuclear or radiation emergency are:

To ensure that arrangements are in place for an effective response at the scene and, as appropriate, at the local, regional, national and international levels, to a nuclear or radiation emergency;

- To ensure that, for reasonably foreseeable incidents, radiation risks would be minor;
- For any incidents that do occur, to take practical measures to mitigate any consequences for human life and health and the environment.
Principle 10: Protective actions to reduce existing or unregulated radiation risks. Protective actions to reduce existing or unregulated radiation risks must be justified and optimized.

Radiation risks may arise in situations other than in facilities and activities that are in compliance with regulatory control. In such situations, if the radiation risks are relatively high, consideration has to be given to whether protective actions can reasonably be taken to reduce radiation exposures and to remediate adverse conditions.

- One type of situation concerns radiation of essentially natural origin. Such situations include exposure to radon gas in dwellings and workplaces, for example, for which remedial actions can be taken if necessary. However, in many situations there is little that can practicably be done to reduce exposure to natural sources of radiation.
- A second type of situation concerns exposure that arises from human activities conducted in the past that were never subject to regulatory control, or that were subject to an earlier, less rigorous regime of control. An example is situations in which radioactive residues remain from former mining operations.
- A third type of situation concerns protective actions, such as remediation measures, taken following an uncontrolled release of radionuclides to the environment.

These safety principles have been formulated, on the basis of which safety requirements are developed and safety measures are to be implemented in order to achieve the fundamental safety objective.

In order to satisfy the safety principles, it is required to ensure that for all operational states of a nuclear power plant and for any associated activities, doses from exposure to radiation within the installation or exposure due to any planned radioactive release from the installation are kept below the dose limits and kept as low as reasonably achievable.

To apply the safety principles, it is also required that nuclear power plants be designed and operated so as to keep all sources of radiation under strict technical and administrative control.

To demonstrate that the fundamental safety objective is achieved in the design of a nuclear power plant, a comprehensive safety assessment of the design is required to be carried out. Its objective is to identify all possible sources of radiation and to evaluate possible doses that could be received by workers at the installation and by members of the public, as well as possible effects on the environment, as a result of operation of the plant. The safety assessment is required in order to examine:

- normal operation of the plant;
- the performance of the plant in anticipated operational occurrences
- accident conditions.

On the basis of this analysis, the capability of the design to withstand postulated initiating events and accidents can be established, the effectiveness of the items important to safety can be demonstrated and the inputs (prerequisites) for emergency planning can be established.

Measures are required to be taken to ensure that the radiological consequences of an accident would be mitigated. Such measures include the provision of safety features and safety systems, the establishment of accident management procedures by the operating organization and, possibly, the establishment of off-site protective actions by the appropriate authorities, supported as necessary by the operating organization, to mitigate exposures if an accident occurs.

**B.1.1.3 Fundamental safety concepts**

Nuclear safety requirements were developed decades ago using deterministic approaches with a defence-in-depth (DID) philosophy as the foundation of the regulatory requirements.

The primary means of preventing accidents in a nuclear power plant and mitigating the consequences of accidents if they do occur is the application of the concept of defence in depth.
The fundamental safety requirements of most countries are based on deterministic considerations that employ DID safety philosophy. The defence-in-depth philosophy is a cornerstone of design and operational safety and the prevention of accidents. It provides for a series of successive barriers between the radioactive source and the harmful effects of radiation on people and the environment. Independence of the barriers provides protection against the risk of random failures of separate barriers although several barriers can be endangered in more serious accidents. As a whole, the set of barriers supported by independent reliable safety systems designed to protect their integrity provide a reliable containment of radioactive material within the plant. In principle, all countries utilize the DID safety philosophy in the design and operation of nuclear power plants.

There are five levels of defence:

1. Normal operation. The purpose of the first level of defence is to prevent deviations from normal operation and the failure of items important to safety (prevention of abnormal operation).
2. Anticipated operational occurrences. The purpose of the second level of defence is to detect and control deviations from normal operational states in order to prevent anticipated operational occurrences at the plant from escalating to accident conditions (control of abnormal operation).
3. Design basis accidents. For the third level of defence, it is assumed that, although very unlikely, the escalation of certain anticipated operational occurrences or postulated initiating events might not be controlled at a preceding level and that an accident could develop (control of design basis accidents).
4. Design extensions conditions without significant core degradation. The purpose of the fourth level of defence is to mitigate the consequences of accidents that result from failure of the third level of defence in depth. This is achieved by preventing the progression of such accidents and mitigating the consequences of a severe accident (control of beyond design basis accidents: prevention and mitigation).
5. Design extensions conditions with core melting. The purpose of the fifth level of defence is to mitigate the radiological consequences of radioactive releases that could potentially result from accidents (mitigation of off-site releases).

DID levels are presented in Figure. B.1.

The design, construction, operation and commissioning of a nuclear power plant might be shared between a number of organizations. However, the operating organization could set up a formal process to maintain the integrity of design of the plant throughout the lifetime of the plant (i.e., during the operating lifetime and into the decommissioning stage).
B.1.2 Management of safety in design

The management of safety in design is given by the safety requirements described below [2].

Requirement 1: Responsibilities in the management of safety in plant design. An applicant for a licence to construct and operate a nuclear power plant shall be responsible for ensuring that the design submitted to the regulatory body meets all applicable safety requirements.

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.

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.

B.1.3 Principal technical requirements

The principal technical requirements are described below [2].

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; (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 5: Radiation protection in design. The design of a nuclear power plant shall be such as to ensure that radiation doses to workers at the plant and to members of the public do not exceed the dose limits, that they are kept as low as reasonably achievable in operational states for the entire lifetime of the plant, and that they remain below acceptable limits and as low as reasonably achievable in, and following accident conditions.

Requirement 6: Design for a nuclear power plant. The design for a nuclear power plant shall ensure that the plant and items important to safety have the appropriate characteristics to ensure that safety functions can be performed with the necessary reliability, that the plant can be operated safely within the operational limits and conditions for the full duration of its design life and can be safely decommissioned, and that impacts on the environment are minimized.

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.

Requirement 8: Interfaces of safety with security and safeguards. Safety measures, nuclear security measures and arrangements for the State system of accounting for, and control of, nuclear material for a nuclear power plant shall be designed and implemented in an integrated manner so that they do not compromise one another.

Requirement 9: Proven engineering practices. Items important to safety for a nuclear power plant shall be designed in accordance with the relevant national and international codes and standards.

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.

Requirement 11: Provision for construction. Items important to safety for a nuclear power plant shall be designed so that they can be manufactured, constructed, assembled, installed and erected in accordance with established processes that ensure the achievement of the design specifications and the required level of safety.
Requirement 12: Features to facilitate radioactive waste management and decommissioning. Special consideration shall be given at the design stage of a nuclear power plant to the incorporation of features to facilitate radioactive waste management and the future decommissioning and dismantling of the plant.

B.1.4 General safety requirements for plant design

The general safety requirements are provided for [2]:

- design basis
- design for safe operation over the lifetime of the plant
- human factors
- other design consideration
- safety analyses

B.1.4.1 Design basis

Requirement 13: Categories of plant states. Plant states shall be identified and shall be grouped into a limited number of categories primarily on the basis of their frequency of occurrence at the nuclear power plant. Plant states shall typically cover the DID levels. Criteria shall be assigned to each plant state, such that frequently occurring plant states shall have no, or only minor, radiological consequences and plant states that could give rise to serious consequences shall have a very low frequency of occurrence.

Requirement 14: Design basis for items important to safety. The design basis for items important to safety shall specify the necessary capability, reliability and functionality for the relevant operational states, for accident conditions and for conditions arising from internal and external hazards, to meet the specific acceptance criteria over the lifetime of the nuclear power plant.

Requirement 15: Design limits. A set of design limits consistent with the key physical parameters for each item important to safety for the nuclear power plant shall be specified for all operational states and for accident conditions. The design limits shall be specified and shall be consistent with relevant national and international standards and codes, as well as with relevant regulatory requirements.

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. 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. 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. 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 18: Engineering design rules. The engineering design rules for items important to safety at a nuclear power plant shall be specified and shall comply with the relevant national or international codes and standards and with proven engineering practices, with due account taken of their relevance to nuclear power technology. Methods to ensure a robust design shall be applied, and proven engineering practices shall be adhered to in the design of a nuclear power plant to ensure that the fundamental safety functions are achieved for all operational states and for all accident conditions.

Requirement 19: Design basis accidents. A set of accidents that are to be considered in the design shall be derived from postulated initiating events for the purpose of establishing the boundary conditions for the nuclear power plant to withstand, without acceptable limits for radiation protection being exceeded. Design basis accidents shall be used to define the design bases, including performance criteria, for safety systems and for other items important to safety that are necessary to control design basis accident conditions, with the objective of returning the plant to a safe state and mitigating the consequences of any accidents. The design shall be such that for design basis accident conditions, key plant parameters do not exceed the specified design limits. A primary objective shall be to manage all design basis accidents so that they have no, or only minor, radiological consequences, on or off the site, and do not necessitate any off-site protective actions.

Requirement 20: Design extension conditions. A set of design extension conditions shall be derived on the basis of engineering judgement, deterministic assessments and probabilistic assessments for the purpose of further improving the safety of the nuclear power plant by enhancing the plant's capabilities to withstand, without unacceptable radiological consequences, accidents that are either more severe than design basis accidents or that involve additional failures. These design extension conditions shall be used to identify the additional accident scenarios to be addressed in the design and to plan practicable provisions for the prevention of such accidents or mitigation of their consequences. An analysis of design extension conditions for the plant shall be performed. The main technical objective of considering the design extension conditions is to provide assurance that the design of the plant is such as to prevent accident conditions that are not considered design basis accident conditions, or to mitigate their consequences, as far as is reasonably practicable. This might require additional safety features for design extension conditions, or extension of the capability of safety systems to prevent, or to mitigate the consequences of, a severe accident, or to maintain the integrity of the containment. These additional safety features for design extension conditions, or this extension of the capability of safety systems, shall be such as to ensure the capability for managing accident conditions in which there is a significant amount of radioactive material in the containment (including radioactive material resulting from severe degradation of the reactor core). The plant shall be designed so that it can be brought into a controlled state and the containment function can be maintained, with the result that the possibility of plant states arising that could lead to an early radioactive release or a large radioactive release is practically eliminated (physically impossible). The effectiveness of provisions to ensure the functionality of the containment could be analysed on the basis of the best estimate approach.

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 22: Safety classification. All items important to safety shall be identified and shall be classified on the basis of their function and their safety significance.

Requirement 23: Reliability of items important to safety. The reliability of items important to safety shall be commensurate with their safety significance.

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 25: Single failure criterion. The single failure criterion shall be applied to each safety group incorporated in the plant design.

Requirement 26: Fail-safe design. The concept of fail-safe design shall be incorporated, as appropriate, into the design of systems and components important to safety.

Requirement 27: Support service systems. Support service systems that ensure the operability of equipment forming part of a system important to safety shall be classified accordingly.

Requirement 28: Operational limits and conditions for safe operation. The design shall establish a set of operational limits and conditions for safe operation of the nuclear power plant.

B.1.4.2 Design for safe operation over the lifetime of the plant

Requirement 29: Calibration, testing, maintenance, repair, replacement, inspection and monitoring of items important to safety. Items important to safety for a nuclear power plant shall be designed to be calibrated, tested, maintained, repaired or replaced, inspected and monitored as required to ensure their capability of performing their functions and to maintain their integrity in all conditions specified in their design.

Requirement 30: Qualification of items important to safety. A qualification programme for items important to safety shall be implemented to verify that items important to safety at a nuclear power plant are capable of performing their intended functions when necessary, and in the prevailing environmental conditions, throughout their design life, with due account taken of plant conditions during maintenance and testing.

Requirement 31: Ageing management. The design life of items important to safety at a nuclear power plant shall be determined. Appropriate margins shall be provided in the design to take due account of relevant mechanisms of ageing, neutron embrittlement and wear out and of the potential for age related degradation, to ensure the capability of items important to safety to perform their necessary safety functions throughout their design life.

B.1.4.3 Human factors

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.
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.

B.1.4.4 Other design consideration

Requirement 33: Safety systems, and safety features for design extension conditions, of units of a multiple unit nuclear power plant. Each unit of a multiple unit nuclear power plant shall have its own safety systems and shall have its own safety features for design extension conditions.

Requirement 34: Systems containing fissile material or radioactive material. All systems in a nuclear power plant that could contain fissile material or radioactive material shall be so designed as: to prevent the occurrence of events that could lead to an uncontrolled radioactive release to the environment; to prevent accidental criticality and overheating; to ensure that radioactive releases are kept below authorized limits on discharges in normal operation and below acceptable limits in accident conditions, and are kept as low as reasonably achievable; and to facilitate mitigation of radiological consequences of accidents.

Requirement 35: Nuclear power plants used for cogeneration of heat and power, heat generation or desalination. Nuclear power plants coupled with heat utilization units (such as for district heating) and/or water desalination units shall be designed to prevent processes that transport radionuclides from the nuclear plant to the desalination unit or the district heating unit under conditions of operational states and in accident conditions.

Requirement 36: Escape routes from the plant. A nuclear power plant shall be provided with a sufficient number of escape routes, clearly and durably marked, with reliable emergency lighting, ventilation and other services essential to the safe use of these escape routes.

Requirement 37: Communication systems at the plant. Effective means of communication shall be provided throughout the nuclear power plant to facilitate safe operation in all modes of normal operation and to be available for use following all postulated initiating events and in accident conditions.

Requirement 38: Control of access to the plant. The nuclear power plant shall be isolated from its surroundings with a suitable layout of the various structural elements so that access to it can be controlled.

Requirement 39: Prevention of unauthorized access to, or interference with items important to safety. Unauthorized access to, or interference with, items important to safety, including computer hardware and software, shall be prevented.

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 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.

B.1.4.5 Safety analyses

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
effect 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.
B.1.1.5 Design of specific plant systems

The safety requirements are defined for design of specific plant systems [2]:

- reactor core and associated features
- reactor coolant system
- containment structure and containment system
- instrumentation and control system
- emergency power supply
- supporting systems and auxiliary systems
- power conversion systems
- treatment of radioactive waste
- fuel handling system
- radiation protection

B.1.5.1 Reactor core and associated features

Requirement 43: Performance of fuel elements and assemblies. Fuel elements and assemblies for the nuclear power plant shall be designed to maintain their structural integrity, and to withstand satisfactorily the anticipated radiation levels and other conditions in the reactor core, in combination with all the processes of deterioration that could occur in operational states.

Requirement 44: Structural capability of the reactor core. The fuel elements and fuel assemblies and their supporting structures for the nuclear power plant shall be designed so that, in operational states and in accident conditions other than severe accidents, a geometry that allows for adequate cooling is maintained and the insertion of control rods is not impeded.

Requirement 45: Control of the reactor core. Distributions of neutron flux that can arise in any state of the reactor core in the nuclear power plant, including states arising after shutdown and during or after refuelling, and states arising from anticipated operational occurrences and from accident conditions not involving degradation of the reactor core, shall be inherently stable. The demands made on the control system for maintaining the shapes, levels and stability of the neutron flux within specified design limits in all operational states shall be minimized.

Adequate means of detecting the neutron flux distributions in the reactor core and their changes shall be provided for the purpose of ensuring that there are no regions of the core in which the design limits could be exceeded.

In the design of reactivity control devices, due account shall be taken of wear out and of the effects of irradiation, such as burnup, changes in physical properties and production of gas.

The maximum degree of positive reactivity and its rate of increase by insertion in operational states and accident conditions not involving degradation of the reactor core shall be limited or compensated for, to prevent any resultant failure of the pressure boundary of the reactor coolant systems, to maintain the capability for cooling and to prevent any significant damage to the reactor core.

Requirement 46: Reactor shutdown. Means shall be provided to ensure that there is a capability to shut down the reactor of the nuclear power plant in operational states and in accident conditions, and that the shutdown condition can be maintained even for the most reactive conditions of the reactor core.

The effectiveness, speed of action and shutdown margin of the means of shutdown of the reactor shall be such that the specified design limits for fuel are not exceeded.

In judging the adequacy of the means of shutdown of the reactor, consideration shall be given to failures arising anywhere in the plant that could render part of the means of shutdown inoperative (such as failure of a control rod to insert) or that could result in a common cause failure.

The means for shutting down the reactor shall consist of at least two diverse and independent systems.
At least one of the two different shutdown systems shall be capable, on its own, of maintaining the reactor subcritical by an adequate margin and with high reliability, even for the most reactive conditions of the reactor core.

The means of shutdown shall be adequate to prevent any foreseeable increase in reactivity leading to unintentional criticality during the shutdown, or during refuelling operations or other routine or non-routine operations in the shutdown state.

Instrumentation shall be provided and tests shall be specified for ensuring that the means of shutdown are always in the state stipulated for a given plant state.

B.1.5.2 Reactor coolant system

Requirement 47: Design of reactor coolant systems. The components of the reactor coolant systems for the nuclear power plant shall be designed and constructed so that the risk of faults due to inadequate quality of materials, inadequate design standards, insufficient capability for inspection or inadequate quality of manufacture is minimized.

Requirement 48: Overpressure protection of the reactor coolant pressure boundary. Provision shall be made to ensure that the operation of pressure relief devices will protect the pressure boundary of the reactor coolant systems against overpressure and will not lead to the release of radioactive material from the nuclear power plant directly to the environment.

Requirement 49: Inventory of reactor coolant. Provision shall be made for controlling the inventory, temperature and pressure of the reactor coolant to ensure that specified design limits are not exceeded in any operational state of the nuclear power plant, with due account taken of volumetric changes and leakage.

Requirement 50: Cleanup of reactor coolant. Adequate facilities shall be provided at the nuclear power plant for the removal from the reactor coolant of radioactive substances, including activated corrosion products and fission products deriving from the fuel, and non-radioactive substances.

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;
- 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. Systems for transferring heat shall have adequate reliability for the plant states in which they have to fulfill the heat transfer function. This may require the use of a different ultimate heat sink or different access to the ultimate heat sink. 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.

B.1.5.3 Containment structure and containment system
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 56: Isolation of the containment. Each line that penetrates the containment at a nuclear power plant as part of the reactor coolant pressure boundary or that is connected directly to the containment atmosphere shall be automatically and reliably sealable in the event of an accident in which the leak tightness of the containment is essential to preventing radioactive releases to the environment that exceed acceptable limits.

Lines that penetrate the containment as part of the reactor coolant pressure boundary and lines that are connected directly to the containment atmosphere shall be fitted with at least two adequate containment isolation valves or check valves arranged in series and shall be provided with suitable leak detection systems. Containment isolation valves or check valves shall be located as close to the containment as is practicable, and each valve shall be capable of reliable and independent actuation and of being periodically tested.

Requirement 57: Access to the containment. Access by operating personnel to the containment at a nuclear power plant shall be through airlocks equipped with doors that are interlocked to ensure that at least one of the doors is closed during reactor power operation and in accident conditions.

Requirement 58: Control of containment conditions. Provision shall be made to control the pressure and temperature in the containment at a nuclear power plant and to control any build-up of fission products or other gaseous, liquid or solid substances that might be released inside the containment and that could affect the operation of systems important to safety.

The capability to remove heat from the containment shall be ensured, in order to reduce the pressure and temperature in the containment, and to maintain them at acceptably low levels after any accidental release of high energy fluids. The systems performing the function of removal of heat from the containment shall have sufficient reliability and redundancy to ensure that this function can be fulfilled.

Design provision shall be made to prevent the loss of the structural integrity of the containment in all plant states. The use of this provision shall not lead to an early radioactive release or a large radioactive release.

Design features to control fission products, hydrogen, oxygen and other substances that might be released into the containment shall be provided as necessary:

- To reduce the amounts of fission products that could be released to the environment in accident conditions;
- To control the concentrations of hydrogen, oxygen and other substances in the containment atmosphere in accident conditions so as to prevent deflagration or detonation loads that could challenge the integrity of the containment

B.1.5.4 Instrumentation and control system

Requirement 59: Provision of instrumentation. Instrumentation shall be provided for: determining the values of all the main variables that can affect the fission process, the integrity of the reactor core, the reactor coolant systems and the containment at the nuclear power plant; for obtaining essential information on the plant that is necessary for its safe and reliable operation; for determining the status of the plant in accident conditions; and for making decisions for the purposes of accident management.
Instrumentation and recording equipment shall be provided to ensure that essential information is available for monitoring the status of essential equipment and the course of accidents, for predicting the locations of releases and the amounts of radioactive material that could be released from the locations that are so intended in the design, and for post-accident analysis.

Requirement 60: Control systems. Appropriate and reliable control systems shall be provided at the nuclear power plant to maintain and limit the relevant process variables within the specified operational ranges.

Requirement 61: Protection system. A protection system shall be provided at the nuclear power plant that has the capability to detect unsafe plant conditions and to initiate safety actions automatically to actuate the safety systems necessary for achieving and maintaining safe plant conditions.

The protection system shall be designed:

- To be capable of overriding unsafe actions of the control system;
- With fail-safe characteristics to achieve safe plant conditions in the event of failure of the protection system.

The design:

- Shall prevent operator actions that could compromise the effectiveness of the protection system in operational states and in accident conditions, but shall not counteract correct operator actions in accident conditions;
- Shall automate various safety actions to actuate safety systems so that operator action is not necessary within a justified period of time from the onset of anticipated operational occurrences or accident conditions;
- Shall make relevant information available to the operator for monitoring the effects of automatic actions.

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. 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.

Requirement 64: Separation of protection systems and control systems. Interference between protection systems and control systems at the nuclear power plant shall be prevented by means of separation, by avoiding interconnections or by suitable functional independence.
If signals are used in common by both a protection system and any control system, separation (such as by adequate decoupling) shall be ensured and the signal system shall be classified as part of the protection system.

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.

Requirement 67: Emergency response facilities on the site. The nuclear power plant shall include the necessary emergency response facilities on the site. Their design shall be such that personnel will be able to perform expected tasks for managing an emergency under conditions generated by accidents and hazards.

Information about important plant parameters and radiological conditions at the nuclear power plant and in its immediate surroundings shall be provided to the relevant emergency response facilities. Each facility shall be provided with means of communication with, as appropriate, the control room, the supplementary control room and other important locations at the plant, and with on-site and off-site emergency response organizations. For nuclear power plants, emergency response facilities (which are separate from the control room and the supplementary control room) include the technical support centre, the operational support centre and the emergency centre.

B.1.5.5 Emergency power supply

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

B.1.5.6 Supporting systems and auxiliary 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 71: Process sampling systems and post-accident sampling systems. Process sampling systems and post-accident sampling systems shall be provided for determining, in a timely manner, the concentration of specified radionuclides in fluid process systems, and in gas and liquid samples taken from systems or from the environment, in all operational states and in accident conditions at the nuclear power plant.

Appropriate means shall be provided at the nuclear power plant for the monitoring of activity in fluid systems that have the potential for significant contamination, and for the collection of process samples.

Requirement 72: Compressed air systems. The design basis for any compressed air system that serves an item important to safety at the nuclear power plant shall specify the quality, flow rate and cleanliness of the air to be provided.

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.

Requirement 74: Fire protection systems. Fire protection systems, including fire detection systems and fire extinguishing systems, fire containment barriers and smoke control systems, shall be provided throughout the nuclear power plant, with due account taken of the results of the fire hazard analysis.

The fire protection systems installed at the nuclear power plant shall be capable of dealing safely with fire events of the various types that are postulated. Fire extinguishing systems shall be capable of automatic actuation where appropriate. Fire extinguishing systems shall be designed and located to ensure that their
rupture or spurious or inadvertent operation would not significantly impair the capability of items important to safety

Requirement 75: Lighting systems. Adequate lighting shall be provided in all operational areas of the nuclear power plant in operational states and in accident conditions.

Requirement 76: Overhead lifting equipment. Overhead lifting equipment shall be provided for lifting and lowering items important to safety at the nuclear power plant, and for lifting and lowering other items in the proximity of items important to safety.

The overhead lifting equipment shall be designed so that:

- Measures are taken to prevent the lifting of excessive loads;
- Conservative design measures are applied to prevent any unintentional dropping of loads that could affect items important to safety;
- The plant layout permits safe movement of the overhead lifting equipment and of items being transported;
- Such equipment can be used only in specified plant states (by means of safety interlocks on the crane);
- Such equipment for use in areas where items important to safety are located is seismically qualified.

B.1.5.7 Power conversion systems

Requirement 77: Steam supply system, feedwater system and turbine generators. The design of the steam supply system, feedwater system and turbine generators for the nuclear power plant shall be such as to ensure that the appropriate design limits of the reactor coolant pressure boundary are not exceeded in operational states or in accident conditions.

The design of the steam supply system shall provide for appropriately rated and qualified steam isolation valves capable of closing under the specified conditions in operational states and in accident conditions.

The steam supply system and the feedwater systems shall be of sufficient capacity and shall be designed to prevent anticipated operational occurrences from escalating to accident conditions.

The turbine generators shall be provided with appropriate protection such as overspeed protection and vibration protection, and measures shall be taken to minimize the possible effects of turbine generated missiles on items important to safety.

B.1.5.8 Treatment of radioactive waste

Requirement 78: Systems for treatment and control of waste. Systems shall be provided for treating solid radioactive waste and liquid radioactive waste at the nuclear power plant to keep the amounts and concentrations of radioactive releases below the authorized limits on discharges and as low as reasonably achievable.

Systems and facilities shall be provided for the management and storage of radioactive waste on the nuclear power plant site for a period of time consistent with the availability of the relevant disposal option.

Requirement 79: Systems for treatment and control of effluents. Systems shall be provided at the nuclear power plant for treating liquid and gaseous radioactive effluents to keep their amounts below the authorized limits on discharges and as low as reasonably achievable.

Liquid and gaseous radioactive effluents shall be treated at the plant so that exposure of members of the public due to discharges to the environment is as low as reasonably achievable.

The design of the plant shall incorporate suitable means to keep liquid radioactive releases to the environment as low as reasonably achievable and to ensure that radioactive releases remain below the authorized limits on discharges.
B.1.5.9 Fuel handling system

Requirement 80: Fuel handling and storage systems. Fuel handling and storage systems shall be provided at the nuclear power plant to ensure that the integrity and properties of the fuel are maintained at all times during fuel handling and storage.

The design of the plant shall incorporate appropriate features to facilitate the lifting, movement and handling of fresh fuel and spent fuel.

The design of the plant shall be such as to prevent any significant damage to items important to safety during the transfer of fuel or casks, or in the event of fuel or casks being dropped.

The fuel handling and storage systems for irradiated and non-irradiated fuel shall be designed:

- To prevent criticality by a specified margin, by physical means or by means of physical processes, and preferably by use of geometrically safe configurations, even under conditions of optimum moderation;
- To permit inspection of the fuel;
- To permit maintenance, periodic inspection and testing of components important to safety;
- To prevent damage to the fuel;
- To prevent the dropping of fuel in transit;
- To provide for the identification of individual fuel assemblies;
- To provide proper means for meeting the relevant requirements for radiation protection;
- To ensure that adequate operating procedures and a system of accounting for, and control of, nuclear fuel can be implemented to prevent any loss of, or loss of control over, nuclear fuel.

In addition, the fuel handling and storage systems for irradiated fuel shall be designed:

- To permit adequate removal of heat from the fuel in operational states and in accident conditions;
- To prevent the dropping of spent fuel in transit;
- To avoid causing unacceptable handling stresses on fuel elements or fuel assemblies;
- To prevent the potentially damaging dropping of heavy objects such as spent fuel casks, cranes or other objects onto the fuel;
- To permit safe keeping of suspect or damaged fuel elements or fuel assemblies;
- To control levels of soluble absorber if this is used for criticality safety;
- To facilitate maintenance and future decommissioning of fuel handling and storage facilities;
- To facilitate decontamination of fuel handling and storage areas and equipment when necessary;
- To accommodate, with adequate margins, all the fuel removed from the reactor in accordance with the strategy for core management that is foreseen and the amount of fuel in the full reactor core;
- To facilitate the removal of fuel from storage and its preparation for off-site transport.

For reactors using a water pool system for fuel storage, the design shall be such as to prevent the uncovering of fuel assemblies in all plant states that are of relevance for the spent fuel pool so that the possibility of conditions arising that could lead to an early radioactive release or a large radioactive release is `practically eliminated` and so as to avoid high radiation fields on the site. The design of the plant:

- Shall provide the necessary fuel cooling capabilities;
- Shall provide features to prevent the uncovering of fuel assemblies in the event of a leak or a pipe break;
- Shall provide a capability to restore the water inventory.
- The design shall also include features to enable the safe use of non-permanent equipment to ensure sufficient water inventory for the long term cooling of spent fuel and for providing shielding against radiation.

The design shall include the following:

- Means for monitoring and controlling the water temperature for operational states and for accident conditions that are of relevance for the spent fuel pool;
- Means for monitoring and controlling the water level for operational states and for accident conditions that are of relevance for the spent fuel pool;
- Means for monitoring and controlling the activity in water and in air for operational states and means for monitoring the activity in water and in air for accident conditions that are of relevance for the spent fuel pool;
- Means for monitoring and controlling the water chemistry for operational states

**B.1.5.10 Radiation protection**

Requirement 81: Design for radiation protection. Provision shall be made for ensuring that doses to operating personnel at the nuclear power plant will be maintained below the dose limits and will be kept as low as reasonably achievable, and that the relevant dose constraints will be taken into consideration.

Radiation sources throughout the plant shall be comprehensively identified, and exposures and radiation risks associated with them shall be kept as low as reasonably achievable, the integrity of the fuel cladding shall be maintained, and the generation and transport of corrosion products and activation products shall be controlled.

Materials used in the manufacture of structures, systems and components shall be selected to minimize activation of the material as far as is reasonably practicable.

For the purposes of radiation protection, provision shall be made for preventing the release or the dispersion of radioactive substances, radioactive waste and contamination at the plant.

The plant layout shall be such as to ensure that access of operating personnel to areas with radiation hazards and areas of possible contamination is adequately controlled, and that exposures and contamination are prevented or reduced by this means and by means of ventilation systems.

The plant shall be divided into zones that are related to their expected occupancy, and to radiation levels and contamination levels in operational states (including refuelling, maintenance and inspection) and to potential radiation levels and contamination levels in accident conditions. Shielding shall be provided so that radiation exposure is prevented or reduced.

The plant layout shall be such that the doses received by operating personnel during normal operation, refuelling, maintenance and inspection can be kept as low as reasonably achievable, and due account shall be taken of the necessity for any special equipment to be provided to meet these requirements.

Plant equipment subject to frequent maintenance or manual operation shall be located in areas of low dose rate to reduce the exposure of workers.

Facilities shall be provided for the decontamination of operating personnel and plant equipment.

Requirement 82: Means of radiation monitoring. Equipment shall be provided at the nuclear power plant to ensure that there is adequate radiation monitoring in operational states and design basis accident conditions and, as far as is practicable, in design extension conditions.

Stationary dose rate meters shall be provided for monitoring local radiation dose rates at plant locations that are routinely accessible by operating personnel and where the changes in radiation levels in operational states could be such that access is allowed only for certain specified periods of time.

Stationary dose rate meters shall be installed to indicate the general radiation levels at suitable plant locations in accident conditions. The stationary dose rate meters shall provide sufficient information in the control room or in the appropriate control position that operating personnel can initiate corrective actions if necessary.

Stationary monitors shall be provided for measuring the activity of radioactive substances in the atmosphere in those areas routinely occupied by operating personnel and where the levels of activity of airborne radioactive substances might be such as to necessitate protective measures. These systems shall provide an indication in the control room or in other appropriate locations when a high activity concentration of radionuclides is detected. Monitors shall also be provided in areas subject to possible contamination as a result of equipment failure or other unusual circumstances.
Stationary equipment and laboratory facilities shall be provided for determining, in a timely manner, the concentrations of selected radionuclides in fluid process systems, and in gas and liquid samples taken from plant systems or from the environment, in operational states and in accident conditions.

Stationary equipment shall be provided for monitoring radioactive effluents and effluents with possible contamination prior to or during discharges from the plant to the environment.

Instruments shall be provided for measuring surface contamination. Stationary monitors (e.g., portal radiation monitors, and hand and foot monitors) shall be provided at the main exit points from controlled areas and supervised areas to facilitate the monitoring of operating personnel and equipment.

Facilities shall be provided for monitoring for exposure and contamination of operating personnel. Processes shall be put in place for assessing and for recording the cumulative doses to workers over time.

Arrangements shall be made to assess exposures and other radiological impacts, if any, in the vicinity of the plant by environmental monitoring of dose rates or activity concentrations, with particular reference to:

- Exposure pathways to people, including the food chain;
- Radiological impacts, if any, on the local environment;
- The possible build-up, and accumulation in the environment, of radioactive substances;
- The possibility of there being any unauthorized routes for radioactive releases

**B.2 Application of safety criteria to the design for protection against external hazards**

The applicable design requirements have to ensure that the overall safety concept of defence in depth is maintained, the design shall be such as to prevent as far as practicable [13]:

- challenges to the integrity of physical barriers;
- failure of a barrier when challenged;
- failure of a barrier as a consequence of failure of another barrier.

There are two basic forms of plant protection against external hazards:

- either the causal influences of an external event are reduced by means of a passive barrier (e.g., site protection dam for flood, external shield for aircraft crash, barriers for explosions and building base isolation for earthquake) or
- the ability of the safety systems to resist the effects of external hazards is assessed by means of adequate item qualification (including redundancy, diversity or segregation).

The solution should represent the best balance among safety aspects, operational aspects and other important factors. For example, an inherent capability to withstand localized events (e.g., aircraft crash) can be provided by the physical separation of redundant systems, such that the simultaneous failure of the redundant systems due to the effects of building vibration, debris or fire from aircraft fuel is precluded. Otherwise, it is necessary to provide additional protection in the form of barriers or to increase the spatial separation by modification of the plant layout.

In particular, special provisions against common cause failure should be made for large and extensive systems, namely the systems used to transport heat to the UHS, pump houses, cooling towers, etc. A combination of the following protection strategies should be implemented:

- An adequate redundancy of safety related items. The level of redundancy should be an outcome of the application of the single failure approach to the design. Exceptions to the single failure approach may be accepted on a case by case basis where the external hazard has a very low probability and the systems are passive
- Extensive spatial separation between redundant components. This measure should prevent both common cause failures from localized external events (e.g., missile impact) and interactions in the event of failure of one system that could be a source of internal accidents. A detailed analysis of the
areas of influence or expected damage from the external hazard should be carried out for the purpose of application of the physical separation.

- Diversity in the redundant components. In the case of external event scenarios with a potential for common cause failures, the benefits of diversity should be evaluated with care. Diversity should be combined with separation when possible.

To provide additional defence in depth to the basic forms of protection defined above, for some external events proactive, active or administrative measures based on forewarning can also provide safety benefits. Examples of such measures include the reduction of fire loading materials adjacent to or on the nuclear site, the installation of additional barriers (damboards) or the closure of watertight gates in anticipation of flooding, and the inspection of drainage channels. While these measures are not normally as reliable as passive engineered systems, they nevertheless can provide additional safety benefits. The reliability ascribed to such measures should be commensurate with the reliability of the monitoring and forecasting equipment and operator reliabilities.

The effectiveness of administrative measures is strongly dependent on their enforcement level, particularly when different administrations are involved. Their reliability should therefore be evaluated with care.

The following aspects should also be considered in a design for safety:

- Following the occurrence of an external hazard the design should ensure accessibility to the main control room, to supplementary control points and to the points, rooms and facilities necessary for meeting the requirements
- The design should ensure that during the occurrence of an external hazard the plant status does not deteriorate to the extent that it cannot be controlled by the safety measures;
- The systems not protected against external hazards should be assumed to be operable or non-operable, depending on which status provides the more conservative scenario in the design of protection measures.

In the plant design for protection against external hazards, adequate robustness should be used to provide the plant with some additional capacity for beyond design basis values for conditions in the selected external event scenarios. In general, this capacity should be provided by a combination of the following: high quality design, low sensitivity to variation in design parameters, and high and demonstrable conservatism in material selection, construction standards and QA. An evaluation of the design conservatism should be carried out either with probabilistic tools or by simplified deterministic bounding analysis.

Moreover, a special evaluation should be carried out so as to avoid potential small deviations in plant parameters from giving rise to severely abnormal plant behaviour (cliff edge effects) in relation to the specific nature of the external hazard scenario (e.g., in the case of a site protection dam, if as soon as the dam is overtopped with a small additional steady state water level, the site could be suddenly flooded to the maximum level of the flood). In this case, additional engineering provisions should be implemented on safety systems at least for a safe shutdown mode, such as warning, monitoring and operating procedures.

Particular operating limits and conditions should be defined for any external hazard that proves to be important for plant design, in terms of relevance of the hazard, contribution to sizing of safety related items and contribution to the results of probabilistic safety assessment (PSA). It should be associated with dedicated surveillance procedures (pre- and post-hazard), a plant safe state (possibly a reactor shutdown) that is to be reached after such ‘abnormal’ events and a post-event revalidation procedure for any item important to safety that may have been challenged.

A set of operational limits should be defined for items classified for external hazards:

- Safety limits (safe operating limits): these are specified in the safety classification and represent the design basis conditions for the items. Their exceedance represents a challenge for plant safety and therefore a plant shutdown is required with precise post-event revalidation;
- Limits and conditions for normal operation: these represent the limits for safe operation with due consideration of the uncertainties in the design process described above. They do not affect the design being intrinsically related to the uncertainty of the hazard for a very low probability of exceedance. Their exceedance is preliminary to the activation of the safety systems in the safety group able to bring the plant into a safer state, such as power reduction or reactor shutdown.
• Limits and conditions for normal operation should be identified in the hazard evaluation phase. Adequate procedures should be implemented for monitoring and for the prompt evaluation of their exceedance, to be specified in terms of all the parameters affecting the hazard definition. Actions arising from the exceedance of limits and conditions could include enhanced monitoring, administrative measures and review of forecasts.

The plant operation can be extended up to safety limits, on the assumption of a high degree of conservatism in the design of the barrier, provided that no cliff edge effects are foreseen for beyond design basis values. However, due account should be taken of the uncertainties, of the reliabilities of monitoring and forecasting systems and of the margin between the time needed for shutdown and the time before the external event parameters exceed the barrier’s capacity.

In any case, in relation to the development of an external event, plant shutdown should start if any of the following conditions is met:

- If the operating personnel cannot ascertain that the power plant is being operated within normal limits and conditions;
- If there is any evidence of damage to classified items;
- If there is reasonable confidence that the normal limits and conditions will be exceeded in a shorter time than is needed for a shutdown, according to reliable forecasting procedures for the development of the event (e.g., for flood or cyclones).

For most external events with sudden or unexpected effects, the parameters associated with the design basis cannot be monitored: examples would include aircraft impact parameters, blast pressures or impulse. In such cases a precautionary principle should apply and shutdown should be initiated after the event upon the basis of operator judgement.

To prevent unnecessary trips or demands on safety systems, for those external hazards whose parameters are continuous variables, such as water level or wind speed, consideration should be given to making routine measurements. The equipment and systems used to measure and report these parameters should have a reliability and accuracy commensurate with the safety claims made upon them.

### B.3 Design basis for external hazards

The first step in the design of a nuclear power plant against external events is to identify those events that are considered credible for a particular site. Reference [1] provides a methodology for selecting credible external hazards for the site. A general approach in the design is to establish the design input parameters by a combination of deterministic and probabilistic methods and to proceed with the design in a deterministic manner.

When the hazard is defined in a probabilistic context, because of the deterministic approach applied in the design, the site hazard should be analysed and a single value on the hazard curve should be selected to be used in the design basis. In this case, the selection of the design basis includes an implicit probabilistic assumption concerning the risk of a radiological accident that a nuclear installation can present. Therefore, the final target of such an action is to keep the risk acceptably small, which implies an evaluation of the probability that an event will affect safety related items and then the probability of unacceptable consequences of their failure.

However, a complete probabilistic analysis is usually carried out only in the framework of a PSA, i.e., in a confirmatory phase of the design. In the early design phase, therefore, assumptions for such conditional probabilities should be made, driven mainly by deterministic calculations (e.g., stress analysis and impact damage evaluation) and expert judgement, so as to select a design basis value on the hazard curve in a reasonable way. Because of its nature, this process is strictly plant dependent and should be assessed in the design assessment phase. This value should also be compatible with the criteria applied in the probabilistic screening at the site evaluation phase.

The following issues should be considered in the definition of the probability levels for the design basis external hazards [13]:
- Installed power or hazard characteristic of the radiological source (reactor building and the spent fuel pool);
- Concentration of hazard effects: probability of common cause failures as a consequence (e.g., large fire, flood or extreme ambient temperature would be more prone to develop common cause failures than an aircraft crash);
- The need for active versus passive safety systems to prevent or mitigate unacceptable effects;
- The possible installation of warning systems able to detect in time the potential unfavourable development of an event (e.g., meteorological events versus aircraft crashes);
- The potential for quick dispersion following an event (e.g., explosions, flood and wind might have higher dispersion potential than extreme ambient temperature);
- The kind of potential contamination: long term effects, difficulties in decontamination, dispersed versus concentrated contamination and direct effects on the population;
- Easy implementation of emergency planning in relation to the event: access to the site, availability of evacuation routes and time delay between accident and releases;
- Characteristics of the engineering features that might exhibit some form of cliff edge effect in the event of an accident (e.g., overtopping of a dyke in the event of a flood), without the possibility of preventing a degeneration of the situation with radiological consequences.

External event PSA, monitoring, inspection, surveillance and periodic safety reviews are the tools that should be used to confirm the selected target probability levels.

Once an external hazard is identified as a design basis event, the design to protect against it is generally based on a deterministic analysis. Different ways of ensuring the safety objectives are:

- To strengthen the items so that they can withstand the impact, if their inherent capabilities would otherwise be insufficient;
- To protect them either by passive means (such as barriers) or by active means (such as qualified actuators that operate closure valves);
- To provide redundant items in a different location with sufficient separation between them;
- To limit the consequences of damage.

If the affected area is limited but is not confined to a specific location, the designer should analyse which functions could be impaired, on the assumption that the impact area may be anywhere on the site. As a case in point, it is not possible to predict the location of the impact area for an aircraft crash or a missile, but it may be possible to identify areas where aircraft crashes are not probable. For example, when a building is near other buildings these may serve to shield against the effects of an aircraft crash.

If the affected area is plant-wide, as would be expected in the case of high winds or toxic clouds, items important to safety located anywhere in the plant could be affected coincidentally. This possible coincidence should be taken into consideration in analysing whether necessary functions might be affected. Therefore, for protection against events that may affect plant-wide areas, separation by distance alone may not be adequate, and special provisions should be considered to strengthen the items or to protect them from the effects; for example, to isolate the air intake of the main control room in the event of toxic clouds.

Systematic inspections by expert engineers organized in a formal plant walkdown should be performed during commissioning to provide final verification of the design for external events, particularly floods, including also internal interactions through internal fire, flood, mechanical impact and electromagnetic interference; to verify that there are no unanticipated situations; and to provide sample verification of specific design features. The walkdown team should consist of experts in external events, design of nuclear structures and component design, together with systems analysts and plant operators.

**B.3.1 Loading derivation**

The derivation of the design basis parameters and the relevant loading scheme for the selected external hazards should be carried out consistently with the level of detail required for the design limit assessment (e.g., leak tightness, perforation and scabbing) and to the accuracy level associated with the design methods and procedures to be applied (e.g., linear, non-linear, three dimensional and dynamic).
Particular care should be taken with the derivation of static loads equivalent to time dependent effects, of load functions modelling the impacts between rigid bodies, of spatial averaging and of specific load cases for specific components from the same event.

Many of the loads corresponding to external events are loads of short duration and rapid rise time which are characterized by a finite energy or a defined momentum transfer. The loads are often localized, causing substantial local response of the individual target but with little effect on massive structures as a whole. Load–time functions can be derived by experimentation or analytical simulation, usually on rigid targets.

In general, full three dimensional finite element analysis of the fluid domain (impulse, in the case of wind or explosions) or full impact analysis (impact, in the case of aircraft crash or tornado missiles) are not used in the design process for the derivation of a suitable load function. Very detailed research programmes have been carried out in the engineering community and in some cases simplified engineering approaches are now available for a reliable design process, on the basis of the interpretation of test data or data from numerical analysis.

A very careful assessment of the basic assumptions and applicability limits of such simplified techniques should be carried out by the designer to check their applicability to the case of interest and their compatibility with the general accuracy level required in the design. A sensitivity analysis should always be conducted on input data and among different acceptable approaches.

Refined studies supported by numerical analyses and physical testing should be carried out for specific layout configurations: typical examples are the grouping effects among cooling towers, dynamic amplification of tall and slender stacks or, in the case of aircraft crash, the dynamic interaction effects on large and flexible slabs.

**B.3.2 Load combinations and acceptance criteria**

Because of their infrequent nature and very short duration, statistically independent loadings from any single external hazard are usually combined only with normal operational loads using unity load factors for all loadings. Multiple loadings such as aircraft crash and explosions usually do not have to be combined together. However, all effects from a single hazard should be properly time phased and combined, with due attention paid to the physical meaning of the combinations. Thus, for aircraft crash, the various effects of the impact (e.g., missiles, induced vibrations and fuel fires) should be combined. Furthermore, when a causal relationship exists between events (such as explosions or tsunami induced by earthquakes or a flood induced by a dam break), the effects should be properly time phased and combined.

Acceptance criteria (e.g., leak tightness, stability and operability) should be assessed according to the external event classification of the items. Such criteria should be interpreted in design terms, leading to appropriate design limits (e.g., allowed leak rate, maximum crack opening, elasticity and maximum displacement). However, for this process, it should be noted that while it is the practice to design for hazard loads on an elastic basis with normal operating limits, the severe local nature of these loads might make the evaluation of the safety margin very unreliable, and therefore a proper modelling of the physical reality, to the extent possible, should always be preferred.

Design which utilizes localized plastic deformation to absorb the energy input of the load is acceptable, provided that the overall stability of the structure is not impaired. Inelastic behaviour (localized plastic) is generally permissible for individual ductile structural elements (beams, slabs and their connections) where local inelastic deformation would not jeopardize the stability of the structure as a whole, and for protective substructures (restraints and barriers) whose sole function is to provide protection against hazard loads. Limited global or system inelastic behaviour (global plastic) is also permitted for frames, shear walls and other types of structural systems. However, the overall structure should be checked against reaction loads from the individual elements or substructures, and its response should generally remain within the linear domain.

**B.3.3 General guidance on the procedures for structural design**
Design for external hazards often requires a series of numerical models (finite elements, finite differences and fixed control volumes), local and global, and design formulas, oriented to capture the specific structural behaviour to be assessed.

The design models should be consistent and therefore special attention should be paid to the assessment of the data flow from one to another. In the case of numerical models used in sequence, attention should be paid to the accuracy level of any task of the sequence, in order to guarantee that the final results are representative of the real structural response.

The level of detail to be represented in the numerical models should allow an adequate representation of the reference structural behaviour: the need for very refined modelling (e.g., structural joints, steel rebars in reinforced concrete, structural interfaces and liners) should be reviewed, mindful of the need to balance the accuracy and the reliability of the analysis.

The finite element grid should be validated for any specific load case to be represented. Short duration loads (typical in explosions) often require dedicated models, different, for example, from the traditional dynamic models used for seismic analysis. Particularly, in order to avoid spurious filtering effects, a dense finite element grid should be used to represent the vibration field in the structure at high frequencies (above 20 Hz). Moreover, limitations to the finite element grid size should be adopted in explicit time integration schemes to avoid numerical instabilities.

In the definition of boundary conditions for the numerical models, the following should be considered:

- An evaluation of the influence of foundation or support properties on the response of the global models;
- An evaluation of the boundary conditions for local models, equivalent to the response of the remaining structural parts.

The design methodology, static or dynamic, linear or non-linear, should be consistent with the main loading characteristics and appropriate to the design limit to be assessed. Special care should be taken to ensure that the model dynamic behaviour is representative of the input frequency content.

Owing to the high variability of the results implicit in the complicated modelling approaches, any design procedures used in the external hazard simulation, numerical or analytical, should be validated through sensitivity analyses of the input data and assessed by means of alternative approaches with different complexity levels.

Design methods based on test results are particularly appropriate for loads in design basis external human induced events, on account of the wide spread of response predictions observed in non-linear numerical analyses not using benchmarked computer solutions. However, extreme care should be taken when empirical or semi-empirical approaches are employed outside the range of parameters of the corresponding database.

Vibratory motions and mechanical actions (e.g., those caused by debris, secondary missiles and gaps) calculated on the protecting structures should be analysed independently of and prior to any design limit assessment and prior to the qualification of anchored safety related equipment. Engineering judgement should be exercised in order to associate an appropriate uncertainty margin with the results (typically the floor response spectra) related to the modelling assumptions and to the intrinsic scattering of the input data.

Equipment required for performing the safety functions during and after the occurrence of an external hazard should be functionally qualified for the induced conditions, including vibrational loading. Particularly, qualification for impact or impulse loading may be quite different from qualification for earthquake induced vibrations, and therefore specific procedures should be selected, according to the performance required (stability, integrity and functionality).

The qualification conditions should be compared with the demand, usually represented by vibration, impact or impulse forcing functions at the anchoring on the structural support, but very stringent requirements could be derived by functionality under conditions of dust, smoke, humidity, cold temperatures or corrosive atmospheres, combined with stress. Adequate safety margins should be provided according to the item classification.
For some hazards, such as corrosive actions or biological phenomena, the degradation occurs over a considerable time period. In such cases, the design may not need to provide a high performance and durability of protective measures provided that the items or parts of items subject to degradation can be inspected. The inspection regimes should have scope, periodicity and method commensurate with the degradation rates. The installed protective measures should also be capable of reapplication or else the design should permit treatment to inhibit, stop or reverse the degradation.

B.3.4 Interaction effects

External hazards may cause direct damage to the plant: such effects are called primary effects. In addition, they may cause indirect damage (secondary effects) by means of interaction mechanisms that can propagate the damage. This indirect damage should be included in the analysis as it may cause damage which could exceed that caused by the primary effects.

In the systematic analysis of the interaction effects on safety related items and operator actions to be addressed in the design, the following should be evaluated and possibly included in the design basis:

- Secondary missiles (such as pieces of metal or concrete scabbed off walls, steel structures or parts of an aircraft itself, typically the engines);
- Falling objects loosened as a consequence of vibrations (mechanical interaction);
- Failure of high energy pipes and components;
- Flooding, from liquid retaining structures;
- Tsunami from earthquake;
- Chemical reactions: combustion, release of asphyxiant and toxic substances and corrosive liquids;
- Secondary fires from failures of electrical equipment;
- Electromagnetic interference.

All cascading secondary effects of the failure caused by an external hazard should be evaluated in the design process. Interaction effects are of such a nature that the potential damage can vary widely. Many factors come into play that are beyond the control of a designer and should be assessed by an appropriate walkdown. Because of these difficulties, preferred practice should be to emphasize the means of stopping the cascading effect, preferring global protection against the event rather than individual protection from all potential secondary effects.

Special emphasis should be given to potential interaction effects between UHS components (such as failure of cooling towers and flooding from the UHS basin) and other safety related structures.

A screening process should be carried out to evaluate the situations that give rise to the need for safety systems to operate as a consequence of interactions from a main hazard scenario.

The possibility of a hazard resulting in common cause failures through interaction effects should be considered.

B.3.5 Documentation and QA

The evaluation of a nuclear power plant for protection against external hazards should be documented in a manner suitable for a detailed technical review of conceptual assumptions and of detailed calculation procedures. As a minimum, the documentation should identify the events considered, their primary and secondary effects (if any) and the basis for determining the adequacy of protection for each case. The technical documentation should allow for a complete record of the data flow among the different design tasks for the purpose of accuracy assessment.

A technical evaluation should be carried out in accordance with the requirements of the quality assurance programme implemented for the design and operation of the nuclear power plant.

B.3.6 Accident monitoring and post-accident procedures
When an external hazard is deemed to be a sizing scenario for most safety related SSCs, a structural monitoring system (e.g., for displacement, deformation or stress) should be designed, installed and operated to prevent the development of accidents, as support for design confirmation and to guide post-event operator actions. Such systems should include sensors at the site, in the structure and in some critical equipment.

When practicable according to event characteristics (e.g., development time and possibility of forecasting), environmental monitoring should be designed, installed and operated to provide adequate warning signals for emergency operator actions for the external hazard with a relatively slow development time and to support the periodic safety review at the site as confirmation of the site specific hazard. Guidelines for emergency operator action should be developed. Such a system should include sensors at the site and at the potential sources of design basis events. When such a system supports emergency action by the operator, it should be classified as safety related.

The occurrence of external events significant to plant safety should be documented and reported. An extensive plant inspection after the occurrence of an external event should be performed in order to assess the behaviour and consequences for SSCs against their safety classification and accessibility and their representativeness of all external hazard classification items.

Provisions should be made in the design of the UHS and its directly associated heat transport systems to permit in-service monitoring and inspection so as to provide adequate assurance of its continued functional capability throughout the lifetime of the plant.

Water levels at intakes, tanks or reservoirs and water or air temperatures should be monitored. Instrumentation should be provided for the heat transport systems directly associated with the UHS to verify performance or to detect failures and malfunctions during system operation. The system flow rate, temperatures and activity, the status of components and other relevant parameters should be monitored.

The design should also include provisions for periodic testing of the heat transport systems directly associated with the UHS. The design should allow, to the extent practicable, testing of all the systems during power generation or at least during shutdown conditions, to the extent necessary to demonstrate their capability.
This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 945138.