Deliverable 3.4
Results of cross-case comparison of Safety Engineering processes
December 2022
Version 1.0

Elias Brådenmark, Carl Sunde and Stefan Authén
Risk Pilot AB
Blekholmstorg 30F
111 64 Stockholm
elias.bradenmark@riskpilot.se, carl.sunde@riskpilot.se, stefan.authen@riskpilot.se,
+46 8 652 84 50

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 945138.
## Table of Deliverables

<table>
<thead>
<tr>
<th>Deliverable No.</th>
<th>Deliverable title</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>D3.4</td>
<td>Results of cross-case comparison of Safety Engineering processes</td>
<td>1.0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Type</th>
<th>Dissemination level</th>
<th>Due date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Report</td>
<td>Public</td>
<td>M28</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Lead beneficiary</th>
<th>WP No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Pilot AB</td>
<td>3</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Main author</th>
<th>Reviewed by</th>
<th>Accepted by</th>
</tr>
</thead>
<tbody>
<tr>
<td>Elias Brådenmark, Carl Sunde, Stefan Authén</td>
<td>Frans Davelaar</td>
<td>Atte Helminen</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Contributing author(s)</th>
<th>Pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>213214</td>
<td></td>
</tr>
</tbody>
</table>

## Abstract

The main objective of Task 3.4 is to perform a cross-case comparison between the case studies belonging to the same case study group. The case studies were developed in Task 3.1 where first concise case study descriptions were elaborated by the project partners. Then the case studies were grouped into four different groups and a detailed case study description was elaborated for each case study. In Task 3.2 the grouping of case studies was revised and further developed, and BESEP Safety Requirement Topics were assigned to each case study group. Finally, self-evaluations of the case studies were performed within Task 3.3. The cross-case comparison that is described in this deliverable within Task 3.4 is based on the detailed case study descriptions (Task 3.1), the grouping of case studies (Task 3.2) and the self-evaluations of the case studies (Task 3.3). The results of the cross-case comparison will be used as input to Task 3.5 (elaboration of generalized cases) and as a support to the tasks to be performed within WP4 aiming at further detailed and overall evaluations.

The cross-case comparison has been performed within the four case study groups based on a template that provides guidance on the required contents and format of the comparison. Prior to the cross-case comparison the self-evaluations were to be complemented with a verification of all assigned BESEP requirement topics for each group and a more detailed description of the Safety Engineering Process. A short summary of the cross-case comparisons for each case study group is included in this report and the detailed comparisons are given in Appendix C-F.

The following are the key success factors for an efficient and integrated SEP identified by the four groups during the cross-case comparison (see Appendices for details):

### Structural Integrity (STIN):

- Safety measures should help ensure the fulfilment of current safety regulations unless they are explicitly related to a requested exemption.
- Safety measures should be consistent with the DID philosophy.
- Safety measures should help maintain sufficient safety margins.
- If there is some increase in risk despite the implementation of safety measures, such increase should be small and consistent with the intent of the regulatory policy statement on safety goals for the operations of nuclear power plants.
- The impact of safety measures should be monitored using performance measurement strategies, wherever possible and relevant.

### Loss of Ultimate Heat Sink (LUHS):

- The preferred main flow of information and actions: hazard analysis -> plant response analysis -> PSA model -> plant design.
- The safety analyses and their interconnections should be defined.
- Analyses should provide feedback to the design process and the modified design should be again analyzed.
A safety graded approach should be applied.
Evidence of the safety requirement fulfilment should be established via the pre-defined analyses and their interconnections.

Plant Vulnerability to Extreme Snow (PVES):

- A safety analysis master plan should be developed
- A multidisciplinary expert should be nominated.
- Planning of the interconnections between the different types of analyses and analysis steps should include the definition of milestones, application of unified input data, scheduling meetings to be organized to inform each other on intermediate or final results of a certain type of analysis.


- The application of a Claim, Argument and Evidence approach (CAE), makes it easier to identify possible shortcomings in requirement verifications.
- The three level SEP representation gives good insight to the failure analysis and their objective in the overall picture. The identified shortcomings can be removed by performing additional or more detailed failure analysis.
- A combination of the SEP approaches of the two case studies can help reach common understanding for the safety justifications and the application of a graded approach for failure analysis more efficiently, i.e., the three-level approach from the second case study is reinforced with the CAE approach from the first case study.

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

Notification
The use of the name of any authors or organization in advertising or publication in part of this report is only permissible with written authorisation from the VTT Technical Research Centre of Finland Ltd.

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

<table>
<thead>
<tr>
<th>Date</th>
<th>Version</th>
<th>Author</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>2022-10-21</td>
<td>V0.1</td>
<td>Elias Brådenmark, Stefan Authén, Carl Sunde</td>
<td>First draft of report sent to IAB and project partners.</td>
</tr>
<tr>
<td>2022-11-21</td>
<td>V0.2</td>
<td>Elias Brådenmark, Carl Sunde, Stefan Authén</td>
<td>Second draft of report sent to project partners for review.</td>
</tr>
<tr>
<td>2022-12-01</td>
<td>V0.3</td>
<td>Elias Brådenmark, Carl Sunde, Stefan Authén</td>
<td>Third draft of report sent to EDF for peer review.</td>
</tr>
<tr>
<td>2022-12-20</td>
<td>V1.0</td>
<td>Elias Brådenmark, Carl Sunde, Stefan Authén</td>
<td>Final version</td>
</tr>
</tbody>
</table>
**LIST OF ABBREVIATIONS**

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BESEP</td>
<td>Benchmark Exercise on Safety Engineering Practices</td>
</tr>
<tr>
<td>CCF</td>
<td>Common Cause Failure</td>
</tr>
<tr>
<td>CDF</td>
<td>Core Damage Frequency</td>
</tr>
<tr>
<td>CEA</td>
<td>Claim-Argument-Evidence approach</td>
</tr>
<tr>
<td>DBA</td>
<td>Design Basis Accident</td>
</tr>
<tr>
<td>DEC</td>
<td>Design Extension Condition</td>
</tr>
<tr>
<td>DID</td>
<td>Defense-In-Depth</td>
</tr>
<tr>
<td>DSA</td>
<td>Deterministic Safety Assessment</td>
</tr>
<tr>
<td>EIIC</td>
<td>External Impact on Safety Classified Instrumentation and Control Systems</td>
</tr>
<tr>
<td>ESWS</td>
<td>Essential Service Water System</td>
</tr>
<tr>
<td>FDF</td>
<td>Fuel Damage Frequency</td>
</tr>
<tr>
<td>HEP</td>
<td>Human Error Probability</td>
</tr>
<tr>
<td>HFE</td>
<td>Human Factors Engineering</td>
</tr>
<tr>
<td>HRA</td>
<td>Human Reliability Analysis</td>
</tr>
<tr>
<td>HSI</td>
<td>Human-System Interface</td>
</tr>
<tr>
<td>IHA</td>
<td>Important Human Actions</td>
</tr>
<tr>
<td>I&amp;C</td>
<td>Instrumentation and Control</td>
</tr>
<tr>
<td>LERF</td>
<td>Large Early Release Frequency</td>
</tr>
<tr>
<td>LUHS</td>
<td>Loss of Ultimate Heat Sink</td>
</tr>
<tr>
<td>PSA</td>
<td>Probabilistic Safety Assessment</td>
</tr>
<tr>
<td>PVES</td>
<td>Plant Vulnerability to Extreme Snow</td>
</tr>
<tr>
<td>SEP</td>
<td>Safety Engineering Process</td>
</tr>
<tr>
<td>SSC</td>
<td>Structure, System and Component</td>
</tr>
<tr>
<td>STIN</td>
<td>Structural Integrity</td>
</tr>
<tr>
<td>V&amp;V</td>
<td>Verification and Validation</td>
</tr>
<tr>
<td>WP</td>
<td>Work Package</td>
</tr>
</tbody>
</table>
# Table of Contents

## History of Changes .................................................................................................... 4

## List of Abbreviations ................................................................................................. 5

## List of Figures .............................................................................................................. 7

## List of Tables ................................................................................................................. 7

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

2. **The Basis for the Cross-Case Comparison** .......................................................... 8
   2.1 Objectives of BESEP .............................................................................................. 8
   2.2 BESEP Safety Requirement Topics ........................................................................ 9
   2.3 Grouping of case studies and assignment of BESEP requirement topics .......... 10
   2.4 Safety Margin and Safety Engineering Process .................................................... 12
       2.4.1 Safety Margin .................................................................................................. 12
       2.4.2 Safety Engineering Process ............................................................................ 14
   2.5 Self-evaluations of case studies .......................................................................... 16

3. **Development of a Method for Cross-Case Comparison** ....................................... 16
   3.1 Cross-case comparison method outline ............................................................... 16
   3.2 Workshop .............................................................................................................. 17
       3.2.1 BESEP Safety requirement topics ................................................................. 17
       3.2.2 Safety Engineering Process ......................................................................... 17
       3.2.3 Updating the self-evaluations ...................................................................... 19
       3.2.4 Template for cross-case comparison ........................................................... 20

4. **Cross-Case Comparison Conclusions** .................................................................. 20
   4.1 Structural Integrity (STIN) ..................................................................................... 21
       4.1.1 Fulfilment of BESEP Safety Requirements .................................................... 21
       4.1.2 Safety Margins Assessment ........................................................................... 21
       4.1.3 Interactions between DSA, PSA and HFE ..................................................... 21
       4.1.4 Overall Safety Engineering Process .............................................................. 22
       4.1.5 Key Success Factors for an Efficient and Integrated SEP ......................... 22
   4.2 Loss of Ultimate Heat Sink (LUHS) ...................................................................... 22
       4.2.1 Fulfilment of BESEP Safety Requirements .................................................... 22
       4.2.2 Safety Margins Assessment ........................................................................... 23
       4.2.3 Interactions between DSA, PSA and HFE ..................................................... 23
       4.2.4 Overall Safety Engineering Process .............................................................. 23
       4.2.5 Key Success Factors for an Efficient and Integrated SEP ......................... 24
   4.3 Plant Vulnerability to Extreme Snow (PVES) ....................................................... 24
       4.3.1 Fulfilment of BESEP Safety Requirements .................................................... 24
       4.3.2 Safety Margins Assessment ........................................................................... 24
       4.3.3 Interactions between DSA, PSA and HFE ..................................................... 25
4.3.4 Overall Safety Engineering Process

4.3.5 Key Success Factors for an Efficient and Integrated SEP

4.4 External Impact on Safety Classified I&C Systems (EIIC)

4.4.1 Fulfilment of BESEP Safety Requirements

4.4.2 Safety Margins Assessment

4.4.3 Interactions between DSA, PSA and HFE

4.4.4 Overall Safety Engineering Process

4.4.5 Key Success Factors for an Efficient and Integrated SEP

5 CONCLUSIONS OF THE CROSS-CASE COMPARISON

REFERENCES

APPENDIX A: INSTRUCTIONS FOR UPDATING SELF-EVALUATIONS OF THE CASE STUDIES

APPENDIX B: TEMPLATE FOR CROSS-CASE COMPARISON

APPENDIX C: CROSS-CASE COMPARISON IN CASE STUDY GROUP STIN

APPENDIX D: CROSS-CASE COMPARISON IN CASE STUDY GROUP LUHS

APPENDIX E: CROSS-CASE COMPARISON IN CASE STUDY GROUP PVES

APPENDIX F: CROSS-CASE COMPARISON IN CASE STUDY GROUP EIIC

LIST OF FIGURES

Figure 1: The overall structure of the benchmark exercise [1].

Figure 2: Setting safety limit and keeping operating values below the safety limit [5].

Figure 3: Safety limit and safety margin concepts in deterministic safety analysis [5].

Figure 4: Probabilistic safety margin [5].

Figure 5: The safety analyses element of safety design [5].

Figure 6: NPP V-model [5].

Figure 7: Illustration of different levels of the SEP (using PSA as an example).

Figure 8: Example of a graphical representation of the SEP.

Figure 9: Overview of the generalised SEP from case study group EIIC.

LIST OF TABLES

Table 1: Final Case Study Groups and the Corresponding Case Studies [4].

Table 2: Assignment of BESEP Safety Requirement Topics to Case Study Groups [4].
1 Introduction

The main objective of Task 3.4 was to perform a cross-case comparison between the case studies belonging to the same case study group. The case studies were developed in Task 3.1 where first concise case study descriptions were elaborated by the project partners. Then the case studies were grouped into four different groups and a detailed case study description was elaborated for each case study. In Task 3.2 the grouping of case studies was revised and further developed, and BESEP Safety Requirement Topics were assigned to each case study group. Finally, self-evaluations of the case studies were performed within Task 3.3. The cross-case comparison that is described in this deliverable within Task 3.4 was based on the detailed case study descriptions (Task 3.1), the grouping of case studies (Task 3.2) and the self-evaluations of the case studies (Task 3.3). The results of the cross-case comparison will be used as input to Task 3.5 (elaboration of generalized cases) and as a support to the tasks to be performed within WP4 aiming at evaluations.

The basis for cross-case comparison, as stated above, is Tasks 3.1-3.3. Moreover, the work done in Tasks 2.1-2.3 also forms the basis for the cross-case comparison. Before the method for cross-case comparison was developed the work done previously in the project was re-visited (Section 2).

A method outline for performing the cross-case comparison was presented. The method was discussed and developed during a project workshop (Section 3). This resulted in the need of an up-date of the self-evaluations that was supported by creating instructions for the up-date. A template for the cross-case comparison was also prepared to give guidance on the required contents and format of the comparison.

The cross-case comparisons were made by each case study group based on the template. A short summary of the cross-case comparisons for each case study group is included in Section 4 and the detailed comparisons are given in Appendix C-F.

Finally, conclusions from general findings during the work in Task 3.4 are presented in Section 5.

2 The Basis for the Cross-Case Comparison

This section presents a brief summary of the work performed earlier within the BESEP project that founded the basis of the work performed within Task 3.4.

2.1 Objectives of BESEP

The project proposal [1] provides the plan and scope of the benchmark exercise. In section 1.3.1.1 Safety design and Safety Engineering process the definition for Safety Engineering Process (SEP) is given as activities connecting together the main elements of safety design: safety requirements, safety analyses and plant design. The SEP should take care of a change in any of these elements by reflecting it in the other two elements. The safety analyses can traditionally be categorized into deterministic safety analysis (DSA), probabilistic safety analysis (PSA) and human factors engineering (HFE). It is a task for the SEP to ensure the information flow and utilisation within and between each element.

The project proposal states that case studies shall be collected from the project partners. The case studies should be grouped into case study groups using a set of requirements determined in accordance with a benchmark baseline, developed in WP2. Safety analyses, safety requirements to be met, similarities of the SSCs and external hazards are the attributes that form the basis for grouping. As seen in Figure 1, which serves as an example for grouping, three case study groups are created based on requirements to be met, SSCs, and external hazards.
In Task 3.4 the applied safety analysis methods and SEPs are studied and compared. The vertical flow in Figure 1 illustrates the comparison of compliance of safety margins, requirements verification, the interconnection and flow of information between safety analyses, and possible successes and challenges with the used SEP. The purpose of the comparison is stated as to evaluate the efficiency and integration of safety analysis methods involved in the SEP.

2.2 BESEP Safety Requirement Topics

The work performed in WP 2 started with Task 2.1 Assignment of safety requirement topics for selected external hazards. During this task the initial pool of case studies that were collected prior to the project, presented in [1], was used as a basis for identification of relevant external hazards likely to be included in the BESEP project. The following external hazards were identified:

- Natural non-seismic and seismic hazards:
  - extreme wind,
  - tornado,
  - extreme snow,
  - extreme rain,
  - extremely high or extremely low air temperature,
  - icing (glaze ice and rime),
  - low water level in river,
  - high sea level,
  - earthquake.

- Human-induced hazards:
  - aircraft crash,
  - malicious attacks.

To these external hazards different IAEA requirements and safety analyses were assigned, which are presented in chapter 7 of Deliverable 2.1 [2], intended to be used to identify safety requirement topics for the individual external hazards.

Task 2.2 developed an updated set of requirement topics, based on the preliminary case studies and general experience of the BESEP partners. These sets of requirement topics were related to the different safety analyses identified in Task 2.1:

- Deterministic Safety Analysis
  - Physical separation and structural integrity
o Functional separation to provide defense against failure propagation
o Diversity and common-cause failure criteria
o Redundancy and single failure criteria
o Independence and strength of the individual defense-in-depth levels
o Justification of the engineering assumptions used in analysis

• Probabilistic Safety Analysis
  o Risk-informed management and balance of nuclear power plant design
  o Fulfilment of quantitative safety goals
  o Initiating event frequency estimation
  o Assessment of potential losses of safety functions
  o Uncertainty analysis of accident sequences and operating times
  o Confidence provision for defense against the occurrence of cliff-edge effects
  o Support for developing abnormal and emergency operating procedures and severe accident guidelines

• Human Factors Engineering
  o Situation awareness and assessment
  o Guidance selection, decision making and intelligent use of guidance
  o Applicable HSI (Human System Interface)
  o Team working, effective communication and collaboration
  o Workload, stress and fatigue management

• Safety engineering practices
  o Safety engineering management
  o Safety design and requirement management for external hazards
  o Flow of information between safety analyses
  o Verification and validation (V&V) of design
  o System modification and configuration management
  o Validated modelling and simulation analysis tools

The BESEP Safety Requirement Topics are further explained in chapter 3 of Deliverable 2.2 [3].

2.3 Grouping of case studies and assignment of BESEP requirement topics

The grouping of the case studies was performed in Task 3.2 based on the detailed case study descriptions elaborated during Task 3.1. The benchmark baseline defined in Deliverable 2.2 was the basis of grouping [3]. On these grounds, it was considered that the following attributes should have a key role in the process of grouping:

• IAEA safety requirements
• BESEP safety requirements to be met
• types of safety analyses used to determine safety margin beyond the relevant design basis hazards for a particular SSC
• similarity of external hazards
• similarity of SSCs
• Types of administrative or technical measures implemented as a result

Some key features were identified to capture the commonalities among the case studies. These key features were selected with the expectation that the grouping should differ for the different case study groups. Four types of case study groups were developed with respect to these key features:

• requirement- based case study group;
• safety function-based case study group;
• hazard-based case study group;
• SSC-based case study group.

The final grouping of case-studies is shown in Table 1 and the BESEP requirement topics associated with each case study group are shown in Table 2 with the main topic for each group highlighted in bold letters.
### Table 1: Final Case Study Groups and the Corresponding Case Studies [4].

<table>
<thead>
<tr>
<th>Case Study ID</th>
<th>Responsible Partner</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>STIN_1</td>
<td>RELKO</td>
<td>Collapse of Venting Stack Due to High Wind</td>
</tr>
<tr>
<td>STIN_2</td>
<td>UJV</td>
<td>Probabilistic Analysis of Aircraft Crash Risk for NPP Dukovany</td>
</tr>
<tr>
<td>STIN_3</td>
<td>VTT</td>
<td>Loss of Heat Removal of Spent Fuel Pool due to External Impact</td>
</tr>
<tr>
<td>LUHS_1</td>
<td>FORTUM</td>
<td>Loss of Ultimate Heat Sink (Frazil Ice or Oil Spill)</td>
</tr>
<tr>
<td>LUHS_2</td>
<td>RELKO</td>
<td>Loss of the Service Water System due to Extremely Low Temperature</td>
</tr>
<tr>
<td>LUHS_3</td>
<td>RISK PILOT</td>
<td>Blockage of (Water) Intake Building</td>
</tr>
<tr>
<td>LUHS_4</td>
<td>NUBIKI</td>
<td>Evaluation of Plant Vulnerabilities to Riverine Events</td>
</tr>
<tr>
<td>PVES_1</td>
<td>RISK PILOT</td>
<td>Extreme Snow and Wind Affecting Diesel Generators</td>
</tr>
<tr>
<td>PVES_2</td>
<td>NUBIKI</td>
<td>Protection of the Reactor Hall from the Effects of Extreme Snow</td>
</tr>
<tr>
<td>PVES_3</td>
<td>UJV</td>
<td>Analysis of Extreme Snow Risk for NPP Dukovany</td>
</tr>
</tbody>
</table>

### Table 2: Assignment of BESEP Safety Requirement Topics to Case Study Groups [4].

<table>
<thead>
<tr>
<th>Discipline</th>
<th>BESEP Safety Requirement Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>STIN – Structural Integrity (requirement based case study group)</td>
<td><strong>Physical separation and structural integrity</strong></td>
</tr>
<tr>
<td>DSA</td>
<td><strong>Physical separation and structural integrity</strong></td>
</tr>
<tr>
<td>PSA</td>
<td>Confidence provision for defence against the occurrence of cliff-edge effects</td>
</tr>
<tr>
<td>HFE</td>
<td>Workload, stress and fatigue management</td>
</tr>
<tr>
<td>SEP</td>
<td>Flow of information between safety analyses</td>
</tr>
<tr>
<td>LUHS – Loss of Ultimate Heat Sink (safety function based case study group)</td>
<td><strong>Functional separation to provide defence against failure propagation</strong></td>
</tr>
<tr>
<td>DSA</td>
<td>Functional separation to provide defence against failure propagation</td>
</tr>
<tr>
<td>PSA</td>
<td><strong>Assessment of potential losses of safety functions</strong></td>
</tr>
<tr>
<td>HFE</td>
<td>Situation awareness and assessment</td>
</tr>
<tr>
<td>SEP</td>
<td>Verification and validation (V&amp;V) of design</td>
</tr>
<tr>
<td>PVES – Plant Vulnerability to Extreme Snow (hazard based case study group)</td>
<td><strong>Justification of the engineering assumptions used in analysis</strong></td>
</tr>
<tr>
<td>DSA</td>
<td>Justification of the engineering assumptions used in analysis</td>
</tr>
<tr>
<td>PSA</td>
<td>Support for developing abnormal and emergency operating procedures and severe accident guidelines</td>
</tr>
<tr>
<td>HFE</td>
<td>Guidance selection, decision making and intelligent use of guidance</td>
</tr>
<tr>
<td>SEP</td>
<td><strong>Safety design and requirement management for external hazards</strong></td>
</tr>
<tr>
<td>EIIC – External Impact on Safety Classified I&amp;C Systems (SSC based case study group)</td>
<td><strong>Diversity and common-cause failure criteria</strong></td>
</tr>
<tr>
<td>DSA</td>
<td>Diversity and common-cause failure criteria</td>
</tr>
<tr>
<td>PSA</td>
<td>Initiating event frequency estimation</td>
</tr>
<tr>
<td>HFE</td>
<td>Applicable HSI (Human System Interface)</td>
</tr>
<tr>
<td>SEP</td>
<td>Validated modelling and simulation analysis tools</td>
</tr>
</tbody>
</table>
2.4 Safety Margin and Safety Engineering Process

The Safety Engineering Process (SEP) and the assessment of Safety Margins are both focus areas of the case study descriptions and self-evaluations. The concept of SEP and Safety Margins related to different topics (DSA, PSA, HFE) were elaborated in Task 2.3. This forms the basis for the cross-case comparison together with the verification of the BESEP Safety requirements.

2.4.1 Safety Margin

In Deliverable 2.3 [5] the concept of Safety margins was elaborated. In Chapter 4.1 of Deliverable 2.3 the safety margin is described on a general level using a load-strength approach which is in line with the IAEA definition. As seen in Figure 2 the parameters $S$ (strength) and $L$ (load) are described by probability density functions. The goal of safety margin presentation is to demonstrate that the overlap between the probability density functions is very small thus producing negligible risk to the plant.

![Figure 2: Setting safety limit and keeping operating values below the safety limit][5].

Based on the general load-strength approach deterministic, probabilistic and HFE safety margins are described and discussed in Deliverable 2.3.

2.4.1.1 Deterministic Safety Margin

In Chapter 4.2 of Deliverable 2.3 the Deterministic Safety Margin is defined. The safety margin is understood as the difference in physical units between the regulatory acceptance criteria and the results provided by the calculation of the relevant plant parameter or physical phenomena, as seen in Figure 3.
2.4.1.2 Probabilistic Safety Margin

The *Probabilistic Safety Margin* is defined in Chapter 4.3 of Deliverable 2.3 as the difference between the established probabilistic safety targets acceptable to the regulatory body and the calculated value of the risk parameter including uncertainties, as demonstrated in Figure 4. The risk parameters considered for *Probabilistic Safety Margin* are core damage frequency (CDF) and large early release frequency (LERF).

2.4.1.3 HFE Safety Margin

Safety margins for human actions are discussed in Chapter 4.4 of Deliverable 2.3. Within the HFE program human actions are typically not associated with safety margins. The HFE program consists of 12 elements, aimed at ensuring that the concept of HFE is incorporated to the plant design. One of those elements is *treatment of important human actions* (IHA). The IHA identifies the human actions most important to safety via the DSA and PSA to address them in the HFE program. In the DSA human actions can be credited to prevent or mitigate accidents or transients. These human actions may or may not be seen as risk-important by the PSA. In Human Reliability Analysis (HRA), which is an integral part of the PSA, human actions are evaluated to determine the probability for human error and the mechanisms of the error. The human actions credited in DSA and the human actions evaluated in HRA are more related to safety margin determination than the HFE-program.

It is possible to characterize the safety margin to the human action by demonstrating that the action can be performed within a certain time span or try to identify any safety margin that may be applicable to the particular case. In the HRA the qualitative analysis of identified human actions is quantified into *human error probabilities*.
HEPs). If there is evidence that the human action can be performed within a certain time span which is shorter than the available time the difference in time could be interpreted as a safety margin. The human actions considered in HRA, and thus relevant, are divided into three categories:

1. Actions causing PSA initiating events;
2. actions causing failures in safety-related systems with possible latent effect on system availability;
3. actions taken in response to initiating event occurrence.

2.4.2 Safety Engineering Process

In Deliverable 2.3, Chapter 2 and 3, [5] the SEP for the BESEP project is elaborated. It is concluded that the three main elements of the SEP for BESEP are safety requirements, plant design and safety analyses, as can be seen in Figure 5. The BESEP objective is developing practices for safety requirements verification, against external hazard using efficient and integrated set of Safety Engineering practices and probabilistic safety assessment. Different safety analyses and their interactions are vital for providing insight to this.

![Figure 5: The safety analyses element of safety design [5].](image)

The SEP definition presented in Deliverable 2.3 is based on the ISO/IEC/IEEE 15288 standard. The relevant activities in the standard have been selected and studied within BESEP as is presented in Chapter 3.4 of Deliverable 2.3. The deliverable presents the activities in a V-model, as it can be seen in Figure 6.
The left side in the V-model divides the process based on functional, architectural, system and equipment level. The right side of the model presents the V&V, analyses and interconnection tests. In stage 10 typically FMEA, initiating event analysis and CCF analysis are performed. In steps 11 and 12 hazard and interface analyses, separation analyses and consequential failure analyses are typical analyses. Functional level analyses are deterministic, probabilistic, and human factors. In step 13, the role of PSA for integration of individual conclusions regarding plant safety is pointed out.

To evaluate and assess the efficiency and integration of the different safety analyses methods in the SEP, Deliverable 2.3 Appendix B is suggested for process capability assessment. This approach is based on ISO/IEC 33020 and assumes that the different steps in the SEP are clearly defined.

However, in the conclusions of Deliverable 2.3 it is stated:

*The Safety engineering process provided in this report is at quite an abstract level to be compliant with the level of typical process capability assessment. Hence, the ideas and suggestions listed above in this chapter should be developed further in Work Packages 3 and 4 to identify the more specific safety engineering and safety margin assessment criteria in the scope of BESEP project.*

Hence, the Safety Engineering Process would need to be better defined to be able to perform a meaningful cross-case comparison within Task 3.4.
2.5 Self-evaluations of case studies

The primary basis for the cross-case comparison is the detailed case study descriptions elaborated in Task 3.1 (but presented in Deliverable 3.3) [6] and the Self-evaluations from Task 3.3. For each case study a self-evaluation was elaborated based on the template given in Deliverable 3.3 [7].

During the development of the self-evaluations, it was realized that the case studies within the same case study group had not always addressed the same safety requirement topics and the associated safety requirements from each requirement topic, see Chapter 2.3 regarding the assigned BESEP safety requirement topics. This lack of completeness of the self-evaluations was foreseen to negatively affect the usefulness of the self-evaluation in support of cross-case comparison. Accordingly, the partners were encouraged to address as many requirements of the four topics assigned to each case group in the case studies as possible. However, after the update of the detailed case study descriptions and self-evaluations, not all the assigned BESEP requirements were addressed completely by all case studies. Therefore, this needed to be further elaborated in Task 3.4.

3 Development of a method for cross-case comparison

The comparison between individual case studies within the same case study group should be performed to evaluate the efficiency and integration of different safety analysis methods. As stated in section 2.1 the cross-case comparison achieves this through comparing the cases based on safety requirements, external event, SSCs, and safety analyses. The method development intended to include all partners and therefore the Task Leader of T.3.4 prepared a method outline to present to the rest of the partners during a project workshop. After the workshop a template for the cross-case comparison was to be compiled by the Task Leader and then sent out to the partners for commenting. The following subchapters present the conclusions made during the workshop and the work performed thereafter.

3.1 Cross-case comparison method outline

The outline of the method prepared by the Task Leader prior to the workshop consisted of five steps:

1. Establish common definition/baseline
2. Define criteria for cross-case comparison
3. Collect additional information
   a. Up-date of self-evaluation
   b. Up-date of detailed case study description
4. Self-evaluation within case study groups
5. Compilations and conclusions

The first step intended to create a common definition of both the BESEP Safety Margins, respectively for DSA, PSA and HFE and the SEP to be used as a basis for the comparison within the case study groups. The Safety Margins and SEP were developed for the purposes of the project in Deliverable 2.3, but it was found important to revisit the findings of Deliverable 2.3 before starting the cross-case comparison.

During the second step the partners defined criteria for evaluation of compliance of Safety Margins and requirements verification, as well as criteria for evaluating the interconnection and flow of information between Safety Analyses, and criteria for comparing the possible successes and challenges of the SEP.

Based on the common baseline and the defined evaluating criteria, as well as what had been stated in Deliverables 2.3 and 3.2 step three intended to identify information that was missing in the detailed case study descriptions and self-evaluations. The missing information needed was to be added.

The fourth step was the self-evaluation. The evaluation is proposed to be done within the case study groups with one partner assigned as responsible for the evaluation. The self-evaluation was done based on a template to be distributed after the workshop. However, there might be a need for an iterative process regarding the definition of criteria for comparison.
The last step of the method outline was the compilation of results from the case study group specific self-evaluations and the compilation of Deliverable 3.4.

3.2 Workshop

During the beginning of Task 3.4 a common 3-day workshop was organized with all the participants of the project. The first part of the workshop was dedicated to discussing the previous tasks in the project which builds the foundation for the cross-case comparison. The focus was on discussing and elaborating the link between Task 3.4 and the previous Tasks 2.3 and 3.1-3.3.

The method for performing the cross-case comparison was presented and discussed during the workshop. In order to be able to perform the cross-case comparison the following issues were identified that needed to be solved:

- **BESEP Safety requirement topics**
  All case studies should revise which BESEP safety requirement topics to address.

- **Safety Engineering Process**
  The definition and description of the SEP was refined during the workshop

- **Up-dating of self-evaluations**
  The self-evaluations need to be updated prior to the cross-case comparison

- **Template for cross-case comparison**
  A template for cross-case comparison should be developed.

The above bullets resulted in updating self-evaluations and development of a template for cross-case comparison. These activities are described below.

3.2.1 BESEP Safety requirement topics

One group of the attributes used for dividing the case studies into case study groups were the BESEP Safety Requirements. When the detailed case study descriptions were prepared by the partners as a part of Task 3.1 the work regarding dividing the case studies into case study groups in Task 3.2 was performed in parallel. The work in Task 3.2 included assigning BESEP Safety Requirement topics to the preliminary case study groups consisting of 13 detailed case studies. The partners were to address at least one of the BESEP Safety Requirements related to the relevant Safety Requirement Topic. The assignment of the BESEP Safety Requirement Topics intended to help ensuring a good coverage of the BESEP Safety Requirement Topics in each group and to create a common BESEP requirement baseline for the cross-case comparison. During Task 3.3 disparities within case studies in the same case study group concerning addressing the assigned BESEP requirements within the assigned Safety Requirement Topic were identified. The self-evaluations should therefore iterate through the BESEP Safety Requirements to ascertain that they are addressed in the self-evaluation.

During the workshop it was concluded that for the respective self-evaluations there were still several BESEP Safety Requirements left out to be addressed to enable a meaningful cross-case comparison within the case study groups. The partners therefore concluded that this should be performed as a part of the update of the self-evaluation described in section 3.3.

3.2.2 Safety Engineering Process

The SEP consists of three main elements: plant design, safety analyses and safety requirements. One important goal of the SEP is to show that the plant design fulfils the safety requirements through safety analyses.

During the workshop the method for evaluating the respective SEPs presented in the different case studies was discussed. The method proposed in Deliverable 2.3 Appendix B consists of different so called process
capability assessment attributes that would be applicable to isolated steps within a SEP (the steps are described in Deliverable 2.3 Appendix A). During the workshop it was concluded that the use of those process capability assessment attributes would not be feasible for the project since the process steps and the process capability assessment attributes are given at a too abstract level. Hence, the related ideas and suggestions should be developed further in Work Packages 3 and 4. Therefore it was discussed during the workshop how the description of the SEP could be made more specific. This resulted in a view of the SEP on three different levels (see Figure 7):

- Level 1: Relations between Safety requirements- Safety analysis- Plan design
- Level 2: Interconnection between DSA-PSA-HFE(HRA)
- Level 3: Relations within the analyses, e.g. PSA

![Figure 7: Illustration of different levels of the SEP (using PSA as an example)](image)

It was also decided during the workshop that it would be fruitful for the cross-case comparison to describe the SEP using a graphical representation together with a textual presentation of the activities/steps and the flow of information defining the SEP. The description should include all levels of the SEP as stated above. In Figure 8 an example of a graphical representation of the SEP is shown. The boxes represent different activities within the SEP and the arrows represent the flow of information between the different activities.
3.2.3 Updating the self-evaluations

Based on the above discussions held during the workshop related to the BESEP Safety Requirement Topics and the SEP it was decided that the case self-evaluations were to be updated with the aim to facilitate a better cross case comparison. It was also seen useful to up-date the general quality of the self-evaluations in order to follow the template for the self-evaluations given in Task 3.3. Since the self-evaluations are based on the case study description it was also proposed to update the case study descriptions.

Instructions for updating the self-evaluations were developed within Task 3.4 and sent to the project partners, the complete instruction for updating the self-evaluations is presented in Appendix A. The following topics were to be addressed in the update:

- Address all requirement topics assigned to the case study group.
- If decided within the case study group, evaluate additional requirement topics and requirements as agreed upon.
- Perform a quality check of the self-evaluation to improve the general quality, i.e., check that the template for the self-evaluation is followed and all questions therein are clearly answered in the self-evaluation.
- Update the detailed case study descriptions based on the update of the self-evaluations, if seen necessary.
- Make a graphical representation of the SEP with a description of the relations (flow of information) and steps.

According to the instructions the partners made updates to their self-evaluations, the updated self-evaluations are not included in this report. However, they are the foundation of the cross-case comparison which are given in Appendix C-F.
3.2.4 Template for cross-case comparison

The cross-case comparison was performed within each case-study group. One project partner per case-study group was assigned as a leader of the work:

- STIN - RELKO
- LUHS - FORTUM
- PVES - NUBIKI
- EIIC - VTT

The cross-case comparison was discussed during the workshop, and it was agreed that a template for performing the cross-case comparison should be developed to facilitate the comparison. The purpose of the template was to align the comparison between the different groups, to enable easy documentation in the deliverable of Task 3.4 and utilize the work performed during Tasks 3.1-3.3.

The basis for the template of cross-case comparison was the template used for the self-evaluations in Task 3.3. Moreover, insights from the development of the self-evaluations were used. The complete template is presented in Appendix B and it includes the following main topics:

- General information
  General information about the case studies should be included in the case study group. Information about involved project partners should be given.

- Fulfilment of BESEP Safety Requirements
  Key features and adequacy of the verification process of the fulfilment of BESEP Safety Requirements should be compared. Proposals for improvement of the verification process should be identified. All BESEP requirement topics assigned to the case study group and all BESEP requirements within each topic (unless otherwise decided within the case study group) should be addressed.

- Safety Margins Assessment
  A comparison of the definition, assessment and evaluation of the Safety Margins (DSA, PSA and HFE) used in the case studies should be performed. It should be discussed in relation to the definitions used for Safety Margin in Task 2.3. Improvements should be identified.

- Interactions between DSA, PSA and HFE
  The interconnections and exchange of information between PSA and DSA should be compared and described. A comparison should be performed on how the HFE is connected to safety analyses methods DSA/PSA. Strengths and good practices of interconnecting the safety analyses and possible alternative interconnections and information exchange that could be beneficial to apply should be identified.

- Overall Safety Engineering Process
  The overall Safety Engineering Process approaches, steps and flows of information should be compared. Strengths and weaknesses, and challenges and successes of the different SEP approaches should be revealed and evaluated.

- Key success factors for an efficient and integrated SEP
  Based on the comparison, the key success factors for an efficient and integrated SEP should be described and elaborated. A generalised SEP should be elaborated and described which can be used in Task 3.5 (Description of generalized case studies).

The above topics were prescribed to be elaborated in free text format by each case study group using the self-evaluations of the case studies included in each group. The most important information should then be extracted into a table-format.

4 Cross-case comparison conclusions

In the following sections, the results from the cross-case comparisons of the four case study groups are summarized. The detailed cross-case comparisons are given in Appendix C-F.
4.1 Structural Integrity (STIN)

The STIN (Structural Integrity) case study group consists of three case studies:

- Collapse of Venting Stack Due to High Wind (STIN 1)
- Probabilistic Analysis of Aircraft Crash Risk for NPP Dukovany (STIN 2)

The complete cross-case comparison can be found in Appendix C and a short summary is presented in this section.

4.1.1 Fulfilment of BESEP Safety Requirements

Since all the case studies address structural analysis the BESEP requirement topics related to Physical separation and structural integrity were fulfilled in a similar way by all case studies, DSA were performed to show that the redundant safety systems are able to perform safety functions despite the effects of external events.

Related to the BESEP requirement topic Confidence provision for defence against the occurrence of cliff-edge effects PSA were used in two of the three case studies for requirement verification.

4.1.2 Safety Margins Assessment

**DSA safety margin**

No common definition of the deterministic safety margin exists within the case study group. In the comparison it is stated that the different definitions of safety margin coincide with Deliverable 2.3. Moreover, it is concluded that interpretation of relevant safety margins in the case studies are in good agreement with chapter 4.1 of Deliverable 2.3.

**PSA safety margin**

All the case studies within the group uses Core Damage Frequency (or Fuel Damage Frequency) and LERF as the measure for PSA Safety Margin. The mean values of CDF (FDF) and LERF are used for comparison with the safety targets. Chapter 4.3 of Deliverable 2.3 proposed the upper bound for comparison. Therefore, the PSA safety margin in the case studies is not directly in line with the definition in Chapter 4.3 of Deliverable 2.3.

**HFE safety margin**

No clear definition of HFE safety margins is made within the case studies. It is stated that in general, HFE safety margins are not really defined, but HRA may contribute to the discussion of human factor related margins. A more holistic approach is needed to better integrate stress, workload, fatigue and other factors that contribute to operators’ cognitive readiness into HFE analyses. Procedure development should be based on systematic task analysis and task complexity analysis.

4.1.3 Interactions between DSA, PSA and HFE

There are some interactions described between the different categories of analyses. However, two of the case studies have a focus on PSA which means that the DSA and HFE (HRA) only supports the PSA-study with inputs. There seems to be little feed-back from the PSA to the DSA and HFE which means that the interactions are basically one-way interactions.

One case study describes possible improvements stating that the inputs from DSA/PSA to HFE could be made more systematic. The other two case studies have not identified any improvements in the interaction between the safety analyses.
4.1.4 Overall Safety Engineering Process

The safety analyses needed within the SEP are identified in the case studies. PSA models are developed in two of the three case studies. The cross-case comparison refers to the self-evaluations for details about the overall Safety Engineering Process.

4.1.5 Key Success Factors for an Efficient and Integrated SEP

The key success factors for an efficient and integrated SEP which is used to implement changes (safety measures) into the plant to remove weaknesses have been identified. The proposed safety measures are implemented on the basis of risk-informed decision making where a set of key principles (success factors) should be met:

- Safety measures should help ensure the fulfilment of current safety regulations unless they are explicitly related to a requested exemption.
- Safety measures should be consistent with the DID philosophy.
- Safety measures should help maintain sufficient safety margins.
- If there is some increase in risk despite the implementation of safety measures, such increase should be small and consistent with the intent of the regulatory policy statement on safety goals for the operations of nuclear power plants.
- The impact of safety measures should be monitored using performance measurement strategies, wherever possible and relevant.

It is emphasized that the SEP is not a linear process. In particular, the definition of the change can be modified as the analysis progresses, for example, when more is known about the risk contributors or when more is learned about how the various key principles (success factors) are affected.

The generalized SEP is identified using figures describing the connection between requirements, safety analyses and plant design. The details about the flow of information within the PSA study are described. See appendix C for all details.

4.2 Loss of Ultimate Heat Sink (LUHS)

The Loss of Ultimate Heat Sink (LUHS) case study group includes four case studies.

- Loss of Ultimate Heat Sink (Frazil Ice or Oil Spill)
- Loss of the Service Water System due to Extremely Low Temperature
- Blockage of (Water) Intake Building
- Evaluation of Plant Vulnerabilities to Riverine Events

The complete comparison is presented in Appendix D.

4.2.1 Fulfilment of BESEP Safety Requirements

The requirement topics that were evaluated by the LUHS group are Functional separation to provide defence against failure propagation, Assessment of potential losses of safety functions, Situation awareness and assessment, and Verification and validation (V&V) of design. For the first requirement topic the different approaches used in the cases were DSA failure analyses with input from PRA, finite elements calculation, verification of structural and functional independency through inclusion of results from more severe event and, verification of available plant equipment not affected by the course of event.

The LUHS group demonstrates verification of the second requirement topic, Assessment of potential losses of safety functions, using plant response analyses and safety margin analyses that have been conducted. Development of PRA with updated time windows were used to provide evidence on the potential loss of safety functions. Further modelling of the use of additional equipment has also been conducted.
For the verification of the third requirement topic, *Situation awareness and assessment*, the cases have demonstrated the use of full-scale simulator, 3D-models, and task analyses. Parameters relevant to assessing the state of the plant given the case specific course of events have been determined using information from DSA and the use of guidelines for the design of control rooms.

Fulfilment of *Verification and validation (V&V) of design*, the fourth requirement topic, is demonstrated by the use of DSA for the DBA (Design Basis Accident) events by the cases. For the DEC (Design Extension Condition) events PSA is used as evidence that the SSCs and human actions are working together as required. Tracing of decisions made based on V&V results are possible through the use of PSA in one of the cases. Procedures and guidelines are verified and validated through full-scale simulator, hands-on tests of equipment with evaluation of results and feed-back to improve the procedures. The test and training programs reinforce the validation and verification for the case studies by ensuring that the plant design is consistent.

### 4.2.2 Safety Margins Assessment

For the deterministic safety margin two of the cases in the group use the same definition for deterministic safety margin as Deliverable 2.3 for their specific DEC external events. One of the other cases use the results from plant response analysis in which they verify the availability and capacity of SSCs, including auxiliary safety systems. The last case verifies the functionality and independence of a safety system for a limited number of DEC external events using a realistic, best estimate, approach, as described in Appendix D.

Two of the cases use the same definition for probabilistic safety margin as defined in Deliverable 2.3. The other two cases use the same definition for level 1 PSA although one of the cases does not use parametric uncertainties even though the analysis was performed and the other defines the safety margin as the difference between the mean value and the upper bound uncertainty range. None of the other two cases use LERF, one of them use unacceptable release frequency and the other uses the result of hazard assessment, as described in Appendix D.

No safety margin for human actions can be found in three of the case studies. In the fourth the identification of three attributes of the safety margin for human actions was presented. The first attribute was the conditional success probability of automatic recovery from loss of Essential Service Water System (ESWS) if the off-site power is restored. The second attribute was the difference between the time window automatic interventions can prevent core damage if normal power supply is available and the mean time to recovery from loss of ESWS was considered as a relevant indicator of safety margins for human actions. The third attribute was the risk increase factor for all human actions beyond recovery from loss of ESWS was regarded as an additional attribute to safety margin, since it indicates core damage risk when all human actions fail and the role of human actions in such scenarios.

### 4.2.3 Interactions between DSA, PSA and HFE

All the separate cases emphasise the need for a clear structure and that would be beneficial to perform the different analyses simultaneously. Another common factor is that the PSA provides information to the deterministic plant response analysis which respectively feeds information back to the PSA. Also, identification of the possibilities and limitations of human actions is identified as important during the early stages of a modification process. The different analyses, DSA, PSA and HFE, should be performed simultaneously with extensive interaction.

### 4.2.4 Overall Safety Engineering Process

In the case studies the SEP approach is case-dependent with similarities that can be generalized as a three-level process (see, Appendix D for details). The first level is defined by the interactions between safety requirements, analyses and plant design where a design modification have been triggered by for example an updated requirement from an authority. The current plant design, including human actions, and safety analyses are evaluated to identify interactions with the design modification. The identified interactions constitute the basis for safety analyses that needs to be performed, revised, or complemented.
The second level consists of the work to create a plan for performing different analyses with unified input data, scheduling and organizing meetings for information exchange on both intermediate and final results. The integration of various types of analyses within DSA, PSA, and HFE are planned to support the requirement verification.

The third level is where the analyses are performed. This level includes work performed to assign proper resources to the different analyses. Graded approach should be applied to ensure that the work performed is effective considering level of detail necessary for the specific analysis.

### 4.2.5 Key Success Factors for an Efficient and Integrated SEP

Based on the comparison presented in Appendix D the following key success factors for an efficient and integrated SEP are defined for the LUHS group:

- the preferred main flow of information and actions: hazard analysis -> plant response analysis -> PSA model -> plant design
- the safety analyses and their interconnections should be defined,
- analyses should provide feedback to the design process and the modified design should be again analyzed,
- a safety graded approach should be applied by defining how deep the analysis should be and what analyses are the most important,
- evidence of the safety requirement fulfilment should be established via the pre-defined analyses and their interconnections.

### 4.3 Plant Vulnerability to Extreme Snow (PVES)

The PVES (Plant Vulnerability to Extreme Snow) case study group consists of three case studies:

- Snow and Wind Affecting Diesel Generators (PVES_1)
- Protection of the Reactor Hall from the Effects of Extreme Snow (PVES_2)
- Analysis of Extreme Snow Risk (PVES_3)

The complete cross-case comparison can be found in Appendix E and a short summary is provided in this section.

#### 4.3.1 Fulfilment of BESEP Safety Requirements

The responsible organizations of the PVES (Plant Vulnerability to Extreme Snow) case study group agreed on focusing the comparative assessment regarding the fulfilment of BESEP Safety Requirements to a limited number of requirements and not comparing all requirements within each assigned topic. Two out of the five topics addressed in the comparison are highlighted hereby.

The BESEP Safety Requirement related to the requirement topic Physical separation and structural integrity was fulfilled in a similar way in all the case studies by using structural strength analysis of buildings and/or fragility analyses in the verification process.

The BESEP Safety Requirement related to the requirement topic Guidance selection, decision making and intelligent use of guidance was also fulfilled in a similar way in all the case studies, procedures for snow removal were involved in the verification process.

#### 4.3.2 Safety Margins Assessment

**DSA safety margin**

The deterministic safety margin related to structural analysis, that is in the focus of the deterministic analyses in this case study group, is defined similarly and in mutual agreement within the different case studies. Although, the deterministic structural analyses were performed in a very similar manner, there are some slight
differences in the interpretation of the deterministic safety margins derived from the structural analyses. This may be due to small differences in national practices.

A widely accepted standard system (e.g. Eurocode) was applied during the structural re-analysis of the different safety buildings and systems in the case studies. In buildings and systems designed by applying such standards, a sufficiently high level of reliability (safety margin) is ensured by the use of partial factors. In this framework, it shall be justified that the design values of actions (loads) and the effects thereof, the material properties and the geometrical data are in the established limit states in any of the possible design situations.

The deterministic analyses in the case studies focus on the protection of safety related buildings and systems from structural integrity point of view, as this aspect is generally the most relevant concern when the protection against snow load is to be verified. Chapter 4.2 of Deliverable 2.3 deals mostly with physical phenomena and plant parameters to be assessed primarily by thermal-hydraulic and reactor physics calculations (see the listing at the end of the Chapter). These phenomena and parameters are not in the forefront of the case studies. The interpretation of the relevant safety margins as well as their assessments in the case studies is, however, in good agreement with the description in Chapter 4.1 of Deliverable 2.3. The load and strength density functions as well as their relative position are the basis of the applicable structural analysis standards.

**PSA safety margin**

All three case studies in the PVES case study group define probabilistic safety margins primarily according to the traditional interpretation, i.e. the calculated mean risk values are compared to pre-defined probabilistic safety criteria or targets. The core or fuel damage frequency was in the focus of each case study.

The interpretation of probabilistic safety margins given in the case study descriptions is in good agreement with the approach discussed in Chapter 4.3 of Deliverable 2.3. In general, the regulatory probabilistic safety criteria were compared to the calculated mean risk values, which is similar to the approach described in Deliverable 2.3. The only difference is that in Deliverable 2.3, the upper bound of the uncertainty range is applied instead of the mean value. The difference between the mean value and the upper bound of the uncertainty range is often significant. Therefore, this deviation in the definition of relevant measures can be regarded as substantial. It is noted that in the majority of national requirements and international recommendations, probabilistic risk criteria or targets are typically defined considering the mean values with additional requirements to assess the effects of uncertainties in the fulfillment of the safety goals. Therefore, a revision of the approach described in Deliverable 2.3 can be useful from this aspect. The development and publication of a refined definition of probabilistic safety margin is seen necessary in the next project phases.

**HFE safety margin**

There are no explicitly defined quantitative safety margins in place for human actions in the national practices of the countries the case studies are relevant to. Hence, the partners made an attempt to define safety margins for human actions in their case studies themselves, which led to quite different approaches.

Both in the case studies within the PVES group and in Deliverable 2.3, the focus is on the reliability of human actions rather than HFE in its entirety. This is in agreement with Deliverable 2.3, referring to the possibility to define safety margins in connection to HRA. A precise definition of HFE safety margin and an applicable, well-founded analysis method thereof have not been developed yet, at least not in such level of detail as it is described above for deterministic and probabilistic safety margins. It should also be noted that the human actions (or HRA) are strongly connected to the PSA study and the concept of safety margins within the PSA as described above.

4.3.3 Interactions between DSA, PSA and HFE

The initial DSA needs no input from PSA or HFE other than the specification of the design basis loads. However, PSA and HFE should utilize the results of DSA as input. Consequently, it is seen appropriate to perform structural strength analysis and other types of DSA (e.g. selection of safety related SSCs, evaluation of the consequences of a roof collapse) in the first place, presumably without a need to use support from the other two disciplines. Details about the interactions between the analyses can be found in the graphical representation of the SEP in Appendix E.
The results of DSA were used in HFE and PSA in all the case studies to the extent it seemed practicable and feasible. These interactions can also be regarded as appropriate in the case studies; however, they could have been more intense and frequent. The operating procedures that control snow removal had been elaborated earlier than the snow PSAs were completed. The available information from HFE was considered in the PSAs.

A conclusion from the comparison is that it is seen advantageous and advisable to utilize PSA and PSA insights as an integral part of developing operating procedures for coping with external events, rather than making use of risk insights in a follow-on manner, i.e. mostly for the purposes of reviews. In summary, PSA and HFE should be performed simultaneously, interacting actively so that PSA insights can be used effectively to underpin HFE. Moreover, more dynamic and frequent interactions between the different types of safety analyses can be beneficial for improving the efficiency of the SEP.

4.3.4 Overall Safety Engineering Process

All the case studies focus on the description and evaluation on the interactions between and within the main tasks and steps of the major types of analyses and disciplines (i.e. DSA, PSA and HFE), that belongs to the 2nd and 3rd level of the SEP. Level 1 of the SEP, i.e. the interactions between requirements, analyses and plant design, is described similarly and on a very high level in each case study.

It can be concluded that the SEP, in all case studies, was initiated by some high-level safety requirements as well as the conclusions of periodic safety reviews or stress-tests.

4.3.5 Key Success Factors for an Efficient and Integrated SEP

The identified success factors for the SEP are the development of a safety analysis master plan and nomination of a multidisciplinary expert. During the justification of fulfilling some complex requirements related to multiple disciplines, a safety analysis master plan (including the methodology, criteria and schedule) should be developed. The master plan should identify and integrate the various types of analysis necessary for verification of safety requirements. Of particular importance is planning of the interconnections between the different types of analyses and analysis steps including the definition of milestones, application of unified input data, scheduling meetings to be organized to inform each other on intermediate or final results of a specific analysis.

The generalized SEP is identified as both a description of flow and activities within all parts of the SEP (Safety Requirements, Safety Analysis and Plant Design) and as a description of classical V-model involving both SEP and the engineering process.

4.4 External Impact on Safety Classified I&C Systems (EIIC)

The EIIC case study group consists of two case studies:

- Loss of I&C due to High Ambient Temperature (EIIC_1)
- Loss of on-site Power Supply and Control due to Lightning (EIIC_3)

The complete cross-case comparison can be found in Appendix F and a short summary is given in this section.

4.4.1 Fulfilment of BESEP Safety Requirements

The responsible organizations of the EIIC (External Impact on Safety Classified I&C Systems) case study group agreed on focusing the comparative assessment regarding the fulfilment of BESEP safety requirements on the ones that were shared between both case studies.

The two cases used different approaches to the safety requirement verification, where case EIIC_1 in general uses a Claim-Argument-Evidence approach. The requirement BESEP_DSA_DCCF_002 (Diversity shall be applied within and between defence-in-depth levels so that a common-cause failure of any individual component type shall not prevent managing the initiating event), were verified differently, EIIC_1 concentrated on the margins of the I&C components, while EIIC_3 concentrated on the impact of a common
cause failure. For both cases it was found that improved data quality was needed, as well as improved methodologies for evaluating CCF of software. Also, verification of the requirement with regard to manual actions was missing in both cases.

The verification of BESEP_PSA_EIF_003 (The results from long-term monitoring of the NPP site and the surroundings shall be taken into account in the initiating event frequency estimation for external hazards) was similar and found to be rather straightforward by use of validated data and statistical tools. However, better interaction and sharing of data and results between PSA, DSA and HFE were identified as an area need for improvement in order to give better insights into the sensitivity of variation of weather parameter on the margins of each domain.

One case-study verifies the requirement BESEP_HFE_HSI_001 (The HSI shall be adapted to human capabilities and limitations and it shall prevent the risk of incorrect action as much as possible), mainly based on the evaluation made by HF experts to avoid explicit and detailed HFE requirements, it evaluates how well or poorly the potential challenge is managed. This approach differs from the second case-study where a requirement-based human factors evaluation is applied enabling the acceptance or rejection of the system, which exposes the arguments and evidence for safety and hence provides a robust verification.

The final requirement to be evaluated within the EIIC group is BESEP_SEP_MST_002 (The results gained with modelling and simulation analysis tools shall be collected to enable comparison to previous and following results gained with comparable models and tools). Both cases approach the verification of the results by judging the trustworthiness of the tools, not specifically comparing the results which is seen as a possible improvement.

4.4.2 Safety Margins Assessment

**DSA safety margin**

The definition as stated in Deliverable 2.3 of the deterministic safety margin was adopted for case-study EIIC_1 where the main focus is on the allowable temperature for the I&C components. The second case has focused on the lightning strike frequency, its effects and component reliability estimates and uncertainties. The main deterministic safety margins were in both of the case studies found to be in line with Deliverable 2.3. It could be argued whether the component reliability estimates should be considered in deterministic or probabilistic safety margins but in this comparison they were not categorised, since it was found that these estimates are used by both.

More data and better implementation of the results from the over-voltage simulation in the reliability estimates, and a comprehensive PSA model to guide where the reliability estimations have the most impact, would improve the process.

**PSA safety margin**

The probabilistic safety margins listed in Deliverable 2.3 have been acknowledged, but not applied in the case studies, since none of the cases have access to a PSA model. Both cases concentrate on the evaluation of the initiating event frequency (the requirement to be verified in this group: BESEP_PSA_EIF_003), or its progression to a certain plant state, which has been different from CDF or LERF.

**HFE safety margin**

Both cases have defined safety margins for human actions by the use of human performance analysis, through different approaches, but as stated in Deliverable 2.3, the safety margins are not defined by numerical values as for PSA (CDF, LERF) or DSA (fuel temperature, etc). Instead, qualitative methods and reasoning is used to assess how well the system copes in certain situations. A possible improvement could be a triangulation approach in which multiple qualitative methods and data sources are used to provide cumulative evidence of the acceptability of the requirements.
4.4.3 Interactions between DSA, PSA and HFE

Interconnections between safety analyses were relatively straightforward and limited in the studied cases. This was mainly due to the boundary conditions and hypotheses formulated for the accident scenarios and the related analyses. Interconnections and flow of information are beneficial as long as they support the main goal of verifying the safety requirements without bringing in unnecessary complexity. Graded approach can be used to limit this complexity. It is therefore beneficial to identify the role and significance of each safety analysis within the case under study.

Specific difficulties that need particular interest, which may need to be addressed by the help of other disciplines are nowadays treated in more multi-disciplinary way. It seems efficient to keep the interactions simple (also for in-depth analyses) and concentrate only on specific multi-disciplinary topics if necessary.

The case studies were found to have the following similarities in interactions:

- Accident progression or the definition of the scenarios to simulate by DSA are derived from PSA
- Mainly the results from DSA are fed to the PSA
- HFE communicates results to DSA and PSA, but is less connected to them and is more at the end of the total analysis.

Both case studies treat the usability of the system from a human factor point of view (workload, situation awareness, physiological capabilities, etc.). When regarding the connection between the disciplines, DSA and PSA provide inputs to HFE, but less information goes the other way around. HFE seems to be capable of dealing with the data coming from DSA/PSA. No distinction between DBA and DEC is made for the information exchange between HFE/DSA/PSA.

It was found important to identify the role and significance of each safety analysis to help recognise their interconnections and how they support each other. The safety analyses show that the requirements are met for each discipline and that their methods / tools are well defined, as well as their role and responsibilities. Nevertheless, while continuous improvements are made to the internal methods and tools, studies on the optimization of efficient information exchange should be looked at.

4.4.4 Overall Safety Engineering Process

Since neither of the cases in this group specifically describe or evaluate an existing plant, case study or Safety Engineering Process (SEP), the SEP described should be considered as prospective or appropriate.

The SEP of the first case focuses on fulfilling the topical requirements with a higher-level Claim-Argument-Evidence (CAE) approach and showing how the topical requirements are in each case broken down into claims and sub claims, and how the possible evidence could be produced with exemplary analyses to support the reasoning (arguments). The focus is placed on proof of concept and not on a complete in-depth implementation with all the details or materials, etc. The method has been mostly applied to the two upper SEP levels, but it is said to be sufficiently generic that it can be used at all levels (like matryoshka dolls). However, it doesn't introduce or specifically explain any designated steps or workflow or V-model for the use of method in any SEP level. The strength of CAE approach to SEP is that complex chains of reasoning are made explicit, it is inspired by mathematical demonstrations, where a theorem (claim) is progressively broken down into lemmas (sub claims). And where each reasoning step is explicit so that it can be understood, verified and if necessary, challenged.

In the second case, the focus on SEP is more about describing the process on all three levels, giving high-level steps, flow of information and specific analyses needed for the assessment of the related safety margins and the requirements topics. The SEP approach helps to show that safety analyses focus on the essential part of plant design and important safety system relevant to the accident scenario. The initiating event has been identified and the accident sequence has been clearly specified. The technical disciplines relevant to the case study and the hazard have been identified from the overall Safety Engineering Process presented in the V-model. Safety analyses and their outcomes were identified in the SEP, which helps to produce the needed evidence for the requirement verification.
In both cases, a more detailed information on system and component level analyses would improve SEP description and would make it more accurate.

4.4.5 Key Success Factors for an Efficient and Integrated SEP

With closer interconnection of requirements, arguments, and evidence, it is easier to identify possible shortcomings. The three level SEP representation gives good insight to the failure analyses and their objective in the overall picture. The identified shortcomings can be removed by performing additional or more detailed failure analysis. A combination of the SEP approaches of the two case studies can help reach common understanding for the safety justifications and the application of graded approach for failure analysis more efficiently. Hence the suggested generalised SEP of EIIC group is a merger of two SEP methods applied in the case studies. The main structure of the generalised SEP is built on the three level approach that can be found in the project proposal and which is applied by the second case study. It is reinforced with the CAE approach from the first case study., see Figure 9.

![Figure 9: Overview of the generalised SEP from case study group EIIC.](image_url)
5 Conclusions of the cross-case comparison

The cross-case comparison has been performed within the four case study groups based on a template that gives guidance on the required contents and format of the comparison. Prior to the cross-case comparison the self-evaluations were to be complemented with a verification of all assigned BESEP requirement topics for each group and a more detailed description of the Safety Engineering Process.

The following are the key success factors for an efficient and integrated SEP identified by the four groups during the cross-case comparison:

**Structural Integrity (STIN):**

- Safety measures should help ensure the fulfilment of current safety regulations unless they are explicitly related to a requested exemption.
- Safety measures should be consistent with the DID philosophy.
- Safety measures should help maintain sufficient safety margins.
- If there is some increase in risk despite the implementation of safety measures, such increase should be small and consistent with the intent of the regulatory policy statement on safety goals for the operations of nuclear power plants.
- The impact of safety measures should be monitored using performance measurement strategies, wherever possible and relevant.

**Loss of Ultimate Heat Sink (LUHS):**

- The preferred main flow of information and actions: hazard analysis -> plant response analysis -> PSA model -> plant design.
- The safety analyses and their interconnections should be defined.
- Analyses should provide feedback to the design process and the modified design should be again analyzed.
- A safety graded approach should be applied by defining how deep the analysis should be and what analyses are the most important.
- Evidence of the safety requirement fulfilment should be established via the pre-defined analyses and their interconnections.

**Plant Vulnerability to Extreme Snow (PVES):**

- A safety analysis master plan should be developed
- A multidisciplinary expert should be nominated.
- Planning of the interconnections between the different types of analyses and analysis steps should including the definition of milestones, application of unified input data, scheduling meetings to be organized to inform each other on intermediate or final results of a certain type of analysis.

**External Impact on Safety Classified I&C Systems (EIIC):**

- The application of a Claim, Argument and Evidence approach (CAE), makes it easier to identify possible shortcomings in requirement verifications.
- The three level SEP representation gives good insight to the failure analysis and their objective in the overall picture. The identified shortcomings can be removed by performing additional or more detailed failure analysis.
- A combination of the SEP approaches of the two case studies can help reach common understanding for the safety justifications and the application of a graded approach for failure analysis more efficiently, i.e., the three-level approach from the second case study is reinforced with the CAE approach from the first case study.
REFERENCES


[2] BESEP Deliverable 2.1: Results on the assignment of safety requirement topics, RELKO spol. s r.o. Bratislava, 2021


APPENDIX A: INSTRUCTIONS FOR UPDATING SELF-EVALUATIONS OF THE CASE STUDIES

During the project meeting in Stockholm on the 14th to 16th of June, it was decided that the self-evaluations were to be up-dated to enable the cross-case comparison to be performed in T3.4. The up-dated self-evaluations are to be uploaded to the Teams area in the folder for T3.4, Updated self-evaluations, no later than 23rd of August.

The following is to be updated:

1. All requirement topics assigned to the case study group should be addressed in the self-evaluation (See table below). All requirements within each topic shall be addressed unless it has been specifically decided within the case study group that some requirement(s) shall be left out.

<table>
<thead>
<tr>
<th>Discipline</th>
<th>BESEP Safety Requirement Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>STIN – Structural Integrity</td>
<td></td>
</tr>
<tr>
<td>DSA</td>
<td>Physical separation and structural integrity</td>
</tr>
<tr>
<td>PSA</td>
<td>Confidence provision for defence against the occurrence of cliff-edge effects</td>
</tr>
<tr>
<td>HFE</td>
<td>Workload, stress and fatigue management</td>
</tr>
<tr>
<td>SEP</td>
<td>Flow of information between safety analyses</td>
</tr>
<tr>
<td>LUHS – Loss of Ultimate Heat Sink</td>
<td></td>
</tr>
<tr>
<td>DSA</td>
<td>Functional separation to provide defence against failure propagation</td>
</tr>
<tr>
<td>PSA</td>
<td>Assessment of potential losses of safety functions</td>
</tr>
<tr>
<td>HFE</td>
<td>Situation awareness and assessment</td>
</tr>
<tr>
<td>SEP</td>
<td>Verification and validation (V&amp;V) of design</td>
</tr>
<tr>
<td>PVES – Plant Vulnerability to Extreme Snow</td>
<td></td>
</tr>
<tr>
<td>DSA</td>
<td>Justification of the engineering assumptions used in analysis</td>
</tr>
<tr>
<td>PSA</td>
<td>Support for developing abnormal and emergency operating procedures and severe accident guidelines</td>
</tr>
<tr>
<td>HFE</td>
<td>Guidance selection, decision making and intelligent use of guidance</td>
</tr>
<tr>
<td>SEP</td>
<td>Safety design and requirement management for external hazards</td>
</tr>
<tr>
<td>EIIC – External Impact on Safety Classified I&amp;C Systems</td>
<td></td>
</tr>
<tr>
<td>DSA</td>
<td>Diversity and common-cause failure criteria</td>
</tr>
<tr>
<td>PSA</td>
<td>Initiating event frequency estimation</td>
</tr>
<tr>
<td>HFE</td>
<td>Applicable HSI (Human System Interface)</td>
</tr>
<tr>
<td>SEP</td>
<td>Validated modelling and simulation analysis tools</td>
</tr>
</tbody>
</table>

2. If decided within the case study group, evaluate additional requirement topics and requirements as agreed upon.

3. Perform a quality check of the self-evaluation to improve the general quality. I.E. check that the template for the self-evaluation is followed and that all questions therein are clearly answered in the self-evaluation.

4. If needed update the case study descriptions based on the update of the self-evaluations and upload the updated case study description to the Teams Task 3.4 area, Updated detailed case study descriptions.
5. Make a graphical representation of the SEP with a description of the relations (arrows) and steps (boxes). See example below for inspiration.

It was also discussed during the project meeting to view the SEP in three different levels:
- Level 1: Relations between Safety requirements- Safety analysis- Plan design
- Level 2: Interconnection between DSA-PSA-HFE(HRA)
- Level 3: Relations within the analysis, e.g. PSA

Example of graphical representation of the SEP

In the figure below the safety engineering process for the case study PVES_1 is shown through a graphical representation. It should be noted that the SEP for PVES_1 has iterative steps which are not completely shown in the graphical representation. This should be seen as an example which is under development.

On an overview level the green boxes represent requirement related steps in the process, the different blue boxes represent safety analyses related steps and the purple represent plant design steps. Step 1-3 describes the SEP in a level 1 perspective connecting safety requirement, safety analyses and plant design (step 10-12 is a side process for beyond design base external events and the construction of the independent core cooling system (ICCS)). Step 2 contains all relations and interconnections between the safety analyses and is a combined description of SEP level 2-3.
SEP Level 1:

**Step 1 a:** Issuing or new requirements from the authority which clearly states that all possible external events should be considered and analysed. *Flow A* gives the input to **Step 6a** in the safety analyses that all external events including extreme snow are to be analysed.

**Step 1 b:** The Fukushima event led to requirements on performing the ENSREG stress test to analyse the plant design for design base and beyond design base external events. *Flow B* is the requirement on how to perform the stress test which is used in the analysis in **Step 8**.

**Step 2:** This step contains all the safety analysis which have been performed. The Step is described in more detail in the SEP level 2-3 description below. *Flow C* is information on the structural deficiencies of the emergency diesel generator building (EDG building) as input for the re-construction of the roof in **Step 3**.

**Step 3:** Represent the process step were the roof of the EDG-building is re-constructed (design and construction work) in order to withstand the load from external events (i.e. extreme snow). The design of the reconstructed roof is then feed back to the safety analyses in **Step 4b** through *Flow P*.

SEP Level 2-3:

Here the details of Step 2 are described to highlight the interconnections and interactions of the safety analyses within the SEP.

**Step 4a – Step 9:** *To be described*

**Step 10-12:** *To be described*
## APPENDIX B: TEMPLATE FOR CROSS-CASE COMPARISON

### B.1 General information

**Responsible Organization(s):** List all organizations involved in the cross-case comparison. The responsible organization should be listed first in bold letters.

The following organizations are responsible within each case study group:
STIN: RELKO, LUHS: FORTUM, PVES: NUBIKI, EIIC: VTT

**Case Study Group Identifier:** Use the identifier for the case study group (i.e. STIN, LUHS, PVES or EIIC)

**Date:** Date when the cross-case comparison has been finalized.

**Case Study Titles:** List the title of each case study involved in the cross-case comparison

### B.2 Fulfilment of BESEP Safety Requirements

The verification of the fulfilment of BESEP requirements should be compared. The comparison should consider the following issues:

- Key features of the verification process: Characterize the key features of verification process for each case study, based on the information provided by the information in the self-evaluation sheets.
- The adequacy of verification process: Compare how the verification and justification of the requirements were made, why a certain type of safety analysis is applied for a specific requirement and how the result of that analysis ensures compliance with the requirement. Identify strengths of the chosen approaches and also identify possible alternative approaches that could be beneficial to apply.
- Improvement of the verification process: Identify good practice for the requirement verification, both based on identified improvements in the self-evaluations and on findings and conclusions made in the previous steps of the cross-case comparison. If possible, define an ideal verification process which can be used for the group in the generalised case study to be developed in T3.5.

All BESEP requirement topics assigned to the case study group and all BESEP requirements within each topic (unless otherwise decided within the case study group) should be addressed.

The answers to above topics should be elaborated in free text format by each group, comparing the self-evaluations of the case studies included in each group. The most important information should then be extracted into a table as shown below. Fill in the Case Study Group Identifier in the first row (**XXXX_1**), then complete the table for all Case Studies within the group. Main conclusions should also be presented in the table.

<table>
<thead>
<tr>
<th>BESEP requirement topic: Add the requirement topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>BESEP requirement ID: Add the requirement ID</td>
</tr>
<tr>
<td>Key features of the verification process</td>
</tr>
<tr>
<td>Adequacy of Verification</td>
</tr>
<tr>
<td>Proposals for Improvement</td>
</tr>
</tbody>
</table>

### Table 1. Fulfilment of BESEP Safety Requirements

<table>
<thead>
<tr>
<th>BESEP requirement topic: Add the requirement topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>BESEP requirement ID: Add the requirement ID</td>
</tr>
<tr>
<td>Key features of the verification process</td>
</tr>
<tr>
<td>Adequacy of Verification</td>
</tr>
<tr>
<td>Proposals for Improvement</td>
</tr>
</tbody>
</table>
APPENDIX B

BESEP requirement ID: Add the requirement ID

Key features of the verification process

Adequacy of Verification

Proposals for Improvement

As a reminder, the assignment of safety requirement topics to the different case study groups is as follows:

STIN – Structural Integrity

**DSA**  \[\text{Physical separation and structural integrity}\]
**PSA**  
Confidence provision for defence against the occurrence of cliff-edge effects
**HFE**  
Workload, stress and fatigue management
**SEP**  
Flow of information between safety analyses

**LUHS** – Loss of Ultimate Heat Sink

**DSA**  
Functional separation to provide defence against failure propagation

**PSA**  \[\text{Assessment of potential losses of safety functions}\]
**HFE**  
Situation awareness and assessment
**SEP**  
Verification and validation (V&V) of design

PVES – Plant Vulnerability to Extreme Snow

**DSA**  
Justification of the engineering assumptions used in analysis

**PSA**  
Support for developing abnormal and emergency operating procedures and severe accident guidelines

**HFE**  
Guidance selection, decision making and intelligent use of guidance

**SEP**  \[\text{Safety design and requirement management for external hazards}\]

EIIIC – External Impact on Safety Classified I&C Systems

**DSA**  \[\text{Diversity and common-cause failure criteria}\]

**PSA**  
Initiating event frequency estimation

**HFE**  
Applicable HSI (Human System Interface)

**SEP**  
Validated modelling and simulation analysis tools

B.3 Safety Margins Assessment

A comparison of the different Safety Margins addressed in the case studies belonging to the given case study group should be performed. The comparison should consider the following issues:

- **Definition:** Compare the definition of the Safety Margins used in PSA, DSA and HFE. Compare the interpretation of the safety margins in the different case studies with the definitions in D2.3.
  - If different Safety Margins compared to D2.3 have been used, give an explanation,
  - Try to explain why different approaches have been used to Safety Margins in the different case studies. Is it due to different national requirements, different real margins present in the safety analyses, or due to other reasons?
- **Assessment & evaluation:** Compare the different methods used to assess Safety Margins. Identify strengths of chosen approaches and also identify possible alternative approaches that could be beneficial in pursuit of an improved assessment.
- **Improvements:** Identify good practices for definition, analysis, and assessment of Safety Margins, both based on identified improvements in the self-evaluations and on findings and conclusions made in previous step of the cross-case comparison. If possible, define ideal Safety Margins to be used for the group in the generalised case study to be developed in T3.5

The plant is constructed and operated in accordance with its licensing basis, and the design includes appropriate Safety Margins and is consistent with the Defence-In-Depth philosophy. Depending on the case studies included in the different groups it may be relevant to address how the DID is affected when discussing the above bullet (Impacts on redundancy/diversity, introduction of new CCF mechanism, introduction of new HFE or human performance factors degraded, impacts on clad vessel, RCS or containment integrity).
The answers to above topics should be elaborated in free text format by each group, comparing the self-evaluations of the case studies included in each group. The most important information should then be extracted into a table as shown below. Fill in the Case Study Group Identifier in the first row (XXXX_1), then complete the table for all Case Studies within the group. Main conclusions should also be presented in the table.

Table 2. Assessment of Safety Margins:

<table>
<thead>
<tr>
<th></th>
<th>XXXX_1</th>
<th>XXXX_2</th>
<th>XXXX_3</th>
<th>XXXX_4</th>
<th>Conclusions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Deterministic Safety Margins</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Definition</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assessment &amp; Evaluation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Comparison with D2.3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Proposals for Improvement</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Probabilistic Safety Margins</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Definition</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assessment &amp; Evaluation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Comparison with D2.3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Proposals for Improvement</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Safety Margins for Human Actions</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Definition</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assessment &amp; Evaluation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Comparison with D2.3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Proposals for Improvement</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

B.4 Interactions between DSA, PSA and HFE

A comparison of the interconnections and flow of information between the safety analyses (DSA, PSA and HFE) should be performed. This is level 2 of the SEP as described in the next section of the template. The most important tasks to be completed are the followings:

- Compare and describe the interconnections and exchange of information between PSA and DSA. Identify and describe commonalities and differences of the information interconnection between the case studies. Identify if the interconnections are formalised or if they are situation-based.
- Compare how the HFE is connected to safety analyses methods DSA/PSA. Is the basis of the connection only HRA-activities or are there any other relevant areas of connection?
• Compare how the interactions have been made for analyses of DBA and for the analyses of DEC respectively. Describe commonalities and differences on how the interconnections and flow of information have been ensured for DBA and DEC external events.
• Identify strengths of different ways of interconnecting the safety analyses and also identify possible alternative interconnections and information exchange that could be beneficial to apply.
• Identify good practice of interconnections and flow of information between DSA, PSA and HFE which can be used in the generalised case study to be developed in T3.5.

The answers to above topics should be elaborated in free text format by each group, comparing the self-evaluations of the case studies included in each group. The most important information should then be extracted into a table as shown below. Fill in the Case Study Group Identifier in the first row (XXXX_1), then complete the table for all Case Studies within the group. Main conclusions should also be presented in the table.

Table 3. Interactions between DSA, PSA and HFE:

<table>
<thead>
<tr>
<th>Evaluation of Adequacy</th>
<th>Proposals for Improvement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interactions between DSA, PSA and HFE</td>
<td>XXXX_1</td>
</tr>
<tr>
<td>Evaluation of Adequacy</td>
<td>XXXX_1</td>
</tr>
<tr>
<td>Proposals for Improvement</td>
<td>XXXX_1</td>
</tr>
</tbody>
</table>

B.5 Overall Safety Engineering Process

A comparison of the overall Safety Engineering Process applied in the Case Studies on a general level should be performed. The SEP can be described in three different levels, level 1 – interactions between requirements, analyses and plant design, level 2 – interactions between safety analyses and level 3 interactions within the different safety analyses. All three levels should be addressed in the comparison. The most important tasks of the comparison are the followings:

• Compare the overall SEP approaches and its steps between the case studies. How different are the approaches and which steps are common and which steps are unique? Explain the underlying causes of the differences, if feasible.
• Compare the flow of information in the SEPs of the case studies. Which flow patterns (interrelationships) are common and which are unique? Explain the underlying causes of the differences, if feasible.
• Reveal and evaluate strengths and weaknesses, and challenges and successes of the different SEP approaches. Provide justifications for the use of the chosen approach. Incorporate findings and conclusions based on the “Further Lessons Learned” section in the self-evaluation sheets.

The answers to above topics should be elaborated in free text format by each group, comparing the self-evaluations of the case studies included in each group. The most important information should then be extracted into a table as shown below. Fill in the Case Study Group Identifier in the first row (XXXX_1), then complete the table for all Case Studies within the group. Main conclusions should also be presented in the table.
Table 4. Characterization of the Overall Safety Engineering Process:

<table>
<thead>
<tr>
<th>Overall approach and steps of the SEP</th>
<th>Interrelationship among the Steps</th>
<th>Strength of the SEP</th>
<th>Weaknesses of the SEP</th>
<th>Proposals for Improvement</th>
</tr>
</thead>
<tbody>
<tr>
<td>XXXX_1</td>
<td>XXXX_2</td>
<td>XXXX_3</td>
<td>XXXX_4</td>
<td>Conclusions</td>
</tr>
</tbody>
</table>

B.6 Key success factors for an efficient and integrated SEP

Based on the above comparison of the case studies, the key success factors for an efficient and integrated SEP should be described and elaborated. The focus should be on the interactions and connections between the safety analyses.

Based on the key success factors and good practice, a generalised SEP should be elaborated which can be used in T3.5. The generalised SEP should be identified and described using a graphical representation together with description of the different steps and flows of the SEP.
APPENDIX C: CROSS-CASE COMPARISON IN CASE STUDY GROUP STIN

C.1 General information

Responsible Organization(s): RELKO, UJV, VTT

Case Study Group Identifier: STIN

Date: 23/9/2022

Case Study Titles:
- Collapse of Venting Stack due to High Wind (STIN_1)
- Probabilistic Analysis of Aircraft Crash Risk for Dukovany NPP (STIN_2)
- Loss of Heat Removal of Spent Fuel Pool due to External Impact (STIN_3)

C.2 Fulfilment of BESEP Safety Requirements

The fulfilment of the following BESEP safety requirements was addressed in every case study:

Physical separation and structural integrity (DSA):

BESEP_DSA_PSEP_001: Redundant safety systems that have a role in mitigating the effects of external hazards shall be located so that these effects cannot hinder the performance of safety functions of all redundant components simultaneously.

BESEP_DSA_PSEP_002: The systems, structures and components, including auxiliary or supporting systems thereof shall be protected from the effects of external hazards as far as reasonably practicable.

Confidence provision for defence against the occurrence of cliff-edge effects (PSA):

BESEP_PSA_CEE_001: Probabilistic safety analyses shall be used to demonstrate that sufficient safety margins are available to avoid cliff-edge effects.

BESEP_PSA_CEE_002: Probabilistic safety analyses shall be used to identify potential areas of improvement in the design to ensure the avoidance of the cliff edge effects.

Workload, stress and fatigue management (HFE):

BESEP_HFE_SM_001: To reduce the stress simulator-based training of stressful events shall be arranged.

BESEP_HFE_SM_002: Training that improves control room personnel communications skills shall be applied to reduce the likelihood that communications will fail under stress.

BESEP_HFE_SM_003: The procedures designed for abnormal and emergency conditions, power plant outages and start-up activities shall support operator work by reducing memory load and need for complex decision making.

Flow of information between safety analyses (SEP):

BESEP_SEP_FISA_001: When several different types of safety analyses are used to provide evidence, the information flow between safety analyses shall be defined.

BESEP_SEP_FISA_002: The flow of information shall support reaching the comprehensive understanding on the issue analysed.

In the next part of the report comparison is performed for the above described BESEP requirements in the case studies.
Requirement No. 1. - BESEP_DSA_PSEP_001: Redundant safety systems that have a role in mitigating the effects of external hazards shall be located so that these effects cannot hinder the performance of safety functions of all redundant components simultaneously.

Summary of the Verification Process

In the first case study, collapse of the venting stack, in case of beyond design-bases wind speeds, may damage the safety-related buildings. The finite elements calculation models were used in ANSYS code to calculate the wind capacity for structural elements. The HCLPF value was calculated to determine their wind capacity.

In the second case study, systematic DSA were performed for all basic safety functions to verify the systems performing a safety function against external hazard (aircraft crash). The analysis broadly used the results of similar analyses carried out for the internal events scenarios.

The third case study is focused on the impact analyses. The impact design load was assessed in different locations of the NPP (layout design) and the effects of induced vibrations on the structural integrity and component fragility were analysed. The following analyses were performed: impact analysis, structural integrity analysis of the fuel pool and capacity check of the residual heat removal (RHR) system components.

Adequacy of Verification

The verification is adequate in the first case study. It was shown that the safety functions cannot be performed, and integrity of all three barriers (fuel clad, RCS and containment) can be lost. Therefore, safety measures must be implemented.

In the second case study the verification of fulfilment of this requirement used broad scope of information from internal events safety analysis. The adequacy of the approach used within the internal events was verified by several reviews and this approach is seen as adequate also for the aircraft crash analysis.

The third case study concluded that the verification is adequate. It is argued that seismic fragility curves can also be used for impact events. Application of the MELCOR code has been verified and validated.

Proposal for Improvement

The conclusion is that no improvement of the verification process is needed in the first case study. In the second case study no direct improvement related to this requirement was proposed. The recommendation in the third case study is to extend the analysis to falling objects.

Requirement No. 2. - BESEP_DSA_PSEP_002: The systems, structures and components, including auxiliary or supporting systems thereof shall be protected from the effects of external hazards as far as reasonably practicable.

Summary of the Verification Process

One safety measure is proposed to be implemented in the first case study. Steel ropes installed on the venting stack to prevent falling of the stack on the safety related structures. This is the way to protect SSCs from high wind effects.

In the second study a very detailed analysis of all aircraft routes with the potential to “touch” the plant in case of aircraft fall was performed. It was found out that the estimated aircraft crash frequencies, multiplied by the conditional probabilities that specific systems are hit, are below the value of 1.0E-7/y.

 Structural integrity and component fragility analyses of the RHR system were performed in the third case study. Structural integrity of the design and attachment of the components to the structures were verified. The isolation and dampers increase the resistance of the components against vibrations induced by the external event impact.
Adequacy of Verification

Angles of interactions in degrees between 0°–360° were calculated for mutual interactions of the buildings and venting stack in the first case study. This is an adequate mode to setup the steel ropes and protect the safety related buildings.

The second case study concluded that the verification is adequate. The case covered possible protection measures against aircraft crash of all categories of aircrafts operated in the Czech Republic. In general, the verification itself was simplified due to the fact that the level of risk related to this external hazard is relatively low and no specific protection measures were proposed.

The verification is quite adequate in the third study. The analyses are limited to fuel pool integrity and cooling. Extending the analyses to additional systems could increase the strength of the verification.

Proposal for Improvement

No improvement of the verification process is needed in the first case study.

In the second case study no direct proposal for improvement was made because of low frequency of accident scenarios generated by this external hazard. It was emphasized, however, that a systematic collection and analysis of data about flights and accidents must continue.

The third case study concluded that more detailed analyses are needed regarding the availability of additional water sources for the RHR system in accident situations.

Requirement No. 3. - BESEP_PSA_CEE_001: Probabilistic safety analyses shall be used to demonstrate that sufficient safety margins are available to avoid cliff-edge effects.

Summary of the Verification Process

PSA is used to show that sufficient SMs are available to prevent cliff-edge effects in the first case study. The calculated mean value of the core damage frequency is 2.23E-7/y. After implementation of safety measures the core damage frequency is reduced to 1.74E-7/y.

The second case study states that no specific probabilistic analysis to estimate the safety margin to cliff-edge effect occurrence has been performed specifically to air crash scenarios yet. However, adequacy of such safety margin, in respect to all external events in general, was considered proven.

In the third study sufficient SM is demonstrated using probabilistic safety analysis for different PGA input values and evaluating the seismic event induced fuel damage frequency.

Adequacy of Verification

The verification is adequate in the first case study. The PSA results have shown that the impact is nearly a practically eliminated event. The total CDF for a plant in operation (internal and external events) should be less than 1.0E-4/y according to the requirement of the regulatory authority. So, sufficient SM exists.

In the second case study, the verification is basically considered adequate for the present time. Nevertheless, future improvements are possible. Specific probabilistic demonstration of sufficient safety margin to avoid cliff-edge effects in the case of air-crash scenario is planned.

In the third case study the PSA model excludes loss of structural integrity of the spent fuel pool.

Proposal for Improvement

No improvement of the verification process is needed in the first study.

Although the level of risk related to aircraft crash accident scenarios was proven as low in the second case study, it might still be useful to search for possible cliff-edge effects connected with these scenarios and their risk impact.
The third case study concluded that the inclusion of the structural integrity of the pool to the evaluation process is needed. In addition, deterministic modelling should support the PSA activities.

**Requirement No. 4. - BESEP_PSA_CEE_002: Probabilistic safety analyses shall be used to identify potential areas of improvement in the design to ensure the avoidance of the cliff edge effects.**

**Summary of the Verification Process**

Using PSA, the possible mutual interactions of the safety related building and the venting stack were identified in the first case study. In case of collapse of the venting stack, the reactor building, longitudinal and transversal buildings, DG station and auxiliary building can be damaged. The proposed safety measures ensure prevention of the cliff edge effects.

The second case study states that no specific probabilistic safety analyses have been performed to demonstrate sufficient safety margin related to cliff-edge effects for the aircraft scenarios. Consequently, no such analyses were performed for identification of potential areas of improvement.

In the third case study the seismically qualified components from the seismic equipment list (SEL) are included in the PSA model, when the deviations of the fuel damage frequency for different ground accelerations are calculated.

**Adequacy of Verification**

Adequate PSA approach for external events is used in the first case study.

For the second case study, verification is irrelevant for this safety requirement.

SEL and the seismically qualified component groups provide strong evidence on the avoidance of cliff-edge effects in the third case study.

**Proposal for Improvement**

No improvement of the verification process is needed in the first study.

There is a statement in the second study that PSA is normally used for evaluation of suggested modifications and their alternatives. So, it can be suitable also for the modifications proposed with the aim to reduce the impact of cliff-edge effects after aircraft crash.

The third case study proposes an improvement that the PSA model could also be used in operator training to avoid cliff-edge effects.

**Requirement No. 5. - BESEP_HFE_SM_001: To reduce the stress simulator-based training of stressful events shall be arranged.**

**Summary of the Verification Process**

High wind affects adversely the environment in which the plant personnel must perform their actions. In the first case study, simulator-based trainings of stressful events are arranged to improve the performance of plant personnel in the stressful situations.

Simulator exercises of accident scenarios represent common part of control room crew training. According to the aircraft category and the places, plant is hit by it, the consequences can be either catastrophic or can belong to some initiating event already modelled in PSA. There are no training programs for the catastrophic events at Czech NPPs. Plant response to the initiating events modelled in PSA forms standard subject of simulator training for the control room operators. This is the summary from the second case study.

Regular refresher training including selected transients and accidents that are stressful and cognitively demanding is conducted in the third case study.
Adequacy of Verification

In the first case study, new operator actions are created within the external event PSA, some actions are eliminated from the internal event PSA, new dependencies are among operator actions. Adequate HRA approach for external events is used.

The scenarios of plant response to the initiating events possibly generated by aircraft crash are systematically identified and modelled in internal event PSA. On the other hand, one of the applications of the plant PSA is to support the definition of priorities in simulator training by selection and sorting the scenarios in accordance with their risk significance. This process was verified and found useful for fulfilling of the requirement. This is the conclusion of the second case study.

The third case study concludes adequate verification, although at present workload, stress and fatigue of control room operators are not evaluated.

Proposal for Improvement

No improvement of the verification process is needed in the first case study.

In the second case study, it is proposed to continue in selection of exercised scenarios by internal event PSA and to define priorities in training systematically in sophisticated manner, taking into account: 1) estimated frequency of occurrence of the scenario 2) estimated difficultness of the scenario for CR crew (given by human error probabilities of the actions, which are part of the scenario) 3) relative risk impact of the actions forming the human part of the scenario (given by importance measures of the actions which are modelled in PSA as a part of the scenario).

Operator stress, workload and fatigue should be measured both by subjective and objective measures. Online evaluation of stress by measurement of stress-related biosignals is especially valuable, although it has to be considered that the stress during training exercise may differ from the real danger stress during plant operation. This is the conclusion for improvement from the third case study.

Requirement No. 6. - BESEP_HFE_SM_002: Training that improves control room personnel communications skills shall be applied to reduce the likelihood that communications will fail under stress.

Summary of the Verification Process

The first case study concludes that the training improves personnel communications under stress due to high wind.

According to the second case study, training control room personnel communications skills is done by simulator exercises. The operators are obliged to use three-way communication and this way of communication is applied at each training. Also, the (more problematic) communication with rest of the plant personnel, outside the control room, is simulated during the training (by training supervisor) to strengthen the communication capabilities of the control room crew under the accident conditions.

The third case study emphasizes regular refresher training including collaboration within the shift team and between the control room operators and field workers.

Adequacy of Verification

Adequate HRA approach for external events is used in the first study where the training of the personnel is taken into consideration in adequate way, which is the state of the art in this area.

The second study statement is that it was verified that the plant response to the initiating events generated by external hazard “aircraft crash” is trained at full-scope simulator in a way leading to improvement of communication skills.

The third study has a statement about the sufficient adequacy of the verification process.
Proposal for Improvement

No improvement of the verification process is needed in case of the first study.

According to the second study the presented information is an example of good practice and does not need improvement.

According to the third study a more detailed measurement and analysis of communication is important in order to increase the quality of communication in high-stakes situations.

**Requirement No. 7. - BESEP_HFE_SM_003: The procedures designed for abnormal and emergency conditions, power plant outages and start-up activities shall support operator work by reducing memory load and need for complex decision making.**

Summary of the Verification Process

The statement from the first case study is that EOPs and SAMGs are available to reduce memory load of the personnel during high wind. In addition, procedures are available for external events including high wind.

Symptom based procedures are in use in response to initiating events, including those generated by aircraft crash. These procedures significantly reduce the long memory requirements because the required actions are linked with the symptoms, which the operators face at the given time directly in the control room. The need for complex decision making is similarly significantly reduced, as well. This is the summary of the second case study.

Validation of new or revised procedures is based on the Systems Usability Case approach in the third case study.

Adequacy of Verification

Adequate HRA approach for external events is used in the first study. This approach has taken into account the quality of procedures design what is the state of the art in this area.

The system of symptom-based procedures used at the plant was originated in late nineties and has been improved, extended and supplemented by additional means (very detailed explanation of each procedural step in the format of the textbook) since that time. The fulfilment of the requirement is considered verified adequately. This is the conclusion of the second study.

Procedure design is based on analytical and rigorous method, and verification and validation of procedures is based on a systematic and holistic case-based methodology in the third study.

Proposal for Improvement

No improvement of the verification process is needed in the first study.

The process of improvement of the symptom-based procedures has been running for a long time and will address possible changes at the plant design and operation in the future. There is no further proposal for improvement in the second study.

According to the third study more detailed methods for the analysis of operating procedures are needed.

**Requirement No. 8. - BESEP_SEP_FISA_001: When several different types of safety analyses are used to provide evidence, the information flow between safety analyses shall be defined.**

Summary of the Verification Process

DSA and HFE (HRA) provide inputs into the PSA model. The failure probabilities are calculated for SSCs based on these inputs. The DSA and HRA results are conservative values with significant impact on the PSA results. The information flow is exactly defined by the rules of PSA. This is the summary of the verification process from the first case study.
For the second study, both deterministic and probabilistic safety analyses are mostly organized and performed by the same division of the same company. Currently, in addition, all safety analyses (for both NPPs in Czech Republic) are performed within the same large project of engineering support of Czech NPPs conducted by the same TSO - UJV Rez. Hence, a sufficient level and completeness of the information transfer has been ensured for safety analyses. This is the summary of the second case study.

In the third case study defining the safety engineering process for the case and the links between the performed analyses can be identified and the flow of information is ensured.

**Adequacy of Verification**

Adequate DSA, HRA and PSA approaches for external events are used. The results interconnection is convenient to support the PSA activities. It represents the state of the art in this area.

According to the second case study it is concluded that during the verification of fulfilment of this requirement, the above-mentioned process of cooperation within a single TSO focused on deterministic and probabilistic analyses was checked in detail.

In the third study the safety engineering process is used to define the information flow between the analyses.

**Proposal for Improvement**

According to the first study no improvement of the verification process is needed.

There is no proposal for improvement in the second study.

Different information flow models could be integrated more closely, detailed specification of the safety engineering process should be performed as the first step of the analysis. This is the standpoint from the third study.

**Requirement No. 9. - BESEP_SEP_FISA_002: The flow of information shall support reaching the comprehensive understanding on the issue analysed**

**Summary of the Verification Process**

The flow of information supports the understanding of the safety related issues in the first case study.

The validity of the requirement was checked from both sides of the cooperation between DSA and PSA. A close cooperation brings better understanding of the thermohydraulic and other processes to the PSA experts. On the other hand, it brings better overall view of the risk potential at NPP for the specialists developing the individual deterministic analyses. This the summary of the second case study.

In the third case study the flow of information between central topics in the accident scenario (connections of DSA, PSA and HFE) has been roughly specified in the safety engineering process.

**Adequacy of Verification**

Adequate DSA, HRA and PSA approaches for external events are used in the first study. It means that the flow of information supports reaching the comprehensive understanding on issue analysed.

The verification process has proven sufficiently that this requirement was fulfilled in the second study.

Analysis is not necessarily comprehensive in means of analysis areas but it represents a form of adequate verification according to the third study.

**Proposal for Improvement**

No improvement of the verification process is needed in the first study.

In the field of aircraft crash safety analyses, there are still many assumptions related to plant vulnerability and plant response to the hazard. The best continuation of solving the matter is to discuss and possibly justify the
needs for additional DSA analyses, if some scenarios are found where the risk impact may not be negligible. This is the proposal of the second study.

Accommodating the pool leakage to the case study would make the interaction of the analyses more complicated and increase the value of the flow of information management. This is the conclusion from the third study.

Summary of the comparison process is provided in Table C.1.
**Table C.1: Fulfilment of BESEP Safety Requirements**

<table>
<thead>
<tr>
<th>STIN_1</th>
<th>STIN_2</th>
<th>STIN_3</th>
<th>Conclusions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>BESEP requirement topic:</strong> Requirements related to physical separation and structural integrity (DSA)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>BESEP requirement ID:</strong> BESEP_DSA_PSEP_001: Redundant safety systems that have a role in mitigating the effects of external hazards shall be located so that these effects cannot hinder the performance of safety functions of all redundant components simultaneously.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Key features of the verification process</td>
<td>DSA were performed for all basic safety functions. The analyses broadly used the results of similar analyses carried out for the internal events scenarios.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The finite elements calculation models were used in ANSYS code to calculate the wind capacity for structural elements. The HCLPF value is calculated to determine their wind capacity.</td>
<td>The following analyses were performed: impact analysis, structural integrity analysis of the fuel pool and capacity check of the residual heat removal (RHR) system components.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Adequacy of Verification</td>
<td>Adequate, it is argued that seismic fragility curves can also be used for impact events. Used MELCOR code has been verified and validated.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The verification is adequate. It is shown that the safety functions cannot be performed, integrity of all three barriers (fuel clad, RCS and containment) can be lost. Therefore, safety measures must be implemented.</td>
<td>Adequate methods were used to confirm the safety requirement.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Proposals for Improvement</td>
<td>No direct improvement related to this requirement was proposed.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>No improvement of the verification process is needed.</td>
<td>Extend the analysis to falling objects.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>BESEP requirement ID:</strong> BESEP_DSA_PSEP_002: The systems, structures and components, including auxiliary or supporting systems thereof shall be protected from the effects of external hazards as far as reasonably practicable.</td>
<td>No improvement is needed in the first and second case study to meet the requirement. The third study proposed to extend the analysis to falling objects.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Key features of the verification process

<table>
<thead>
<tr>
<th>STIN_1</th>
<th>STIN_2</th>
<th>STIN_3</th>
<th>Conclusions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Safety measures are proposed to be implemented to protect SSCs.</td>
<td>The estimated aircraft crash frequencies, multiplied by the conditional probabilities that specific systems are hit, are below the value of 1.0E-7/y (practically eliminated event).</td>
<td>Structural integrity and component fragility analyses of the RHR system; structural integrity design and attachment of components to the structures; isolation and dampers increase the resistance of the components against vibrations induced by the impact.</td>
<td>The aircraft crash in the second study is a practically eliminated event. In the other studies the safety impacts are identified and analysed.</td>
</tr>
</tbody>
</table>

### Adequacy of Verification

<table>
<thead>
<tr>
<th>STIN_1</th>
<th>STIN_2</th>
<th>STIN_3</th>
<th>Conclusions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adequate mode is presented for protection of the safety related buildings.</td>
<td>The verification is considered adequate. The verification itself was simplified due to the fact that the level of risk related to this external hazard is relatively low and no specific protection measures were proposed, in general.</td>
<td>Quite adequate, analysis limited to fuel pool integrity and cooling.</td>
<td>Adequate analyses were performed to confirm that the safety requirement is fulfilled.</td>
</tr>
</tbody>
</table>

### Proposals for Improvement

<table>
<thead>
<tr>
<th>STIN_1</th>
<th>STIN_2</th>
<th>STIN_3</th>
<th>Conclusions</th>
</tr>
</thead>
<tbody>
<tr>
<td>No improvement.</td>
<td>No proposal for improvement was made because of low frequency of accident scenarios generated by this external hazard.</td>
<td>Analysing in more detail the availability of additional water reserves and approachability of RHR system in accident situations are needed.</td>
<td>An improvement is proposed in the third case study.</td>
</tr>
</tbody>
</table>

**BESEP requirement topic:** Requirements related to confidence provision for defence against the occurrence of cliff-edge effects (PSA):

**BESEP requirement ID:** BESEP_PSA_CEE_001: Probabilistic safety analyses shall be used to demonstrate that sufficient safety margins are available to avoid cliff-edge effects.
### Key features of the verification process

<table>
<thead>
<tr>
<th>STIN_1</th>
<th>STIN_2</th>
<th>STIN_3</th>
<th>Conclusions</th>
</tr>
</thead>
<tbody>
<tr>
<td>PSA is used to show that sufficient SMs are available to avoid cliff-edge effect.</td>
<td>No specific probabilistic analysis to estimate the safety margin to cliff-edge effect occurrence has been performed.</td>
<td>Demonstrated with probabilistic safety analysis by varying the input PGA value of the seismic PSA and evaluating the fuel damage frequency</td>
<td>No PSA is used in the second case study to confirm the fulfilment of the safety requirement.</td>
</tr>
<tr>
<td>Adequacy of Verification</td>
<td>Adequacy of Verification</td>
<td>Adequacy of Verification</td>
<td></td>
</tr>
<tr>
<td>The verification is adequate. The PSA results have shown us that the impact is early a practically eliminated event.</td>
<td>The verification is basically considered adequate for the present time.</td>
<td>The PSA model excludes the structural integrity of the spent fuel pool.</td>
<td>The first and second case study have adequate verification. In the third study the structural integrity of the pool should be included into the PSA.</td>
</tr>
<tr>
<td>Proposals for Improvement</td>
<td>Proposals for Improvement</td>
<td>Proposals for Improvement</td>
<td></td>
</tr>
<tr>
<td>No improvement.</td>
<td>Future improvement is possible to search for cliff-edge effects.</td>
<td>Inclusion of the structural integrity of the pool to the evaluation; deterministic modelling to support PSA.</td>
<td>Improvement is possible in the second and third study.</td>
</tr>
</tbody>
</table>

**BESEP requirement ID: BESEP_PSA_CEE_002: Probabilistic safety analyses shall be used to identify potential areas of improvement in the design to ensure the avoidance of the cliff edge effects.**

### Key features of the verification process

<table>
<thead>
<tr>
<th>STIN_1</th>
<th>STIN_2</th>
<th>STIN_3</th>
<th>Conclusions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Given collapse of the venting stack, the reactor building, longitudinal and transversal buildings, DG station and auxiliary building can be damaged.</td>
<td>No systematic PSA has been performed with focus on cliff edge effects. So, there is no identification of potential areas for improvement originated in PSA.</td>
<td>Seismic Equipment List (SEL) is included in the model, when evaluating the deviations of the fuel damage frequency with different ground accelerations</td>
<td>The first and third study used PSA to identify potential areas for improvement.</td>
</tr>
</tbody>
</table>

### Adequacy of Verification

<table>
<thead>
<tr>
<th>STIN_1</th>
<th>STIN_2</th>
<th>STIN_3</th>
<th>Conclusions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adequate PSA approach for external events is used.</td>
<td>Irrelevant for this safety requirement.</td>
<td>SEL and the seismic component groups provide</td>
<td>The first and third study presented using of adequate PSA approach.</td>
</tr>
<tr>
<td>Proposals for Improvement</td>
<td>STIN_1</td>
<td>STIN_2</td>
<td>STIN_3</td>
</tr>
<tr>
<td>---------------------------</td>
<td>--------</td>
<td>--------</td>
<td>--------</td>
</tr>
<tr>
<td>No improvement.</td>
<td></td>
<td>PSA can be suitable to reduce the impact of cliff-edge effects.</td>
<td>The PSA model could also be used in operator training to avoid cliff-edge effects.</td>
</tr>
</tbody>
</table>

**BESEP requirement topic:** Requirements related to workload, stress and fatigue management (HFE)

**BESEP requirement ID:** BESEP_HFE_SM_001: To reduce the stress simulator-based training of stressful events shall be arranged.

<table>
<thead>
<tr>
<th>Key features of the verification process</th>
<th>STIN_1</th>
<th>STIN_2</th>
<th>STIN_3</th>
<th>Conclusions</th>
</tr>
</thead>
<tbody>
<tr>
<td>To reduce the stress simulator based training of stressful events is arranged.</td>
<td></td>
<td>Plant response to the initiating events modelled in PSA forms standard subject of the simulator training of control room operators.</td>
<td>Regular refresher training including selected transients and accidents that are stressful and cognitively demanding is conducted.</td>
<td>Simulator-based training of stressful events is documented in the case studies regarding fulfilment of the safety requirement.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Adequacy of Verification</th>
<th>STIN_1</th>
<th>STIN_2</th>
<th>STIN_3</th>
<th>Conclusions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adequate HRA approach for external events is used considering the training of stressful events.</td>
<td></td>
<td>This process was verified and found useful for fulfilling of the requirement.</td>
<td>Adequate, although at present workload, stress and fatigue are not evaluated.</td>
<td>Verification is adequate in the case studies. In the third study more detailed evaluation is needed.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Proposals for Improvement</th>
<th>STIN_1</th>
<th>STIN_2</th>
<th>STIN_3</th>
<th>Conclusions</th>
</tr>
</thead>
<tbody>
<tr>
<td>No improvement.</td>
<td></td>
<td>It is proposed to continue in selection of exercised scenarios by PSA and to define priorities in training systematically in sophisticated manner.</td>
<td>Operator stress, workload and fatigue should be measured both by subjective and objective measures. Online evaluation of stress by measurement of stress-related biosignals is especially valuable.</td>
<td>Improvements are proposed in the second and third studies.</td>
</tr>
</tbody>
</table>

**BESEP requirement ID:** BESEP_HFE_SM_002: Training that improves control room personnel communications skills shall be applied to reduce the likelihood that communications will fail under stress.
### Key features of the verification process

<table>
<thead>
<tr>
<th>STIN_1</th>
<th>STIN_2</th>
<th>STIN_3</th>
<th>Conclusions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Training improves personnel communications under stress due to high wind.</td>
<td>Training improving control room personnel communications skills is given by simulator exercises.</td>
<td>Regular refresher training including collaboration within the shift team and between the control room operators and field workers.</td>
<td>In all studies training improves the communications of the plant personnel.</td>
</tr>
<tr>
<td>Adequate HRA approach for external events is used which has taken into account the communication level.</td>
<td>It was verified that plant response is trained at full-scope simulator for internal events scenarios and some of the exercised actions may be used also in the aircraft crash scenarios.</td>
<td>Sufficient</td>
<td>In all studies the verification is sufficient.</td>
</tr>
<tr>
<td>No improvement.</td>
<td>The presented information is an example of good practice and does not need improvement.</td>
<td>A more detailed measurement and analysis of communication is important in order to increase the quality of communication in high stakes situations.</td>
<td>Improvement is proposed in the third study regarding the analysis of communication in high stakes situations.</td>
</tr>
</tbody>
</table>

**BESEP requirement ID:** BESEP_HFE_SM_003: The procedures designed for abnormal and emergency conditions, power plant outages and start-up activities shall support operator work by reducing memory load and need for complex decision making.

| EOPs and SAMGs are available to reduce memory load of the personnel during high wind. In addition procedures for external events are available. | Symptom based procedures are in use in response to initiating events, including those generated by aircraft crash. These procedures extremely reduce the long memory requirements because the required actions are linked with the systems | Validation of new or revised procedures is based on the Systems Usability Case approach | In all studies the procedures are available to support operator actions in case of external events. |

In all studies the procedures are available to support operator actions in case of external events.
<table>
<thead>
<tr>
<th>STIN_1</th>
<th>STIN_2</th>
<th>STIN_3</th>
<th>Conclusions</th>
</tr>
</thead>
<tbody>
<tr>
<td>symptoms, which the operators face at the given time moment directly in the control room.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Adequacy of Verification**

Adequate HRA approach for external events is used considering the procedures available to support operator action during an external event. The fulfilment of the requirement is considered as verified adequately. Procedure design is based on analytical and rigorous method, and verification and validation of procedures is based on a systematic and holistic case-based methodology. In all studies the verification is sufficient.

**Proposals for Improvement**

No improvement. There is no further proposal for improvement. More detailed methods are needed for the analysis of operating procedures. Only the third study has a proposal for improvement.

**BESEP requirement topic:** Requirements related to flow of information between safety analyses (SEP)

**BESEP requirement ID:** BESEP_SEP_FISA_001: When several different types of safety analyses are used to provide evidence, the information flow between safety analyses shall be defined.

**Key features of the verification process**

DSA, and HRA provide inputs into the PSA model. Sufficient level and completeness of the information transfer has been ensured for safety analyses. By defining the safety engineering process for the case study, the linkages between the performed analyses can be identified and the flow of information is ensured. In the studies the linkages between the performed analyses can be identified and the flow of information is ensured.

**Adequacy of Verification**

Adequate DSA, HRA and PSA approaches for external events are used. The verification is adequate, deterministic and probabilistic analyses were checked in detail. Safety engineering process is used to define the information flow between analyses. In all studies the verification is sufficient.
### Proposals for Improvement

<table>
<thead>
<tr>
<th>STIN_1</th>
<th>STIN_2</th>
<th>STIN_3</th>
<th>Conclusions</th>
</tr>
</thead>
<tbody>
<tr>
<td>No improvement.</td>
<td>No improvement.</td>
<td>Different information flow models could be integrated more closely, detailed specification of the safety engineering process should be performed as the first step of the analysis.</td>
<td>The third study has a proposal for improvement.</td>
</tr>
</tbody>
</table>

**BESEP requirement ID:** BESEP_SEP_FISA_002: The flow of information shall support reaching the comprehensive understanding on the issue analysed.

### Key features of the verification process

<table>
<thead>
<tr>
<th></th>
<th>STIN_1</th>
<th>STIN_2</th>
<th>STIN_3</th>
</tr>
</thead>
<tbody>
<tr>
<td>The flow of information supports the understanding of the safety related issues</td>
<td>The validity of the requirement was checked from both sides of the cooperation between DSA a PSA.</td>
<td>The flow of information between central topics in the accident scenario has been roughly specified in the safety engineering process</td>
<td></td>
</tr>
</tbody>
</table>

### Adequacy of Verification

<table>
<thead>
<tr>
<th></th>
<th>STIN_1</th>
<th>STIN_2</th>
<th>STIN_3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adequate DSA, HRA and PSA approaches for external events are used</td>
<td>The verification process has proven sufficiently that this requirement was fulfilled.</td>
<td>Analysis is not necessarily comprehensive in means of analysis areas</td>
<td></td>
</tr>
</tbody>
</table>

### Proposals for Improvement

<table>
<thead>
<tr>
<th></th>
<th>STIN_1</th>
<th>STIN_2</th>
<th>STIN_3</th>
</tr>
</thead>
<tbody>
<tr>
<td>No improvement.</td>
<td>Additional DSA analyses are needed, if some new scenarios are found where the risk impact may not be negligible.</td>
<td>Accommodating the pool leakage to the case study would make the interaction of the analyses more complicated and increase the value of the flow of information management.</td>
<td>Additional DSA is proposed in the third case study.</td>
</tr>
</tbody>
</table>
C.3 Safety Margins Assessment

There are three types of safety margins (SM) considered in the case studies:

- deterministic SM,
- probabilistic SM and
- SM for human actions.

C.3.1 Deterministic Safety Margins

C.3.1.1 Definition

SM is considered for high wind in the context of the margin to failure, as it is illustrated in Figure 1 of the first case study. This margin consists of the entire range between the operating point of a safety parameter and the failure point. Some of the margin is available to the licensee to allow the flexibility needed for safe and efficient plant operation, while additional margin comes about from regulations and requirements, including compliance with codes and standards that provide built-in margin to failure.

The definition of SM for different case studies should be the same or similar as described above and presented in the Figure C.1. It is also in coincidence with definition in D2.3.

The SM is calculated using CDFM (Conservative deterministic failure margin). The results of FEM calculations are the inputs for CDFM.

![Definition of deterministic SM for high wind](image)

*Figure C.1: Definition of deterministic SM for high wind*

Sufficient safety margins are maintained when the distance between the safety limit and the failure point is not significantly degraded by the external event. A reduction in margin either because the safety limit moves closer to the failure point (for example, plant change or new analysis results) or the failure point moves closer to the safety limit (by some SSC degradation mechanism) does not necessarily imply a lack of sufficiency. However, because this margin is controlled by the regulator, regulatory approval would be necessary for continued NPP operation.

No deterministic SM is defined in the second case study. The study is focused on the probabilistic approach in this area.

According to the third case study authors structural strength and seismic capacity of components for a certain PGA against design and regulatory limits and sufficient time windows evaluated with MELCOR analysis are the DSA safety margins.

C.3.1.2 Assessment and Evaluation

In the first case study the fragility assessment and evaluation is performed for SSCs. The parameters for high wind fragility $V_m$, $\beta_R$ and $\beta_U$ are estimated for different SSCs using design data (e. g. wall thickness,
reinforcement, and anchorage) and variability associated with the wind response and capacity. The HCLPF is connected with the median wind capacity using the following formula:

\[
HCLPF \approx V_m e^{2.326 \beta_c}
\]

where \( \beta_c = (\beta_R^2 + \beta_U^2)^{1/2} \) is the logarithmic standard deviation.

The deterministic parameter obtained from DSA:

\[
HCLPF = V_m \exp(-1.65 (\beta_U + \beta_R)).
\]

The design values of the venting stack for wind loading are the following:

- \( HCLPF = 38.7 \text{ m/s} \) for 10 minutes wind speed, measured at 10 m above the earth’s surface, and
- \( HCLPF = 54 \text{ m/s} \) for gust wind impact at 10 m above the earth’s surface (the stack should withstand both types of wind loads).

Conservative calculations of safety limits are performed. If the conservatism of the finite element models (FEM) is removed, the safety limit of the high wind would be significantly decreased. The EPRI seismic fragility analysis methodology is developed only for seismic event. Normally not used for non-seismic external events.

The second case study is focused on the probabilistic approach.

In the third case study impact and vibrations analyses are used to assess the structural strength of the fuel pool structure, and to produce comparable seismic fragility curves to assess the state of the RHR system equipment. The obtained values are compared with the available design values or regulatory limits. MELCOR analyses produces time windows for the pool coolant heating and boil-off. The time windows are compared with the operator actions. In this case, the fuel pool withstands the impact, so the safety margin for the used PGA value is sufficient. This is the deterministic approach.

C.3.1.3 Comparison of SM Interpretation with Chapter 4 of Deliverable 2.3

Definition is in coincidence with D2.3. It can be concluded that interpretation of relevant safety margins in the case studies are in good agreement with chapter 4.1.

C.3.1.4 Proposals for Improvement

No improvement is needed in this area. The deterministic SM is exactly defined, the CDFM to provide assessment of SSCs capacities is the state of the art method.

C.3.2 Probabilistic Safety Margins

C.3.2.1 Definition

The calculated CDF (FDF) is compared with the safety targets of the regulatory authorities. Level 1 PSA, CDF for internal and external events should be less than 1.0E-4/y for plants in operation and less than 1.0E-5/y for the new plants. The LERF is smaller by one order of magnitude. This is the definition from the first case study.

Provided that the limiting recommended annual CDF frequency is up to 1.0E-4/y, the aircraft crash annual frequencies of order of magnitude of 1.0E-7/y show up sufficient safety margin according to the second study.

PSA safety margin is defined as the difference of the FDF and the regulatory target, and the fragility estimates and margins of SEL components. This is definition from the third case study. According to this study FDF values and potential cliff-edge effect evaluations are compared to the regulatory safety targets and the
existence of sufficient margin is verified. Sufficiency of the fragility estimates of SEL components is checked against the design. FDF acceptance criteria values are not presented in the case study.

C.3.2.2 Assessment and Evaluation

CDF is calculated in the first case study for high wind. Sensitivity analysis on the different factors contributing to the FDF values and possible cliff-edge effects has not been carried out in the third case study for seismic event. The over-simplified PSA model applied in the case study is probably insufficient for the evaluation of potential cliff-edge effects.

The value of aircraft crash and plant hit frequency of 1.0E-7/y is valid for the turbine hall, which represents the far largest structure at the plant. For safety important structure as reactor building, the corresponding annual frequencies of the plant hit by the aircraft crashed are of order of 1.0E-8 – 1.0E-9/y in accordance with the postulated aircraft category. The CDF contribution related to the aircraft crash risk is 5.3E-8/y. It is obvious that aircraft crash belongs to the very small risk contributors from the category of external hazards. It should be also pointed out that the whole aircraft crash risk analysis was done systematically on conservative side. So, the real safety margin could be likely even bigger. Sufficient safety margins exist according to the second study.

C.3.2.3 Comparison of SM Interpretation with Chapter 4 of Deliverable 2.3

The mean values of CDF (FDF) and LERF are used for comparison with the safety targets of the regulatory authority. Deliverable 2.3 proposed the upper bound for comparison. Therefore, this approach is not directly applicable for the case studies discussed here.

C.3.2.4 Proposals for Improvement

There is no proposal from improvement in the first study. The third study proposes that HFE results should be utilized more in HRA to identify and better integrate the different features of human actions. This would help, for example, to generate more accurate estimates for the performance shaping factors improving the estimates on the FDF.

C.3.3 Safety Margins for Human actions

C.3.3.1 Definition

No such definition is used in the first case study. The third study approach is that values of stress and crew communication during the simulated loss of heat removal of spent fuel pool accident have to be compared to baseline levels. Increased knowledge of the effect of stress, workload and fatigue on operator performance enables the development of more demanding stress tests for operator performance evaluation.

In the second case study it was mentioned that there is no explicitly defined formal safety margin for human actions addressed in risk analysis in the Czech Republic, represented by some quantitative limits. In general, HFE safety margins are not really defined, but HRA may contribute to the discussion of human factor related margins. Human error qualitative analysis methods, such as SHERPA and HAZOP, can be used in error identification, categorization, and analysis.

C.3.3.2 Assessment and Evaluation

Detailed HRA is performed in the first case study. HEP < 1.0E-5 are not considered in the internal and external event PSA. However, the HEPs in external event PSA are at least by one order of magnitude higher than the internal event PSA. In the third case study for value comparison detailed data are not available.
Since the human factor analysis and the results reached have often got a relatively subjective character (in comparison with evaluation of equipment role for plant safety), possible assessment and evaluation of human related safety margin should be better based on some way of quantitative analysis, not just on subjective qualitative “expert judgment”. Such approach could prevent bringing additional uncertainty into the plant safety concept. There are two main categories of quantitative variables appearing in risk analysis in connection with human actions. The first one is probability of failure/success of a concrete human (control room crew, plant staff) action. The second category is represented by importance measures of human actions, human action groups and overall human contribution to plant risk. This is the view of the authors of the second case study.

The human failure probabilities do not belong to good candidates for evaluation of safety margin. The plant crew actions are carried out under very different conditions and circumstances, and they have very different impact on the overall value of plant operation risk. So, a relatively high probability of failure does not automatically mean that some safety margin is endangered, and vice versa – a relatively small human failure probability may still represent a serious problem. The values of importance measures of human actions are much better indicators of possible points of decreasing of safety margin. Two out of three most frequently used importance measures, i.e. fractional contribution and risk increase factor can be used for the safety margin related discussions and analyses. In an optimum case, the importance measures of human failures are somewhat balanced. As soon as some human actions with relatively very high value of fractional contribution exist, safety margin can be attacked the more, the lower the estimated failure probability is. Similarly, if the risk-increase factor of some human action (plant CDF in case of some sure human failure divided by the baseline plant CDF) is very high, safety margin is possibly challenged.

C.3.3.3 Comparison of SM Interpretation with Chapter 4 of Deliverable 2.3

No specific approach is presented in Deliverable 2.3 for comparison.

C.3.3.4 Proposals for Improvement

A more holistic approach is needed to better integrate stress, workload, fatigue and other factors that contribute to operators' cognitive readiness into HFE analyses. Procedure development should be based on systematic task analysis and task complexity analysis.

The analysis of the impact of human factor on the safety margin can be started with looking at the values of human actions related importance measures in the PSA study. The actions with high importance measures are possible candidates for reaching plant safety margin in case of human failure. If the risk engineering tools (PSA) point at such actions, these actions should be reviewed carefully. Since importance analysis is an integral part of each important risk analysis activity, the approach described above has been taking place in many recent risk analysis activities, including analyses of risk of external events.

In general, all modelled, and subsequently analysed human actions can be divided into two basic categories in the external events scenarios:

1. human actions performed by operators in the main control room in the process of plant cooling down and transfer to stable safe status;
2. human actions performed locally, mostly with the aim to prevent occurrence of the scenarios requiring actions from control room.

It seems that sufficient balance of error impact potential was reached for the actions performed from control room during years of development of PSA studies of internal events and external hazards and addressing their results in the risk engineering processes so that these actions are not carried out under the specific conditions threatening safety margin. This statement is valid also for the external hazard “aircraft crash”. As soon as the working conditions of control room crew are not impacted by the aircraft hit directly, the operators perform the actions leading to safe cooling down prescribed in the symptom based procedures, which are determined by the available equipment configuration, and the approach used for plant response is similar to the internal events scenarios.
In the external hazard scenarios, generally, the local plant crew actions to be possibly studied regarding human factors related safety margin, can be divided into preventive actions, and the actions carried out in response to the phenomena generated by the external hazard. For the aircraft crash scenarios, however, the potential for determination of human factor related safety margin is very limited for such actions. First, the external events from this category are so much sudden and unexpected that there can be hardly any prevention considered. Secondly, it is very difficult (and unpractical) to try to describe the human factor related safety margin for the catastrophic scenarios after aircraft crash and plant hit (it would be probably better to consider the overall aircraft crash related safety margin directly).

Altogether, probabilistic risk analysis provides useful relevant means how to identify, address and solve possible problems with safety margin related to human actions. There is no suitable means, how to connect (quantified) plant safety margin with human actions in the deterministic analysis. However, for the local plant crew actions after the aircraft crash, in particular, the potential to determine human factor related safety margin is very limited.

Summary of the comparison process is provided in Table C.2.
### Table C.2: Assessment of Safety Margins

<table>
<thead>
<tr>
<th></th>
<th>STIN_1</th>
<th>STIN_2</th>
<th>STIN_3</th>
<th>Conclusions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Deterministic Safety Margins</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Definition</strong></td>
<td>HCLPF (High Confidence of Low probability of Failure)</td>
<td>Deterministic vulnerability characteristics of safety important SSCs</td>
<td>PGA (structural strength &amp; seismic capacity), time windows</td>
<td>The SSCs capacity is calculated for external events using deterministic approach.</td>
</tr>
<tr>
<td><strong>Assessment &amp; Evaluation</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CDFM (Conservative Deterministic Failure Margin) and FEM (Finite Element Method)</td>
<td>Deterministic fragility analysis, expert judgment</td>
<td>Impact and vibrations analyses, MELCOR analysis</td>
<td>Deterministic analyses are used for assessment and evaluation of the SM.</td>
</tr>
<tr>
<td><strong>Comparison with D2.3</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The safety margin is in line with the Chapter 4.2 of Deliverable 2.3.</td>
<td>In line</td>
<td>In line</td>
<td>In line</td>
</tr>
<tr>
<td><strong>Proposals for Improvement</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>None.</td>
<td>None</td>
<td>none for the methodology</td>
<td>None</td>
</tr>
<tr>
<td><strong>Probabilistic Safety Margins</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Definition</strong></td>
<td>Safety targets for CDF, FDF, LERF for plants in operation and for new plants.</td>
<td>CDF, FDF, LERF related</td>
<td>FDF and regulatory target</td>
<td>CDF is calculated in the first case study, no FDF is calculated in third case study. The aircraft crash is a practically eliminated event in the second case study</td>
</tr>
<tr>
<td><strong>Assessment &amp; Evaluation</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Level 1 PSA, CDF for internal and external events should be less than 1.0E-4/y</td>
<td>Level 1 and 2 PSA</td>
<td>Not calculated in the case study</td>
<td>CDF is calculated in the first case study. The aircraft crash is a practically eliminated event in the second case study. FDF is not calculated in third case study.</td>
</tr>
<tr>
<td><strong>Comparison with D2.3</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The safety margin in general level is in line with</td>
<td>In line</td>
<td>In line</td>
<td>The safety margin in general level is in line with the Chapter 4.3 of Deliverable 2.3. However, the mean value of CDF and LERF is</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## STIN_1 STIN_2 STIN_3 Conclusions

<table>
<thead>
<tr>
<th>Proposals for Improvement</th>
<th>None.</th>
<th>None</th>
<th>HFE results should be utilized more in HRA</th>
<th>HFE results should be utilized more in HRA according to the third case study.</th>
</tr>
</thead>
</table>

## Safety Margins for Human Actions

<table>
<thead>
<tr>
<th>Definition</th>
<th>No exact definition</th>
<th>No exact definition</th>
<th>No exact definition, stress and crew communication values are compared to baseline levels</th>
<th>No exact definition is available.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assessment &amp; Evaluation</td>
<td>HEP &lt; 1.0E-5 are not considered. HEPs in external event PSA are at least by one order of magnitude smaller than HEPs in internal event PSA</td>
<td>Importance measures can indicate (relatively) small safety margin</td>
<td>Value comparison, detailed data not available.</td>
<td>HEPs in external event PSA are at least by one order of magnitude smaller than HEPs in internal event PSA. Importance measures can indicate (relatively) small safety margin.</td>
</tr>
<tr>
<td>Comparison with D2.3</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Proposals for Improvement</td>
<td>To remove conservatism from FEM analyses</td>
<td>To postulate suitable variables for measurement (estimation) of human factor related safety margin.</td>
<td>Integrate stress, workload, fatigue and other factors that contribute to operators’ cognitive readiness into HFE analyses.</td>
<td>Different proposals for improvements.</td>
</tr>
</tbody>
</table>
C.4 Interactions between DSA, PSA and HFE

C.4.1 Description of interactions

In the first case study, DSA is used to generate HCLPF for PSA. Using the HCLPF and the uncertainty parameters (the formula is described above) the fragility curves for SSCs are constructed. Failure probability of SSCs can be calculated after implementation of hazard curves and fragility curves into the HazardLite module of the RiskSpectrum code. HazardLite performs convolution of the hazard curves and fragility curves and SSC failure probabilities are calculated.

The third study describes the analyses interactions as follows. The impact loads are used in the component fragility analysis, which is further used in seismic PSA. Seismic PSA is used to update the seismic equipment lists. Time windows for the boil-off of pool coolant are used as PSA success criteria for accident management and in HFE analysis. HFE analyses provide performance shaping factors to HRA, which are then used in the PSA model; PSA modelling also utilizes the component fragility analyses, pool water inventory analyses and accident management, e.g. the operator actions.

Detailed description follows for the second study. The analysis started with Step 1: collection and analysis of the information about the aircraft traffic in plant vicinity which is considered deterministic, in general, although the methods of probabilistic and mathematical statistical analysis are also used. On the base of this information, several (four) categories of aircraft were defined in Step 1a to represent various possible impacts of aircraft fall on plant SSCs. The next Step 2 – determination of structures important as potential targets of damage by crashed aircraft was purely deterministic and there was no direct connection of it with Step 1. In Step 3, annual frequencies of the events “aircraft from category X hits plant structure Y” were determined for all aircraft categories defined in Step 1a and all plant structures listed in Step 2. Step 3, similarly to the Step 1, is considered as deterministic although it includes many features of probabilistic and mathematical statistics work.

The next steps were already oriented to the more detailed analysis of accident scenarios generated by aircraft crash. Although the main aim of these steps is to provide inputs for probabilistic modelling in PSA, the general character of them is still deterministic. In Step 4, possible initiating events generated by aircraft fall and hit were investigated, defined, screened and grouped, taking into consideration the possibility of generation of more than one missile (commercial aircraft usually possess more than one engine), possibility of explosion of military arsenal located at the military aircraft, possibility of damage of neighbour objects (big span of aircraft wings, high kinetic energy generated by the fall, big volume of fuel in the tanks) and possibility of direct damage of reactor core or spent fuel pool (in the case of aircraft fall on reactor building). A more detailed purely deterministic analysis of aircraft fall consequences was done in Step 5, making possible to specify available configurations of plant SSCs modelled in PSA event trees. Step 6 opens the probabilistic part of analysis oriented to development and application of PSA model. This step: Modelling of plant response to the specific variant of aircraft scenario covers all selected combinations of aircraft categories specified in Step 1a and hit locations represented by safety important structures selected in Step 2. The rest of the analysis represents typical final steps of PSA scope: Step 7: Quantification of PSA model and Step 8: Final (quantitative) analysis and interpretation of results. The very last part of the analysis is typically not purely probabilistic, but the interpretation of results and generation of recommendations regarding plant safety on the base of PSA returns back to deterministically oriented views and conclusions. It should be pointed out, however, that a typical (probabilistic) analysis of aircraft crash risk, as performed worldwide, does not generate many recommendations and measures related to plant design and operation, rather it postulates the level of aircraft crash risk as low, or suggest changes related not to plant itself, but the way air traffic should be organized around the plant by the subjects involved (airports, zone defined around the plant to protect it from random hit, training rules and operational conditions on the aircraft at the plant vicinity etc.)

C.4.2 Evaluation of Adequacy

No HFE is involved in DSA in the first case study. HEPs are implemented into the external event PSA. Only HRA activities are considered. DEC analyses are performed in level 2 PSA. So, it is out of scope of the first case study. The interactions have been made in a way typical for interconnections between level 1 PSA
(representing DBA analyses) and level 2 PSA (related to DEC). The PSA study of the plant is based on an integrated level 1 and level 2 model. This model, modified accordingly for aircraft risk analysis, was used in the second case study.

HFE is not directly connected to DSA/PSA, but time windows from MELCOR analysis (DSA) are directly used in HFE. HFE analyses provide performance shaping factors to HRA, which are then used in the PSA model of the third case study.

DSA are providing inputs for PSA in the first study. This interconnection of DSA and PSA is the only way for calculation of CDF and FDF for the plant within a level 1 PSA project. Alternatives exist only in the form of DSA, however, the most acceptable results for the regulatory body are to have conservative results received by CDFM method.

In the third study the use of safety analyses is not necessarily comprehensive, and should preferably be defined more thoroughly in the beginning of the assessment according to needs and resources. One interaction that has been omitted in the analysis, would be maintenance errors, e.g. valves left in wrong positions. The consequences would affect HFE, PSA and DSA analyses.

The response of the second study is the following. The development and up-date of an integrated PSA model (representing both level 1 and 2 PSA, i.e. DBA and DEC scenarios, respectively) is a demanding and time consuming process, but once such model is ready for applications, it is very suitable for risk oriented decision making and risk engineering activities in general.

Similarly, to the risk analysis of other external hazards, the analysis carried out in the aircraft crash case study, although having many probabilistic features, represents a combination of DSA, PSA and HFE analysis. It seems, in general, that the HFE part of the analysis is somewhat limited in comparison with the risk analysis related to the accident scenarios generated by natural hazards – the reason is the suddenness of the hazards impact, where some preventive (human) actions can be hardly part of the accident scenario modelled in PSA.

C.4.3 Proposals for Improvement

In the aircraft case study the meaning and scope of HFE part of the analysis is usually a bit suppressed in comparison with other external hazards analysis (there is another very important part of HFE effort related, which takes place on the air traffic side – training of pilots including simulators, development of procedures and MMI, communication with air traffic controller etc., but these elements are typically considered as internal features of the traffic and not addressed in PSA for nuclear power plants in detail (the question is whether more effort should not be initiated from this point of view).

In Step 6 of the analysis carried out in the second case study: *modelling of plant response to the individual variants of aircraft crash*, there was strong connection of PSA with HFE in the area of control room crew actions, where the developed accident sequences were, to a significant extent, based on the plant internal events PSA model, the actions transferred from that model into the aircraft crash hazard analysis were systematically reviewed from point of view of applicability and possible differences in the operational conditions. In Step 7: *Quantification of PSA model* – similarly to quantification approaches usually used for any PSA model, the scope, style and details of quantification can be adjusted to bring answers to the specific HFE related questions so that this step may use inputs from the HFE related parts of the case study. In Step 8: *Analysis and interpretation of results of risk analysis* a significant part of the results is usually expected to be relevant for HFE and to produce useful conclusions for the process of increasing of plant safety. It can be postulated, altogether, that there is relatively low connection of the HFE area with deterministic and probabilistic part of the analysis in this case study, which is typically limited to the analysis of control room crew actions in response to aircraft crash with the aim to cooling down the plant safely, where many methodical points and data are transferred from the internal events PSA.

Summary of interactions is presented in table C.3.
### Table C.3: Interactions between DSA, PSA and HFE

<table>
<thead>
<tr>
<th>STIN_1</th>
<th>STIN_2</th>
<th>STIN_3</th>
<th>Conclusions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Interactions between DSA, PSA and HFE</strong></td>
<td>DSA is used data to generate failure probabilities for SSCs. HFE and HRA also provides inputs into PSA in form of HEPs.</td>
<td>The case study has many probabilistic features, represents a combination of DSA, HFE and PSA. The HFE part of the analysis may be limited in comparison with analyses of other external hazards.</td>
<td>Impact loads used in the component fragility analysis, which is further used in seismic PSA.; seismic PSA is used to update the seismic equipment lists; The HFE analyses provide performance shaping factors to HRA. The PSA modelling also utilizes the SSCs fragility analyses, pool water inventory analyses and accident management, e.g. the operator actions.</td>
</tr>
<tr>
<td><strong>Evaluation of Adequacy</strong></td>
<td>Adequate DSA, HRA and PSA approaches for external events are used</td>
<td>Adequate</td>
<td>Adequate</td>
</tr>
<tr>
<td><strong>Proposals for Improvement</strong></td>
<td>No improvement is needed.</td>
<td>The process of definition and carrying out the inputs from DSA/PSA to HFE could be made more systematic.</td>
<td>No improvement in the first and third study. The process of definition and carrying out the inputs from DSA/PSA to HFE could be made more systematic according to the second study.</td>
</tr>
</tbody>
</table>
C.5 Overall Safety Engineering Process

Plant response and fragility analyses are performed in the first case study within DSA. High wind PSA is developed in the case study. HRA is performed for human actions, evaluation of adequacy of modelling from the plant safety point of view is performed. The steps of SEP are defined as follows: 1) external hazard analyses, 2) finite elements model of SSCs, 3) fragility analyses of SSC using CDFM, 4) PSA modelling, 5) evaluation of the results and 6) implementation of the safety measures.

The safety engineering process applied in the second case study under concern consisted of the Steps 1-8 described and discussed in previous part of this report. The general framework for this case study was specified by the practice adopted in the long term of NPP Dukovany Living PSA project and by the practice recommended for PSA part of the large new project of cooperation of CEZ company operating NPPs in Czech Republic and UJV company having the role of TSO. The main strength of the overall safety engineering process adopted is foundation of an integrated project, where all participating subjects (both PSA and DSA, but also HFE related) work together in a very close cooperation.

For the third case study see description and figures of the three levels of SEP applied in the study from the updated self-evaluation. In addition, three levels are defined, V-model to identify which plant architectures are affected by the requirements and the external impact and which safety analyses are needed, process schematic to identify the steps of the analysis, and definition of the steps inside a specific analysis (SPSA).

In understanding of the first case study authors the HCLPF calculation is an adequate approach for interconnection of PSA and DSA. For comparison of this SSC capacity calculation with other methods there is not enough information in the case studies.

The strengths and weaknesses of SEP in the case studies are described in the updated self-evaluations. Conservative results to confirm the safety of the plants are identified as the weakness in the first case study. Not detailed PSA was developed in the second study. The third study identified the following weaknesses: SEP could be formulated better, connection of requirements, design and analyses not very detailed.

Summary of SEP and characterization of the whole process are presented in Table C.4.
Table C.4: Characterization of the Overall Safety Engineering Process

<table>
<thead>
<tr>
<th>STIN_1</th>
<th>STIN_2</th>
<th>STIN_3</th>
<th>Conclusions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Overall approach and steps of the SEP</strong></td>
<td><strong>Overall approach and steps of the SEP</strong></td>
<td><strong>Overall approach and steps of the SEP</strong></td>
<td></td>
</tr>
<tr>
<td>Plant response and fragility analyses are performed in the case study within DSA. HRA is performed for human actions based on HFE. External event PSA is developed. Evaluation of adequacy of PSA modelling from the plant safety point of view is performed.</td>
<td>The general framework for this case study was specified by the practice adopted in the long term of NPP Dukovany Living PSA project, which had been running since 1998.</td>
<td>Three levels defined, V-model to identify which plant architectures are affected by the requirements and the external impact and which safety analyses are needed, process schematic to identify the steps of the analysis, and definition of the steps inside a specific analysis (SPSA)</td>
<td>The safety analyses needed within the SEP are identified in the case studies. PSA models are developed in the first case study (High wind PSA) and the third case study (SPSA). No PSA model was developed in the second study.</td>
</tr>
<tr>
<td><strong>Interrelationship among the Steps</strong></td>
<td><strong>Interrelationship among the Steps</strong></td>
<td><strong>Interrelationship among the Steps</strong></td>
<td></td>
</tr>
<tr>
<td>The steps of SEP are defined as follows: 1) external hazard analyses, 2) finite elements model of SSCs, 3) fragility analyses of SSC using CDFM, 4) PSA modelling, 5) evaluation of the results 6) Implementation of the safety measures.</td>
<td>Described in the self evaluation and in the text part of this report.</td>
<td>Steps follow the three levels formulation of SEP</td>
<td>The steps of SEP are exactly defined in the case studies.</td>
</tr>
<tr>
<td><strong>Strength of the SEP</strong></td>
<td><strong>Strength of the SEP</strong></td>
<td><strong>Strength of the SEP</strong></td>
<td></td>
</tr>
<tr>
<td>A very widespread method and the software is available for application. Exact connection of the analysis is the strength of the SEP</td>
<td>The main strength of the overall safety engineering process adopted is foundation of an integrated project, where all participating subjects (both PSA and DSA, but also HFE related – regular simulator data collection is part of the project, for example) work together in a very close cooperation.</td>
<td>Clear connection of analyses</td>
<td>Exact connection of the analyses is the strength of the case studies.</td>
</tr>
<tr>
<td>STIN_1</td>
<td>STIN_2</td>
<td>STIN_3</td>
<td>Conclusions</td>
</tr>
<tr>
<td>--------</td>
<td>--------</td>
<td>--------</td>
<td>-------------</td>
</tr>
<tr>
<td><strong>Weaknesses of the SEP</strong></td>
<td>Conservative results to confirm the safety of the plants.</td>
<td>Not fully consistent approach to PSA.</td>
<td>Could be formulated better, connection of requirements, design and analyses not very detailed</td>
</tr>
<tr>
<td><strong>Proposals for Improvement</strong></td>
<td>To remove the conservatism from FEM analyses</td>
<td>The inconsistency between PSAs, and, more general, safety analyses developed for different plants are being identified and solved with the goal to develop unified approach adaptable for both NPPs. The area of external hazards represents significant part of this effort.</td>
<td>Detailed system and component analysis; formal description of requirement management system</td>
</tr>
</tbody>
</table>
C.6 Key Success Factors for an Efficient and Integrated SEP

Generally, it is assumed that the plant is constructed and operated in accordance with its licensing basis, and the design includes appropriate SMs and is consistent with the DID philosophy (the safety is not wholly dependent on any single element of the design, construction, maintenance, or operation). The net effect of incorporating DID into design, construction, maintenance, and operation is that the plant is more tolerant of failures and external challenges.

C.6.1 Key Success Factors

The key success factors are the following for an efficient and integrated SEP which is used to implement changes (safety measures) into the plant to remove weaknesses. The proposed safety measures are implemented on the basis of risk-informed decision making where a set of key principles (success factors) should be met:

1. change meets the current regulations unless it is explicitly related to a requested exemption,
2. change is consistent with the DID philosophy,
3. change maintains sufficient safety margins,
4. when change results in an increase in risk, the increases should be small and consistent with the intent of the regulatory policy statement on safety goals for the operations of nuclear power plants and
5. the impact of the change should be monitored using performance measurement strategies, wherever possible and relevant.

C.6.2 Generalized SEP

It has been determined that risk information can help inform about the potential impacts of the external event on the principles of DID, SM, and acceptable level of risk are assessed. The questions to be asked include how DID, SM, and risk are impacted and to what extent the PSA can provide adequate insights. The PSA modelling approach is then defined, the analysis performed, uncertainties identified, and sensitivity studies undertaken.

It should be emphasized that the SEP is not a linear process. In particular, the definition of the change can be modified as the analysis progresses. For example, as more is known about the risk contributors or as more is learned about how the various key principles (success factors) are affected. For example, new information on hazards or failure mechanisms, may depend on developing and understanding of how that new information affects the principles of SEP.

The overall SEP (flow of analyses defined in BESEP safety requirements described above) is outlined in Figures 2-4. It is a proposal for a generalized case study.

The safety requirements, legislations and standards are set in such a way that the assessment and design of upgrading measures is compliant with the international and national legislative requirements, international and national codes, standards and practices. The selection of codes and standards follows a hierarchic structure, developed according to the European Utility Requirements for LWR plants (see Figure 2).

After the DSA and HFE necessary to support the assessment of the risk principle (and the DID and SM principles when applicable) have been defined, the existing plant PSA model will be used or modified to account for the effects on risk, DID, and SM (see safety analyses in Figure 2).

When a change affects the performance of an SSC or function, this entails ensuring that the cause-effect relationship can be represented in terms of changes to either the logic structure of the PSA model or to the quantification. The former may be done, for example, by including in the model new risk contributors, and the latter by quantifying the PSA model using updated function, system, or basic event probabilities. To address the DID principles (see Figure 3) and SM principles (see figure 4), the PSA model must include those scenarios for which changes to the DID and SM are predicted.
After the types of risk impacts and the elements of the PSA model that are affected have been identified, it remains to perform the risk evaluations. This typically requires establishing a baseline risk model to reflect the initial status and exercising that model to reflect the effects of the change.

This process requires performing the risk calculations in the following manner:

- The basic risk metrics are properly evaluated.
- The results can be decomposed to identify important contributors (and to provide a means to ensure that the technical quality of the PSA model is maintained).
- Uncertainties and sensitivities should be captured and explained.

In coincidence with the PSA results, the plant design is changed. It means safety upgrading of SSCs with significant contribution to the risk. If necessary, also the relevant plant procedures are updated. Finally, the plant safety upgrading is performed. Performance monitoring is made in the safety analyses as a strategy that can be used to determine whether the implementation of the change is consistent with the assumptions made in the safety analysis. It is not always possible to define a performance monitoring regime, because the anticipated changes may be small enough and sufficiently slowly developing that an effective monitoring strategy cannot be determined. Nevertheless, if such a strategy can be identified, it should be part of the definition of the proposed change (see Figure C.2).

In a generalized study, based on STIN case studies, the above described activities must be performed. In addition, Figure C.5 shows the main steps for development of the external event PSA model for the generalized case study:

- External hazard analyses for the site (the hazard curves were generated in the first case study, deterministic external hazard analyses were performed in the second case study and impact analyses in the third case study – probably the hazard curves are also available)
- Finite elements building models (available in the first study and probably available also in the second and third study). HFE is needed to develop the finite elements models.
- Fragility analyses of SSCs. HCLPF is used to develop the fragility curves (fragility curves are available in the first study for high wind and these curves are probably also available in the third study for seismic event; no information is available about these fragility curves of SSCs in the second study for aircraft crash). Failure probability of SSCs can be calculated by convolution of the hazard curves and fragility curves to support development of the external event PSA. These calculations can be performed using the HazardLite module of the RiskSpectrum PSA code.
- The list of SSCs for fragility analyses is provided from the preliminary PSA model.
- The results of fragility analyses for SSCs are verified by plant walk-downs.
- Failure probabilities of SSCs are inputs to the PSA model.
- HFE provides performance shaping factors for HRA.
Is defense in depth affected and if yes, how?

AFFECTED

Define PSA to support defense in depth insights.

PSA insights on DID impacts?

YES

PSA input

Finite elements models

SAFETY ANALYSES

Define PSA to support safety margin insights.

PSA insights on safety margin?

YES

DSA input

HCLPF for SSCs

List of SSCs

HFE input

Performance shaping factors for HRA

Define how risk is affected.

Are safety margins affected and if yes, how?

AFFECTED

PSA and sensitivity analysis. Identify relevant risk insights.

Summarize defense in depth considerations.

Summarize risk considerations.

Summarize safety margin considerations.

Contribution to overall plant risk (CDF)

Safety upgrading of SSCs.

Updating of the procedures.

Safety upgrading of the plant and performance monitoring.

CONTRIBUTION TO OVERALL PLANT RISK

SUMMARY

SAFETY ANALYSES

PSA input

DSA input

HFE input

Performance shaping factors for HRA

Finite elements models

HCLPF for SSCs

List of SSCs

HFE

PSA

DSA

Figure C.2: SEP for the generalized case study
Figure C.3: Impacts of external event on DID in generalized case study

Figure C.4: Impacts of external event on SM in generalized case study
Figure C.5: Development of the external event PSA model for the generalized case study
APPENDIX D: CROSS-CASE COMPARISON IN CASE STUDY GROUP LUHS

D.1 General information

**Responsible Organization(s): Fortum, NUBIKI, RELKO, Risk Pilot**

**Case Study Group Identifier: LUHS**

**Date:** 3.10.2022

**Case Study Titles:**

LUHS_1 Loss of Ultimate Heat Sink (Frazil Ice or Oil Spill),

LUHS_2 Loss of the Service Water System due to Extremely Low Temperature,

LUHS_3 Blockage of (Water) Intake Building,

LUHS_4 Evaluation of Plant Vulnerabilities to Riverine Events.

D.2 Fulfilment of BESEP Safety Requirements

D.2.1 The key features of verification process for LUHS_1

**BESEP_DSA_FSEP_001:** The safety systems, structures and components, including auxiliary or supporting systems thereof, shall be protected from interaction with failed systems, structures or components as far as reasonably practicable.

*Summary of the Verification Process*

The safety functions designed for LUHS have been verified to withstand the failure propagation as the diverse functions are functionally and by distance separated from the main functions. The verification has been conducted by DSA failure analysis and also with PRA.

*Adequacy of Verification*

DSA, i.e. failure propagation analysis has been conducted to verify the design and the means to cope the events. The safety functions designed for LUHS fulfil the requirement.

*Proposals for Improvement*

No improvement proposals.

**BESEP_DSA_FSEP_002:** The safety divisions hosting redundant parts of safety systems shall be located in different buildings or housed in dedicated compartments to separate them from the other safety divisions in the same building in order to prevent faults from spreading from one redundant system part to another as a result of external events.

*Summary of the Verification Process*

The original design of the NPP with two-redundant main and safety systems and the original layout do not totally comply with the requirement. For all new installations the separation principle is followed. As there exist diverse systems to fulfil the same safety target, and these are located to withstand the failure propagation, the safety targets are met.
Adequacy of Verification

DSA, i.e. failure propagation analysis has been conducted to verify the design and the means to cope the events.

Proposals for Improvement

No improvement proposals.

**BESEP_DSA_FSEP_003: The systems of different safety classes shall be functionally separated so that failure of a system or component of a lower safety class does not affect a function of a higher safety class.**

Summary of the Verification Process

The systems of different safety classes shall be functionally separated so that failure of a system or component of a lower safety class does not affect a function of a higher safety class.

Adequacy of Verification

For renewal projects in the plant the functional separation is verified in DSA. For the existing design the same analysis has been conducted for the systems and safety functions with recognised safety importance, not for the whole plant.

Proposals for Improvement

No improvement proposals.

**BESEP_PSA_ALSF_001: The potential losses of safety functions shall be evaluated based on the resistance of NPP against the hazards, taking into consideration real status of all systems, structures and components relevant to nuclear safety.**

Summary of the Verification Process

The potential losses of safety functions have been adequately evaluated.

Proposals for Improvement

No improvement proposals.

**BESEP_PSA_ALSF_002: Complex failure combinations of systems, structures and components initiated by external hazards shall be identified and their significance to nuclear safety shall be evaluated.**
Summary of the Verification Process

Failure dependencies (designed and statistical) have been analysed. Designed dependencies include initiator dependencies, system dependencies and interactions. Statistical dependencies include dependent/repeated human errors, plant-specific hardware dependencies and residual parametric common cause failures.

HRA supported the evaluation.

Adequacy of Verification

The complex failure combinations related to the loss of ultimate heat sink have been adequately identified.

Proposals for Improvement

No improvement proposals.

**BESEP_PSA_ALSF_003: The important functional dependencies on physical location and from operation, maintenance and the effects of human activities shall be considered in assessing the potential losses of safety functions.**

Summary of the Verification Process

Failure dependencies (designed and statistical) have been analysed. Designed dependencies include initiator dependencies, system dependencies and interactions. Statistical dependencies include dependent/repeated human errors, plant-specific hardware dependencies and residual parametric common cause failures.

HRA supported the evaluation.

Adequacy of Verification

The important functional dependencies related to the loss of ultimate heat sink have been adequately considered in assessing the potential losses of safety functions.

Proposals for Improvement

No improvement proposals.

**BESEP_HFE_SAA_001: The design of user interfaces in NPP shall support the operators in assessing any normal and abnormal situation so that they can perceive the situation, comprehend it and finally anticipate the future status of the event.**

Summary of the Verification Process

A style guide ensures that all new and modernized user interfaces follow the good practices and support the operators in best possible way. For the design two terms have been defined: accident situation ergonomics and normal operation ergonomics. Accident situation ergonomics means adjusting the technology and functions to human behaviour. The accident situation ergonomics has been validated and verified with V&V actions during the design stage and also with integrated sub-system validation, that was conducted in full-scale simulator. Normal operation ergonomics means adjusting the technology and functions to human behaviour in normal operation like situations. The normal operation ergonomics is validated with operational experience.

Adequacy of Verification

In the design of the user interfaces the needs of the operators have been taken into account.

Proposals for Improvement

No improvement proposals.
**BESEP_HFE_SAA_002:** The visual monitors or operating panels shall provide the operators a holistic view on the plant state and feedback from the course of event and effects from activations and passive or automatic functions.

**Summary of the Verification Process**

In the design of user interfaces the tasks, requirements and experiences of the users are taken into account. The design aims to support safe and efficient operation. User interfaces provide information of the process, support observing the state of the process, enable safe control operations and support the maintenance actions.

In the operating panels and visual monitors the information is shown with the same symbols and colours. There are clear rules to provide information for the user. E.g. blinking light is used to indicate information that need special attention.

**Adequacy of Verification**

The visual monitors and operating panels provide the operators a holistic view.

**Proposals for Improvement**

No improvement proposals.

**BESEP_HFE_SAA_003:** Relevant information related to the procedures and guides shall be presented for the operators to assess the situation, to see the plant response to actions and to assess the progress of the plant state.

**Summary of the Verification Process**

Process monitoring system provides procedure support displays to support the operators in decision making and monitoring the situation in addition to the control panels in the control rooms. The displays and panels follow the rules given in style guide.

The suitability of the displays and monitors is verified before commissioning.

**Adequacy of Verification**

All new panels and displays are verified to follow the rules given in style guide.

**Proposals for Improvement**

No improvement proposals.

**BESEP_SEP_VV_001:** V&V shall demonstrate that the included areas, spaces, systems, structures and components, manual tasks and organizational conditions are working together as designed and meet the safety requirements set to them.

**Summary of the Verification Process**

The means to cope with LUHS event have evolved during years as knowledge of the hazards leading to LUHS has been improved and the lacks in the procedures have been found out in PSA and/or DSA. All plant modifications have been verified in the design stage with PSA and DSA and the human actions have been taken into account, the reliability part in PSA and the delays etc. in DSA.

The safety requirements have been validated from the PSA (risk distribution, CDF and LERF) and from the DSA (release).

**Adequacy of Verification**

V&V demonstrates that safety requirements from authorities and legislation are met.
Proposals for Improvement
No improvement proposals.

BESEP_SEP_VV_002: *It shall be possible to trace the decisions made based on the results of V&V to safety design and safety requirements.*

Summary of the Verification Process
If there are findings on the design V&V process, the need for design change is evaluated. If a change is needed, then new analyses are conducted for the updated design before manufacturing and commissioning. The change process is documented.

Adequacy of Verification
The change process is documented.

Proposals for Improvement
No improvement proposals.

BESEP_SEP_VV_003: *The procedures and guidelines shall be systematically validated and verified. Validation shall also address the role of human factors in the procedures and the correct signal generation under the conditions of external hazards.*

Summary of the Verification Process
The procedures designed for the event LUHS have been validated according to the normal plant instructions. In the procedure development PSA and DSA results have been used. When the procedure had been drafted, a thermohydraulic analysis (DSA) was conducted to provide evidence on the correctness of the selected strategy. Based on the analysis the procedure was finalised. If had been needed, supporting tests could have been run in the full-scale simulator.

The validation/verification was done in three steps. The validation/verification was done by operators who had not participated in the creation of the procedure. At first the procedure was validated in the full-scale simulator to ensure that the procedure is suitable for use. Then the procedure was validated by reading to ensure, that the level of instructions is correct, the procedure and its usage is clear. Finally the correspondence between the procedure and the plant was evaluated.

Adequacy of Verification
The validation of the procedures for LUHS followed the normal plant instructions.

Proposals for Improvement
No improvement proposals.

BESEP_SEP_VV_004: *In the case of external hazards the NPP shall be safely shut down and kept in a subcritical state, the residual heat removal shall be ensured and the leakages of radioactive substances shall be kept below the specified limits.*

Summary of the Verification Process
Based on the thermohydraulic analysis (DSA) conducted, the NPP can be safely shut down to a subcritical state and kept in it so that the residual heat is removed in case of LUHS. There are no leakages of radioactive substances in this event, thus also these limits for the event are met.

Adequacy of Verification
The analysis conducted show that the NPP can be safely shut down in case of LUHS.
Proposals for Improvement
No improvement proposals.

**BESEP_SEP_VV_005: The operability of systems, structures and components shall be demonstrated in their design basis external environmental conditions.**

Summary of the Verification Process

The SSC existing in the NPP is classified to their design basis environmental conditions. According to the analysis conducted (PRA, DSA) the LUHS event does not provide environmental conditions exceeding the design basis conditions.

Adequacy of Verification

The requirement is fulfilled.

Proposals for Improvement

No improvement proposals.

D.2.2 The key features of verification process for LUHS_2

**BESEP_DSA_FSEP_001: The safety systems, structures and components, including auxiliary or supporting systems thereof, shall be protected from interaction with failed systems, structures or components as far as reasonably practicable.**

Summary of the Verification Process

In the case study the finite elements calculation models were used in ANSYS code to analyse the impact the extremely low temperatures on the essential SWS (Service Water System). Loss of SWS leads to loss of cooling for AFWS (Auxiliary Feedwater System) and primary feed and bleed. Initiating event occurs due to loss of main coolant pumps (MCP) cooled by SWS. However, the residual heat removal can be performed using EFWS (Emergency Feedwater System) and mobile source to supply SGs. There are impacts on DiD (Defence-in-Depth). Changes in the level of redundancy occur for residual heat removal. New CCFs arise, etc. Control of accidents within the design basis (level 3 of DiD) is partially degraded.

Adequacy of Verification

The verification is adequate in the case study. It is shown that there is no impact on the other DiD levels. All safety functions can be performed to control the accident within the design basis. Initiating event occurs and the residual heat removal is partially impacted.

Proposals for Improvement

Fulfilment of the given requirement is given by the design of the plant. No improvement is needed in the second case study.

**BESEP_DSA_FSEP_002: The safety divisions hosting redundant parts of safety systems shall be located in different buildings or housed in dedicated compartments to separate them from the other safety divisions in the same building in order to prevent faults from spreading from one redundant system part to another as a result of external events.**

Summary of the Verification Process

The redundant parts of safety systems are located in different buildings or compartments. In such a way fault spreading from one system to another is limited. It is resulted from functional and physical separation. Diversity principle is also applied in the plant design. The EFWS is not cooled by SWS. The EFWS tanks are located outside the building, however, they are heated. So, the extremely low temperatures have no impact on the system.
Adequacy of Verification

The verification is adequate. It is shown that there is no impact on the other DiD levels. Control of accidents within the design basis (level 3 of DiD) is only partially degraded.

Proposals for Improvement

Fulfilment of the given requirement is given by the design of the plant. No improvement is needed in the second case study.

**BESEP DSA_FSEP_003: The systems of different safety classes shall be functionally separated so that failure of a system or component of a lower safety class does not affect a function of a higher safety class.**

Summary of the Verification Process

The systems of different safety classes are separated. Failure of a system or component of a lower safety class does not affect a function of a higher safety class. It is exactly given by the design of the plant.

Adequacy of Verification

The verification is adequate. It is shown that there is no impact on the other DiD levels. Control of accidents within the design basis (level 3 of DiD) is partially degraded.

Proposals for Improvement

Fulfilment of the given requirement is given by the design of the plant. No improvement is needed in the second case study.

**BESEP PSA_ALSF_001: The potential losses of safety functions shall be evaluated based on the resistance of NPP against the hazards, taking into consideration real status of all systems, structures and components relevant to nuclear safety.**

Summary of the Verification Process

PSA evaluates the DID and SM impacts. The results have shown us that the extremely low temperatures result in degraded DID and SM. The benefit of the PSA insights is to show, that the safety function (residual heat removal) is degraded and partially lost, but the impact of extremely low temperature on the plant risk is negligible

Adequacy of Verification

The core damage frequency due to extremely low temperature is 9.95E-10/year. This event can be practically eliminated (the requirement of the Slovak Nuclear Regulatory Authority is that the practically eliminated event frequency < 1.0E-7/y). So, LERF is not calculated. Adequacy of verification is confirmed.

Proposals for Improvement

The real status of all systems, structures and components relevant to nuclear safety are taken into consideration within the risk calculation. Fulfilment of the given requirement is adequate.

**BESEP PSA_ALSF_002: Complex failure combinations of systems, structures and components initiated by external hazards shall be identified and their significance to nuclear safety shall be evaluated.**

Summary of the Verification Process

Minimal cut sets are identified and CDF is calculated (see the response to the requirement No. 4 presented above). Given the initiating event (trip of all MCPs), the reactor trip occurs, the residual heat is removed and the safe cooling down of the plant is achieved.

Adequacy of Verification
Adequate PSA approach for external events is used based on the applicable safety standards and guidelines.

Proposals for Improvement

The PSA results have shown us that the extremely low temperatures have no significance to nuclear safety. No proposal for improvement is needed.

**BESEP_PSA_ALSF_003: The important functional dependencies on physical location and from operation, maintenance and the effects of human activities shall be considered in assessing the potential losses of safety functions.**

Summary of the Verification Process

Relevant areas included in the PSA model are changes in the level of redundancy, new common-cause failure mechanisms and dependencies and changes in the existing common-cause failure probabilities. Extremely low temperatures affect adversely the environment in which the plant personnel must perform their actions. New operator actions are created, some actions are eliminated, new dependencies are among operator actions.

**Adequacy of Verification**

Adequate PSA approach for external events is used based on the applicable safety standards and guidelines.

**Proposals for Improvement**

Important functional dependencies from operation, maintenance and the effects of human activities are considered in assessing the risk. No proposal for improvement is needed.

**BESEP_HFE_SAA_001: The design of user interfaces in NPP shall support the operators in assessing any normal and abnormal situation so that they can perceive the situation, comprehend it and finally anticipate the future status of the event.**

Summary of the Verification Process

Extremely low temperature affects adversely the environment in which the plant personnel must perform their actions. As it is described above, new operator actions are created, some actions are eliminated, new dependencies are among operator actions. The impact is significant on the human performance in case of using the mobile source to supply feedwater for the SGs.

**Adequacy of Verification**

Adequate PSA approach for external events is used based on the applicable safety standards and guidelines.

**Proposals for Improvement**

The design of the plant supports the personnel in assessing abnormal and accident situation. So, they can perceive the situation and anticipate the future status of the plant. No proposal for improvement is needed.

**BESEP_HFE_SAA_002: The visual monitors or operating panels shall provide the operators a holistic view on the plant state and feedback from the course of event and effects from activations and passive or automatic functions.**

Summary of the Verification Process

HRA is performed within the PSA and the human – machine interaction is evaluated and implemented into the model. They are the external events response actions which are new post-initiating event operator actions used to mitigate the effects of an external event. This category of HEs is typically not included in the EOPs network of procedures. These operator actions are identified by review of the external event response procedures in conjunction with the modeled PSA functions and sequences. Response actions consist of the following types of actions:
1. Terminating the impact of the external initiating event - actions taken to identify and protect components that are operating in an undesired state or are threatened after the external event has occurred.
2. Mitigation of external initiating event consequences - actions taken to recover failed SSCs by providing an alternate success path or mitigation of external initiating event consequences using alternate components - actions taken to recover failed SSCs by providing an alternate success path. For example, restoration of feedwater supply using the mobile source. Note that human reliability analysis does not address repair of failed components.

Adequacy of Verification

Adequate PSA approach for external events is used based on the applicable safety standards and guidelines.

Proposals for Improvement

The human-machine interaction of the plant provides the personnel a realistic view on the plant state and feedback from the course of event and effects from activations and passive or automatic functions. No proposal for improvement is needed.

BESEP_HFE_SAA_003: Relevant information related to the procedures and guides shall be presented for the operators to assess the situation, to see the plant response to actions and to assess the progress of the plant state.

Summary of the Verification Process

HRA is performed within the PSA and the human – machine interaction is evaluated and implemented into the model. These external events operator actions are identified by review of the external event response procedures in conjunction with the modeled PSA functions and sequences.

Adequacy of Verification

Adequate PSA approach for external events is used based on the applicable safety standards and guidelines.

Proposals for Improvement

The external event response procedures are available for the personnel to assess the situation, to see the plant response to actions and to assess the progress of the plant state. No proposal for improvement is needed.

BESEP_SEP_VV_001: V&V shall demonstrate that the included areas, spaces, systems, structures and components, manual tasks and organizational conditions are working together as designed and meet the safety requirements set to them.

Summary of the Verification Process

The PSA is used to show that SSCs and HFE are working together as it is required. Prior to performing the qualitative analysis in HRA, if operator action did not pass the screening-level feasibility assessment, the feasibility should be reassessed after gathering more details. The feasibility assessment is, at a minimum, made up of the following:

1. timing,
2. manpower,
3. cues,
4. procedures and training,
5. accessible location and environmental factors, and
6. tools and equipment operability.

If operator action is feasible, the analyst can proceed to perform either a screening or a detailed quantification. If the analyst finds the screening to be too conservative or limiting, the analyst is encouraged to apply the detailed HRA method. In the second case study only detailed analysis of HEs are performed.
Adequacy of Verification

Adequate PSA approach for external events is used based on the applicable safety standards and guidelines.

Proposals for Improvement

SSCs, the personnel and organizational conditions are working together as designed and meet the safety requirements set to them. No proposal for improvement is needed.

**BESEP_SEP_VV_002:** *It shall be possible to trace the decisions made based on the results of V&V to safety design and safety requirements.*

Summary of the Verification Process

PSA allows to trace the decisions made on the basis of V&V to safety design and requirements.

Adequacy of Verification

Adequate PSA approach for external events is used based on the applicable safety standards and guidelines.

Proposals for Improvement

In this area no improvement is needed.

**BESEP_SEP_VV_003:** *The procedures and guidelines shall be systematically validated and verified. Validation shall also address the role of human factors in the procedures and the correct signal generation under the conditions of external hazards.*

Summary of the Verification Process

EOPs and SAMGs are systematically validated. Validation also involves the role of human factors under the conditions of external hazards. These human actions are described in the external event procedures of the plant.

Adequacy of Verification

Validation of human actions involved in different plant procedures is performed using the plant simulator. This is the way to perform an adequate verification of the safe plant design and validity of the safety requirements.

Proposals for Improvement

Validation of procedures involves also the role of human factors in the procedures and the correct signal generation under the conditions of external hazards. No improvement is needed.

**BESEP_SEP_VV_004:** *In the case of external hazards the NPP shall be safely shut down and kept in a subcritical state, the residual heat removal shall be ensured and the leakages of radioactive substances shall be kept below the specified limits.*

Summary of the Verification Process

The PSA results have shown negligible level of the risk. So, the plant will be safely shutdown and kept in subcritical state, the residual heat is removed and the release of radioactive substances will be kept below the specified limits.

Adequacy of Verification

Adequate PSA approach for external events is used based on the applicable safety standards and guidelines.

Proposals for Improvement

The PSA results have shown that the NPP shall be safely shut down and kept in a subcritical state. Therefore, no improvement is needed.
BESEP_SEP_VV_005: The operability of systems, structures and components shall be demonstrated in their design basis external environmental conditions.

Summary of the Verification Process

DSA results have shown us that SSCs are able to withstand the design basis external events. HCLPFs (high confidence of low probability of failure) are calculated to demonstrate it.

Adequacy of Verification

Adequate DSA approach for external events is used. The CDFM (conservative deterministic failure margin) approach is used to confirm the design basis values. Input parameters for calculation are provided by applications of finite elements methods (FEM) in ANSYS code.

Proposals for Improvement

The operability of SSCs is demonstrated by deterministic structural analyses for extreme external environmental conditions. Therefore, no improvement is needed.

D.2.3 The key features of verification process for LUHS_3

BESEP_DSA_FSEP_001: The safety systems, structures and components, including auxiliary or supporting systems thereof, shall be protected from interaction with failed systems, structures or components as far as reasonably practicable.

Summary of the Verification Process

Within event class DBA the credited action is manual opening of recirculation of heated outlet water at indication in MCR of low water temperature at the outer strainers. Since the heated water is provided in between the strictly mechanical outer strainers and the automated inner strainers there are no dependencies between the involved SSCs. Verification of the requirement were performed only by qualitative reasoning and reference to amount of heated water and the capacity of the automated cleaning of inner strainers.

Within the event category DEC-A and sub category “Special Events”, the case of complete loss of ultimate heat sink is included, event LUHS, by inclusion in the more severe event of Extended Loss of AC Power, ELAP, which is motivated by that LUHS will eventually result in the same event sequence as ELAP, but has a slower progression. Verification of the requirement is performed by proving the structural and functional independence of SSCs belonging to the independent core cooling function, both from ordinary safety functions and from the screening plant, e.g. the independent core cooling system is housed in a separate building and residual heat removal performed with the filtered pressure relief system is independent of cooling and the screening plant.

Adequacy of Verification

The requirement verification is based on qualitative reasoning and references design documentation and proofs of separation and independence. The methods used is seen as satisfactory.

Proposals for Improvement

Proof of independence could be complemented with input from the PSA, e.g. by performing a Safe Shutdown Analysis.

BESEP_DSA_FSEP_002: The safety divisions hosting redundant parts of safety systems shall be located in different buildings or housed in dedicated compartments to separate them from the other safety divisions in the same building in order to prevent faults from spreading from one redundant system part to another as a result of external events.

Summary of the Verification Process
Within event class DBA the credited action is manual opening of recirculation of heated outlet water at indication in MCR of low water temperature at the outer strainers. The inlet and the outlet channels are connected by the recirculation channel, but since the water of the outlet channel is heated there is no risk for the external event of frazil ice to affect the recirculation function.

Within the event category DEC-A and sub category “Special Events”, the case of complete loss of ultimate heat sink is included, event LUHS, by inclusion in the more severe event of Extended Loss of AC Power, ELAP, which is motivated by that LUHS will eventually result in the same event sequence as ELAP, but has a slower progression. Verification of the requirement is performed by proving the structural and functional independence of SSCs belonging to the independent core cooling function, both from ordinary safety functions and from the screening plant, e.g. the independent core cooling system is housed in a separate building and residual heat removal performed with the filtered pressure relief system is independent of cooling and the screening plant.

**Adequacy of Verification**

The requirement verification is based on qualitative reasoning and references design documentation and proofs of separation. The methods used is seen as satisfactory.

**Proposals for Improvement**

Proof of separation could be complemented with input from the PSA, e.g. by performing a Safe Shutdown Analysis.

**BESEP_DSA_FSEP_003**: The systems of different safety classes shall be functionally separated so that failure of a system or component of a lower safety class does not affect a function of a higher safety class.

See requirement BESEP_DSA_FSEP_002.

**BESEP_PSA_ALSF_001**: The potential losses of safety functions shall be evaluated based on the resistance of NPP against the hazards, taking into consideration real status of all systems, structures and components relevant to nuclear safety.

**Summary of the Verification Process**

The effect of the event frazil ice, and other phenomena that can affect the screening plant, on relevant SSCs was identified by plant response analysis and evaluated in the PRA (see the detailed case study description). The evaluations considered both FLEX actions for recovery of cooling of emergency diesel generators and manual start of the retro-fitted independent core cooling system. Special emphasis was put on the analysis of accident prevention and mitigation strategies in case of loss of SWS. Initially the activity evaluated different conceptual FLEX strategies in order to identify, by use of PRA importance measures, the most efficient strategies. From the PRA were also the need for additions to existing, or the need for new, procedures identified. The final set of strategies was implemented in the PRA considering both new mobile equipment and corresponding manual actions and routines. The PRA was also developed with new time windows in order to address timing issues realistically.

**Adequacy of Verification**

The verification was performed considering both existing and new SSCs, including post-Fukushima stress test developed FLEX strategies. The PRA was also used for improving routines and procedures and to evaluate the risk importance of different possible FLEX strategies. The verification can hence be seen as adequate.

**Proposals for Improvement**

Failure data for FLEX equipment and probabilities for FLEX human actions were estimated based on generic information and data and screening values were adapted. Even though sensitivity analyses were performed, the verification should be performed with site-specific data when such is available.
**BESEP_PSA_ALSF_002: Complex failure combinations of systems, structures and components initiated by external hazards shall be identified and their significance to nuclear safety shall be evaluated.**

Summary of the Verification Process

The effect of the event frazil ice, and other phenomena that can affect the screening plant, on relevant SSCs was identified by plant response analysis and evaluated in the PRA (see the detailed case study description). The evaluations considered both FLEX actions for recovery of cooling of emergency diesel generators and manual start of the retro-fitted independent core cooling system. Special emphasis was put on the analysis of accident prevention and mitigation strategies in case of loss of SWS. Initially the activity evaluated different conceptual FLEX strategies in order to identify, by use of PRA importance measures, the most efficient strategies. From the PRA were also the need for additions to existing, or the need for new, procedures identified. The final set of strategies was implemented in the PRA considering both new mobile equipment and corresponding manual actions and routines. The PRA was also developed with new time windows in order to address timing issues realistically.

Adequacy of Verification

The verification was performed considering both existing and new SSCs, including post-Fukushima stress test developed FLEX strategies. The PRA was also used for improving routines and procedures and to evaluate the risk importance of different possible FLEX strategies. The verification can hence be seen as adequate.

Proposals for Improvement

The PRA assumes LOOP at the event due to rapid shutdown of more than one NPP, which leads to an overestimate of the importance of the sequence. Further development of the initial sequence progression with regard to time dependencies between shutdown of the first and second power plant could be beneficial for the verification process, since this might show that the probability for simultaneous LUHS and LOOP is insignificant.

**BESEP_PSA_ALSF_003: The important functional dependencies on physical location and from operation, maintenance and the effects of human activities shall be considered in assessing the potential losses of safety functions.**

Summary of the verification process

The effect of the event frazil ice, and other phenomena that can affect the screening plant, on relevant SSCs was identified by plant response analysis and evaluated in the PRA (see the detailed case study description). The evaluations considered both FLEX actions for recovery of cooling of emergency diesel generators and manual start of the retro-fitted independent core cooling system. The physical location of recirculation channels was considered in the plant response analysis, and all related and relevant human actions was included in the PRA.

Adequacy of verification

The verification process considered all relevant dependencies and manual actions for 24 hours in the normal PRA. For the DEC event of LUHS an additional reliability analysis was performed to verify the function for 72 hours, where additional failure modes and mitigation actions was considered. The verification process is seen to be adequate.

Proposals for improvement

The process did not consider repair of failed equipment at long time windows, which would improve the realism of the analysis and possibly show larger safety margins. The state of the art HRA methods does not take credit for long grace times, which leads to conservative failure probabilities for manual actions.

**BESEP_HFE_SAA_001: The design of user interfaces in NPP shall support the operators in assessing any normal and abnormal situation so that they can perceive the situation, comprehend it and finally anticipate the future status of the event.**
Summary of the verification process

Within event class DBA the credited action is manual opening of recirculation of heated outlet water at indication in MCR of low water temperature at the outer strainers. The verification process included testing of the technical function of the recirculation in accordance with the instructions for manoeuvring. The communication between MCR and the technician tasked with manoeuvring the hatch where the position of the hatch shall coincide with the temperature readings in MCR for the inlet is verified. For the operators to comprehend and anticipate the future status of the event information regarding the functionality of the hatch and the reliability of the temperature sensors are vital. The seasonal variation in water temperature that normally occurs at the NPP constitutes an annual verification of the functionality of the hatch at the time that the water temperature undergoes a limit value. The reliability of the temperature sensors is verified during prolonged events where the water temperature is low. The operators manually check the water temperature and if needed recalibrate the temperature sensors.

For the DEC event of LUHS the operators are reminded in the procedures for the DBA event of preparing for an eventual LUHS case. This reminder instructs the operators to prepare by ensuring that staff and the proper instructions are available. The design of the user interfaces has been verified through iterative reviews where requirements for the design have had input from operational experience, human factors specialists and safety analyses. The verification is also based on NUREG 0700 and philosophies for the design of central and local control rooms at the NPP. The verification has also included task analyses and scenario-based testing in simulator and 3D models.

Adequacy of verification

The verification is seen as adequate. It is verified that the operators are notified of the screening plant status. The verification is also performed to ensure that the changes in the design are implemented in accordance with the design requirements for the control rooms.

Proposals for improvement

- 

BESEP_HFE_SAA_002: The visual monitors or operating panels shall provide the operators a holistic view on the plant state and feedback from the course of event and effects from activations and passive or automatic functions.

Summary of the verification process

When operating the recirculation hatch the feedback needed to assess the effect from activation is given by the temperature indicator. For the DEC event of LUHS the ICCS is initiated and information regarding the start, regulation, and monitoring is presented in a separate view. The parameters for assessing the plant state and assessing feedback from the course of event and effects from activations and passive or automatic functions are decided by DSA. The verification is performed based on philosophies for the design and operation of central and local control rooms at the NPP and operational experience.

Adequacy of verification

The verification process considers all aspects of the operators needs to be able to assess the plant state and feedback from the course of event through parameters decided by the DSA.

Proposals for improvement

- 

BESEP_HFE_SAA_003: Relevant information related to the procedures and guides shall be presented for the operators to assess the situation, to see the plant response to actions and to assess the progress of the plant state.

See requirements BESEP_HFE_SAA_001 and BESEP_HFE_SAA_002.
BESEP_SEP_VV_001: V&V shall demonstrate that the included areas, spaces, systems, structures and components, manual tasks and organizational conditions are working together as designed and meet the safety requirements set to them.

See requirement BESEP_SEP_VV_004.

BESEP_SEP_VV_002: It shall be possible to trace the decisions made based on the results of V&V to safety design and safety requirements.

Summary of the verification process
Not possible to evaluate within BESEP.

Adequacy of verification
Not possible to evaluate within BESEP.

Proposals for improvement
Not possible to evaluate within BESEP.

BESEP_SEP_VV_003: The procedures and guidelines shall be systematically validated and verified. Validation shall also address the role of human factors in the procedures and the correct signal generation under the conditions of external hazards.

Summary of the verification process
The requirement was verified through the combined evidence of performed deterministic and probabilistic safety analyses and human factors activities.

The PSA performed covered all relevant manual actions including FLEX actions. HRA were performed for manual actions based on existing and newly developed procedures. Initially different conceptual FLEX strategies were evaluated by use of PSA importance measures in order to identify the most efficient strategies. From the PSA were also the need for additions to existing, or the need for new, procedures identified. The final set of strategies was implemented in the PSA considering both new mobile equipment and corresponding manual actions and routines.

Procedures for the credited manual actions were developed based on input from both the PSA (HRA) and the DSA, e.g. dependencies to other actions, timing requirements, training requirements, integration into existing emergency operating procedures, and general factors which would increase the probability of success. All new procedures on use of FLEX equipment were subject to hands-on tests at site, results evaluation and experience feedback for improvement of the procedures.

Adequacy of verification
Verification was performed thru dynamic interaction between mainly PSA and HF activities. Separate coordination activities were deployed in order to ensure satisfying flow of information and identification of dependencies between the different activities. All developed procedures were validated by means of testing.

Proposals for improvement
-

BESEP_SEP_VV_004: In the case of external hazards the NPP shall be safely shut down and kept in a subcritical state, the residual heat removal shall be ensured and the leakages of radioactive substances shall be kept below the specified limits.

Summary of the verification process
The requirement was verified through the combined evidence of performed deterministic and probabilistic safety analyses and human factors activities.
In the deterministic safety analysis it is demonstrated that the plant can cope with the DBA event of frazil ice through use of the recirculation function in combination with manual actions to minimise the expenditure of cooling capacity. These actions ensure sufficient cooling of emergency diesel generators, core cooling pumps and condensation pool, and hence that subcritical state will be reached. The conditions of the more severe event of complete loss of ultimate heat sink, LUHS, is proven to be met by start of the retro-fitted independent core cooling system with residual heat removal performed by filtered venting. The verification process included heat transfer calculations to demonstrate that the NPSH of the pumps of the ordinary residual heat removal system is sufficient for the high temperatures given by filtered venting, and that cold shutdown hence can be reached after 72 hours once ordinary residual heat removal system has been restored. It was also shown that there is sufficient water volume available for 72 hours operation of the independent core cooling system, given implemented procedures for manual refill of water from the demineralized water storage tank after 24 hours. The event classification was based on probabilistic estimation of the frequency of the LUHS event.

The PSA performed covered all relevant dependencies and failure combinations with respect to the event of frazil ice. Probability distributions for water temperatures below 0 degrees Celsius in combination with on-shore windspeeds higher than 10 m/s was considered. The PSA considered all relevant FLEX actions and HRA were performed for manual actions based on existing and newly developed procedures. The PSA was performed with the mission time of 24 hours for level 1 and 48 hours for level 2 with safe and stable state defined as warm or cold shutdown. In addition to the PSA a separate reliability analysis of the independent core cooling system was performed for an operating time of 72 hours in order to prove that reliability requirements were met in the long term.

Procedures for the credited manual actions were developed based on input from both the PSA (HRA) and the DSA, e.g. dependencies to other actions, timing requirements, training requirements, integration into existing emergency operating procedures, and general factors which would increase the probability of success. All new procedures on use of FLEX equipment were subject to hands-on tests at site, results evaluation and experience feed-back for improvement of the procedures.

Separate coordination activities were deployed in order to ensure satisfying flow of information and identification of dependencies between the different activities of PSA, DSA and human factors.

**Adequacy of verification**

The verification is seen as adequate. Performed safety analyses showed that subcritical condition can be reached with sufficient reliability.

**Proposals for improvement**

Verification of possibilities for restoring/repairing ordinary residual heat removal system were not performed. The PSA did not cover the transition from warm to cold shutdown in sequences with residual heat removal by filtered venting.

**BESEP_SEP_VV_005: The operability of systems, structures and components shall be demonstrated in their design basis external environmental conditions.**

See requirement BESEP_SEP_VV_004.

**D.2.4 The key features of verification process for LUHS_4**

**BESEP_DSA_FSEP_001: The safety systems, structures and components, including auxiliary or supporting systems thereof, shall be protected from interaction with failed systems, structures or components as far as reasonably practicable.**

**Summary of the Verification Process**

Based on the post-Fukushima stress test for the NPP, 9 safety measures were implemented to cope with loss of ultimate heat sink situations. The implemented safety measures aim at utilizing plant equipment not affected by river contamination. Initially, the removal of the water intake filters was also considered as a candidate
measure to handle such an event by trying to use contaminated water for cooling purposes with the cooling system of the NPP; however, this option was dismissed.

Adequacy of Verification

Dedicated safety measures were implemented in order to ensure efficient accident mitigation in loss of ultimate heat sink situations. These measures include the application of portable equipment and the support of the on-site fire brigade that may be regarded as a widely accepted approach in the post-Fukushima era. Hence, it can be concluded that the fulfilment of the given requirement can be considered as complete with good technical quality.

Proposals for Improvement

Although the implemented measures have proven to be technically adequate and efficient for accident mitigation purposes, installation of independent, stationary diesel generators to provide power supply to the well station pumps is seen as a most effective measure for safety enhancement.

BESEP_DSA_FSEP_002: The safety divisions hosting redundant parts of safety systems shall be located in different buildings or housed in dedicated compartments to separate them from the other safety divisions in the same building in order to prevent faults from spreading from one redundant system part to another as a result of external events.

Not evaluated.

BESEP_DSA_FSEP_003: The systems of different safety classes shall be functionally separated so that failure of a system or component of a lower safety class does not affect a function of a higher safety class.

Summary of the Verification Process

Plant response analysis was performed to identify the mitigation systems that can be relied upon and the measures to be applied in case of loss of ESWS. The safety class of all the mobile equipment used by the on-site fire brigade of the NPP is lower than the safety classes of the emergency and auxiliary emergency feed water system (safety class 3). The two types of systems share some short common pipelines (e.g. the headers of the auxiliary emergency feed water system). However, despite these common parts, it can be stated that these systems are separated physically so that the failure of the mobile equipment do not have any adverse effects on the operation of the emergency and the auxiliary emergency feed water system.

Adequacy of Verification

The verification process can be regarded as adequate, the separation of the systems of different safety classes is ensured as far as reasonably practicable so that the failure of a system or component of a lower safety class does not affect a function of a higher safety class.

Proposals for Improvement

No proposal for improvement was identified in the verification process of this requirement.

BESEP_PSA_ALSF_001: The potential losses of safety functions shall be evaluated based on the resistance of NPP against the hazards, taking into consideration real status of all systems, structures and components relevant to nuclear safety.

Summary of the Verification Process

Plant response analysis as well as risk assessment were performed for events that can cause loss of the ultimate heat sink due to the discharge of dangerous substances into the river. All the plant modifications implemented on the basis of the conclusions of the stress test of the plant were considered in these analyses. Special emphasis was put on the analysis of accident prevention and mitigation strategies in case of loss of ESWS. The core damage risk attributable to external events endangering water intake was quantified and the main risk contributors were identified.
Adequacy of Verification

The potential loss of a safety function was evaluated by using risk assessment and considering all the systems, including portable equipment, that may serve the purposes of accident mitigation in the event of loss of ultimate heat sink. The use of portable equipment recently made available at the NPP was modelled by applying state-of-practice approaches. Consequently, it can be concluded that the fulfilment of the given requirement may be regarded as complete with high technical quality.

Proposals for Improvement

It was found that the existing PSA data was not applicable to the pumps of the well station at the Danube bank, the diesel driven firewater pumps, the mobile fire-fighting pumps and the diesel generators used for severe accident management. Plant specific reliability data should be collected and evaluated for these components and the reliability parameters taken from international databases should be updated by using plant specific information.

BESEP_PSA_ALSF_002: Complex failure combinations of systems, structures and components initiated by external hazards shall be identified and their significance to nuclear safety shall be evaluated.

Summary of the Verification Process

Risk assessment was performed for events that can cause loss of the ultimate heat sink due to the discharge of dangerous substances into the river. The core damage risk attributable to external events endangering water intake was quantified and the main risk contributors were identified. In accordance with the nature of PSA, the development of accident sequences that can be initiated by the analysed riverine events covered the identification and probabilistic modelling of a broad range of complex failure combinations of systems, structures and components.

Adequacy of Verification

The total loss of the ultimate heat sink can be regarded as complex failure combinations of systems. The LUHS due to external events related to river contamination was identified and the risk attributable thereto was assessed. In summary, it can be concluded that the fulfilment of the requirement in question can be considered as complete with good technical quality in terms of river contaminations.

Proposals for Improvement

Various follow-on analyses and actions are seen necessary to enable a more accurate assessment of the loss of ultimate heat sink potential and an adequate treatment of the consequences of endangering events. The scope of the endangering events that should be subject to detailed risk assessment has to be reviewed after performing the proposed further analyses.

BESEP_PSA_ALSF_003: The important functional dependencies on physical location and from operation, maintenance and the effects of human activities shall be considered in assessing the potential losses of safety functions.

Summary of the Verification Process

HRA within the PSA for external events endangering water intake from the river at the NPP was aimed at identifying and quantifying of those safety significant human failure events that can take place either prior to a plant disturbance or during evolution of an accident. Beyond human actions already modelled in the internal events PSA, eight human actions were identified and the failures to take these actions were newly introduced into the model (besides “recovery from loss of ESWS”). The dependence between the different human actions was also studied (e.g. commonalities or similarities in crew members, operating procedures and human-machine interface) and considered during the introduction of the human failure events and the corresponding human error probabilities into the PSA model.

Adequacy of Verification
With respect to addressing important functional dependencies, the assessment on potential losses of safety functions focused primarily on the dependencies between the effects of human activities. Consideration of all other types of functional dependencies were self-evident, e.g. simultaneous loss of all ESWS, condenser and technological cooling water system trains due to their same physical location. In summary, it can be concluded that the fulfilment of the requirement in question can be regarded as complete with good technical quality.

Proposals for Improvement

The modelling of functional dependencies between human actions was primarily based on expert judgement aimed at avoiding the use of optimistic assumptions. Hence, the assessment may be regarded as rather conservative. Some sensitivity assessment would help to understand the impact of these conservative assumptions on the risk results and the associated conclusions that can be drawn from the analysis.

**BESEP_HFE_SAA_001:** The design of user interfaces in NPP shall support the operators in assessing any normal and abnormal situation so that they can perceive the situation, comprehend it and finally anticipate the future status of the event.

Not evaluated.

**BESEP_HFE_SAA_002:** The visual monitors or operating panels shall provide the operators a holistic view on the plant state and feedback from the course of event and effects from activations and passive or automatic functions.

Not evaluated.

**BESEP_HFE_SAA_003:** Relevant information related to the procedures and guides shall be presented for the operators to assess the situation, to see the plant response to actions and to assess the progress of the plant state.

Summary of the Verification Process

The use of plant systems and components to cope with a loss of ultimate heat sink situation induced by river contamination is described only at a high level in the emergency operating procedures and in the severe accident management guidelines. System specific as well as other types of plant operating procedures provide more detailed guidance on how to tackle such situations. Several measures were aimed at providing supplements or making improvements to these procedures.

Adequacy of Verification

The necessary actions that should be taken to efficiently cope with a loss of ultimate heat sink situation have been specified in plant operating procedures. Hence, it can be concluded that the fulfilment of the given requirement may be regarded as complete with sufficiently high technical quality in terms the relevant operating procedures.

Proposals for Improvement

The symptom-oriented emergency operating procedures in use at the plant do not include the strategy and the associated instructions for secondary side cooling by the use of the fire water system in sufficient details. It appears advisable to set up an operational and transient mitigation strategy and specify the corresponding sequences of actions needed to be taken in case of river contamination.

**BESEP_SEP_VV_001:** V&V shall demonstrate that the included areas, spaces, systems, structures and components, manual tasks and organizational conditions are working together as designed and meet the safety requirements set to them.

Summary of the Verification Process

The on-site fire brigade of the NPP performed extensive tests in order to verify the feasibility of implementing the external injection paths from the river to the auxiliary emergency feed water system using fire hoses and
mobile pumps. The injection path was established between the cooling water channel and the existing connection points in the plant yard area to the auxiliary emergency feed water system. These tests also served the purposes of training the concerned plant personnel on the implementation of the required emergency operations.

**Adequacy of Verification**

On the basis of the abovementioned tests and training sessions, it was properly demonstrated that the included areas, spaces, systems, structures and components, manual tasks and organizational conditions are working together as designed and meet the safety requirements set to them.

**Proposals for Improvement**

To ensure a full scope verification and validation of the capabilities of the mobile equipment and the permeability of the pipelines to the auxiliary emergency feed water system, the full path should be tested, instead of checking the fulfillment of required operational conditions up to the existing connection points in the plant yard area only.

**BESEP_SEP_VV_002: It shall be possible to trace the decisions made based on the results of V&V to safety design and safety requirements.**

Not evaluated.

**BESEP_SEP_VV_003: The procedures and guidelines shall be systematically validated and verified. Validation shall also address the role of human factors in the procedures and the correct signal generation under the conditions of external hazards.**

**Summary of the Verification Process**

The use of plant systems and components to cope with a loss of ultimate heat sink situation induced by river contamination is described only at a high level in the emergency operating procedures and in the severe accident management guidelines. System specific as well as other types of plant operating procedures provide more detailed guidance on how to tackle such situations. Several measures were aimed at providing supplements or making improvements to these procedures. The test and training programs reinforce the validation and verification of the relevant procedures and guidelines.

**Adequacy of Verification**

It can be concluded that the relevant procedures and guidelines have been systematically validated and verified during their review and improvement, as well as in the related test and training programs. This validation also addresses the role of human factors in the procedures.

**Proposals for Improvement**

No proposal for improvement was identified in the verification process of this requirement.

**BESEP_SEP_VV_004: In the case of external hazards the NPP shall be safely shut down and kept in a subcritical state, the residual heat removal shall be ensured and the leakages of radioactive substances shall be kept below the specified limits.**

**Summary of the Verification Process**

It could be assumed that all water intake filters would be blocked shortly after one another in case of a harmful riverine event. Loss of ESWS requires reactor shutdown according to the operational limits and conditions. It was conservatively assumed in the analysis that simultaneous shutdown of all four units would induce loss of off-site power that could presumably be recovered within a couple of hours at maximum. If recovery of off-site power is successful, then the emergency and auxiliary emergency feed water systems can ensure residual heat removal until the demineralized water sources are used up in open loop heat removal. It was justified that the capacity of the fire water system is sufficient to provide the minimum necessary amount of cooling water for all the units.
Adequacy of Verification

According to the results of the plant response analysis summarized above, even though portable equipment should be utilized and support from the on-site fire brigade is necessary to efficiently establish a safe state, it can be concluded that the fulfillment of the given requirement may be regarded as complete with good technical quality.

Proposals for Improvement

Although the implemented measures have proven to be technically adequate and efficient for accident mitigation purposes, installation of independent, stationary diesel generators to provide power supply to the well station pumps is seen as a most effective measure for safety enhancement.

**BESEP_SEP_VV_005: The operability of systems, structures and components shall be demonstrated in their design basis external environmental conditions.**

Summary of the Verification Process

The verification process presented for requirement BESEP_SEP_VV_001 above is fully applicable to this requirement too.

Adequacy of Verification

On the basis of the tests and training sessions described in relation to requirement BESEP_SEP_VV_001, it was adequately demonstrated that the relevant systems and components are operable in their design basis external conditions too, with respect of riverine events.

Proposals for Improvement

The proposal for improvement presented in the context of requirement BESEP_SEP_VV_001 above is fully applicable to this requirement too.

D.2.5 Comparison of the key features

Comparison of the verification and justification of the requirements in and between cases is provided in Table D.1.

For the requirements related to the DSA topic *Functional separation to provide defence against failure propagation*, all case studies show that the NPP can be brought into a safe state without reaching the allowed regulatory limits. There exist some deficiencies in physical separation, but diverse means are available. Analyses provide evidence on staying within the allowed regulatory limits. The verification of the requirement fulfillment is seen adequate in all case studies. For improvement there are some proposals, both the NPP design and the verification methods could be improved in the areas of SSC interaction prevention and physical separation. Method improvement could be implemented for all topic requirements by complementing the proof of independence with input from the PSA.

For the requirements related to the PSA topic *Assessment of potential losses of safety functions* plant response analyses and safety margin analyses have been conducted. Also, PRA development with new time windows provided evidence on the potential losses of safety functions and SSCs in a longer run. Plant response analysis, quantification of relevant human actions, designed and statistical failure dependencies are examples of analyses conducted for the assessment of potential losses. The potential losses of safety functions and SSCs and the complex failure combinations have been adequately evaluated, and the use of additional equipment have been modelled by applying good practice. All relevant dependencies have been evaluated to be included in the verification of the case studies. Improvement in the verification would be reached when site specific data from the commissioned equipment is available. Then the failure calculation and probabilities for human actions should be re-evaluated. Further developing the initial sequence progression focusing on time dependencies as well as several follow-on analyses and actions are seen as possibilities for improvement. Human failure sensitivity studies and partly the human actions during longer time periods would provide some more evidence on verification.
For the requirements related to the HFE topic *Situation awareness and assessment* there are several verification methods used in the case studies. The verification is based on the use of full-scale simulator and 3D-models, task analyses, philosophies for control room design and operational experience. Parameters for assessing the plant state and feedback from the course of event are decided through DSA. They are shown in procedure support displays and control panels, supported by procedures. The verification is seen adequate as the PSA approach for external events has been used. It is also verified that the design of the user interfaces follows the guideline. For improvement it is seen that it would be useful to develop an operational and transient mitigation strategy and specify the corresponding sequences of actions.

For the requirements related to the SEP topic *Verification and validation (V&V) of design* extensive tests were performed in order to verify the feasibility of the implemented safety functions. DSA demonstrated that the plant copes with DBA event. PSA provided evidence on the SSCs operation. There exists also a feedback loop to design from the V&V, and PSA allows to trace the decisions made on the basis of V&V. Tests and training programs as well as the validation procedures provide a systematic validation and verification. Additionally, the role of human factors on manual actions and under the conditions of external hazards has been validated. The adequacy of verification of the requirements is evaluated based on proper demonstration on the basis of tests and training and the fact that safety analyses demonstrate that safe state can be reached with sufficient reliability, so the verification is seen as adequate. Additionally, the design change process is documented, there exist systematic validation procedures available, and also full-scale simulator has been used. Safety analyses demonstrate that safe state can be reached with sufficient reliability. No improvement proposals have been found for two of the five SEP requirements. It would be beneficial to test the full path of operations needed for the initiating event. Both method improvement (PSA for reaching cold shutdown by filtered venting) and plant design improvement (power supply) are seen feasible.
**Table D.1: Fulfilment of BESEP Safety Requirements.**

<table>
<thead>
<tr>
<th>BESEP requirement topic: Functional separation to provide defence against failure propagation (DSA)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>BESEP requirement ID:</strong> BESEP_DSA_FSEP_001</td>
</tr>
<tr>
<td>The safety systems, structures and components, including auxiliary or supporting systems thereof, shall be protected from interaction with failed systems, structures or components as far as reasonably practicable.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Key features of the verification process</th>
<th>LUHS_1</th>
<th>LUHS_2</th>
<th>LUHS_3</th>
<th>LUHS_4</th>
<th>Conclusions</th>
</tr>
</thead>
<tbody>
<tr>
<td>The safety functions designed for LUHS have been verified to withstand the failure propagation as the diverse functions are functionally and by distance separated from the main functions. The verification has been conducted by DSA failure analysis and also with PRA.</td>
<td>The finite elements calculation models were used in ANSYS code to analyse the impact the extremely low temperatures on SWS. Impacts on DID are identified.</td>
<td>The event sequence of LUHS is proven to result in the same event sequence as ELAP, though with slower progression. Verification of structural and functional independency of SSCs belonging to the ICCS.</td>
<td>Implemented safety measures aim at utilizing plant equipment not affected by river contamination.</td>
<td>The case studies show that the NPPs are able to reach safe state in the studied initiating events and they are not challenging the allowed limits.</td>
<td></td>
</tr>
</tbody>
</table>

| Adequacy of Verification | DSA, i.e. failure propagation analysis has been conducted to verify the design and the means to cope the events. | All safety functions can be performed to control the accident within the design basis. There is partial impact only on the residual heat removal. | The requirement verification is based on qualitative reasoning and references design documentation and proofs of separation and independence. The methods used is seen as satisfactory. | Use of portable equipment and the support of the on-site fire brigade can be regarded as a widely accepted approach. | The approaches used in case studies rely on analyses and they are seen adequate. |

| Proposals for Improvement | None. | No improvement is needed. | Proof of independence could be complemented with input from the PSA, e.g. by performing a Safe Shutdown Analysis. | Installation of independent, stationary diesel generators to provide power supply to the well station pumps. | Independence of power supply or the proof of independence could be improved, but otherwise there is no need for |
### LUHS_1

#### BESEP requirement ID: BESEP_DSA_FSEP_002

The safety divisions hosting redundant parts of safety systems shall be located in different buildings or housed in dedicated compartments to separate them from the other safety divisions in the same building in order to prevent faults from spreading from one redundant system part to another as a result of external events.

#### Key features of the verification process

- **The original design of the NPP does not totally comply with the requirement.** For all new installations the separation principle is followed.
- **Functional and physical separation is involved in the design.** Diversity principle is also applied. The EFWS is not cooled by SWS.
- **The event sequence of LUHS is proven to result in the same event sequence as ELAP,** though with slower progression. Verification of structural and functional independency of SSCs belonging to the ICCS.
- **Not evaluated.** In some of the case studies some defects exist in the redundancy separation, but diverse systems are available. Case studies show that the safe state can be reached.

#### Adequacy of Verification

- **DSA, i.e. failure propagation analysis has been conducted to verify the design and the means to cope the events.**
- **The verification is adequate.** It is shown that control of accidents within the design basis (level 3 of DID) is partially degraded.
- **The requirement verification is based on qualitative reasoning and references design documentation and proofs of separation and independence.** The methods used is seen as satisfactory.
- **Not evaluated.** The approaches used in case studies rely on analyses and they are seen adequate.

#### Proposals for Improvement

- **None, as the original design cannot be updated as a whole, only in the partial renewal projects**
- **No improvement is needed.**
- **Proof of independence could be complemented with input from the PSA,**
- **Not evaluated.** Both NPP design and verification methods could be improved in the area of physical separation.

<table>
<thead>
<tr>
<th>LUHS_1</th>
<th>LUHS_2</th>
<th>LUHS_3</th>
<th>LUHS_4</th>
<th>Conclusions</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>improvement in the area of SSC interactions.</td>
</tr>
<tr>
<td>LUHS_1</td>
<td>LUHS_2</td>
<td>LUHS_3</td>
<td>LUHS_4</td>
<td>Conclusions</td>
</tr>
<tr>
<td>--------</td>
<td>--------</td>
<td>--------</td>
<td>--------</td>
<td>-------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**BESEP requirement ID:** BESEP_DSA_FSEP_003

The systems of different safety classes shall be functionally separated so that failure of a system or component of a lower safety class does not affect a function of a higher safety class.

**Key features of the verification process**
- The safety classified systems and components have been functionally separated, also electrically and regarding information processing, from the lower class systems and components.
- The systems of different safety classes are separated. Failure of a system or component of a lower safety class does not affect a function of a higher safety class.

**Adequacy of Verification**
- For renewal projects in the plant the functional separation is verified in DSA. For the existing design the same analysis has been conducted for the systems and safety functions with recognised safety importance, not for the whole plant.
- The verification is adequate. It is shown that control of accidents within the design basis (level 3 of DID) is partially impacted.

**Proposals for Improvement**
- None.
- No improvement is needed.

**BESEP requirement topic:** Assessment of potential losses of safety functions (PSA)

**BESEP requirement ID:** BESEP_PSA_ALSF_001

The safety class of all mobile equipment used by the on-site fire brigade of the NPP is lower than the safety classes of the emergency and auxiliary emergency feed water system (safety class 3).

The case studies show that the NPPs are able to reach safe state in the studied initiating events and they are not challenging the allowed limits.

Separation of the systems of different safety classes is ensured as far as reasonably practicable.

The approaches used in case studies rely on analyses and they are seen adequate.

Proof of independence could be complemented with input from the PSA.
The potential losses of safety functions shall be evaluated based on the resistance of NPP against the hazards, taking into consideration real status of all systems, structures and components relevant to nuclear safety.

| **Key features of the verification process** | **identifier of risky phenomena, screening analysis, threshold and detailed analysis, CDF calculation for weather phenomena** | **PSA evaluates the DID and SM impacts. The results have shown us that the extremely low temperatures result in degraded DID and SM. However, the PSA insights show, that the extremely low temperatures have negligible impact on the plant risk.** | **Plant response analysis identified phenomena that can affect the screening plant. This was evaluated in the PRA. The PRA considered both FLEX actions for recovery of emergency diesel generators and start of the ICCS. Special emphasis was put into prevention and mitigation strategies in case of loss of SWS. The PRA was also developed with new time windows to address timing issues realistically.** | **All the plant modifications implemented on the basis of the conclusions of the stress test of the plant were considered in plant response analysis and risk assessment.** | **Plant response analyses and safety margin analyses have been conducted. Also PRA development with new time windows provided evidence on the losses of safety functions and SSCs.** |
| **Adequacy of Verification** | **The potential losses of safety functions have been adequately evaluated.** | **The core damage frequency due to extremely low temperature is 9.95E-10/year. This event is an practically eliminated event.** | **The verification considered both existing and new SSCs and included post-Fukushima FLEX-strategies. The PRA was used for improving routines and through risk importance evaluate different strategies. The verification is seen as adequate.** | **The use of portable equipment recently made available at the NPP was modelled by applying state-of-practice approaches.** | **The potential losses of safety functions and SSCs have been adequately evaluated, and the use of additional equipment has been modelled by applying good practice.** |
### Proposals for Improvement

<table>
<thead>
<tr>
<th>LUHS_1</th>
<th>LUHS_2</th>
<th>LUHS_3</th>
<th>LUHS_4</th>
<th>Conclusions</th>
</tr>
</thead>
<tbody>
<tr>
<td>None.</td>
<td>No improvement is needed.</td>
<td>Failure data for FLEX equipment and probabilities for human actions should be performed with site specific data when such is available.</td>
<td>Plant specific reliability data should be collected and evaluated, or perform sensitivity studies.</td>
<td>When site specific data from the commissioned equipment is available, failure calculation and probabilities for human actions should be re-evaluated.</td>
</tr>
</tbody>
</table>

**BESEP requirement ID:** BESEP_PSA_ALSF_002

Complex failure combinations of systems, structures and components initiated by external hazards shall be identified and their significance to nuclear safety shall be evaluated.

- **Key features of the verification process**
  - Designed and statistical failure dependencies have been analysed. HRA supported the evaluation.
  - Minimal cut sets are identified and CDF is calculated (see the response to the requirement presented above).
  - See BESEP_PSA_ALSF_001.
- **Adequacy of Verification**
  - The complex failure combinations initiated by external hazards (and related to LUHS) have been adequately evaluated.
  - Adequate PSA approach for external events is used.
  - See BESEP_PSA_ALSF_001.
- **Proposals for Improvement**
  - None.
  - No improvement is needed.
  - The PRA assumes LOOP at the event due to rapid shutdown of more than one NPP which leads to an overestimate of the importance of the sequence. Further developing the initial sequence progression is seen necessary.
  - Various follow-on analyses and actions are seen necessary.
  - Further development of the initial sequence progression focusing on time dependencies as well as several follow-on analyses and actions are seen as possibilities for improvement.
### LUHS_1

- Designed and statistical failure dependencies have been analysed. HRA supported the evaluation.

### LUHS_2

- Extremely low temperatures affect adversely the environment in which the plant personnel must perform their actions. New operator actions are created, some actions are eliminated, new dependencies are among operator actions.

### LUHS_3

- Plant response analysis identified phenomena that can affect the screening plant. This was evaluated in the PRA. The PRA considered both FLEX actions for recovery of emergency diesel generators and start of the ICCS. The physical location of SSCs and related and relevant human actions were included in the PRA.

### LUHS_4

- Identification and quantification of safety significant human failure events; dependence between the different human actions was also studied and considered.

### Conclusions

- Plant response analysis, quantification of relevant human actions, designed and statistical failure analysis.

---

**BESEP requirement ID:** BESEP_PSA_ALSF_003

The important functional dependencies on physical location and from operation, maintenance and the effects of human activities shall be considered in assessing the potential losses of safety functions.

<table>
<thead>
<tr>
<th>Key features of the verification process</th>
<th>Adequacy of Verification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Designed and statistical failure dependencies have been analysed. HRA supported the evaluation.</td>
<td>The functional dependencies related to external hazards (and to LUHS) have been adequately evaluated.</td>
</tr>
<tr>
<td>Extremely low temperatures affect adversely the environment in which the plant personnel must perform their actions. New operator actions are created, some actions are eliminated, new dependencies are among operator actions.</td>
<td>Adequate PSA approach for external events is used.</td>
</tr>
<tr>
<td>Plant response analysis identified phenomena that can affect the screening plant. This was evaluated in the PRA. The PRA considered both FLEX actions for recovery of emergency diesel generators and start of the ICCS. The physical location of SSCs and related and relevant human actions were included in the PRA.</td>
<td>The verification process considered all relevant dependencies and manual actions for the first 24 hours in the PRA. For DEC event LUHS an additional reliability analysis was performed to verify the function for 72 hours. The verification</td>
</tr>
<tr>
<td>Identification and quantification of safety significant human failure events; dependence between the different human actions was also studied and considered.</td>
<td>Dependencies between the effects of human activities; all other types of dependencies are self-evident.</td>
</tr>
</tbody>
</table>

All relevant dependencies have been evaluated to be included in the verification.
<table>
<thead>
<tr>
<th>LUHS_1</th>
<th>LUHS_2</th>
<th>LUHS_3</th>
<th>LUHS_4</th>
<th>Conclusions</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>process is seen as adequate.</td>
<td></td>
<td>Human failure sensitivity studies and partly the human actions during longer time periods would provide some more evidence on verification.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>No improvement is needed.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>None.</td>
<td>The process did not consider repair of failed equipment at long time windows. The state of the art HRA methods does not take credit for long grace times leading to conservative failure probabilities for manual actions.</td>
<td>Some further sensitivity studies on the dependence between human failures.</td>
<td></td>
</tr>
</tbody>
</table>

**BESEP requirement topic:** Situation awareness and assessment (HFE)

**BESEP requirement ID:** BESEP_HFE_SAA_001

The design of user interfaces in NPP shall support the operators in assessing any normal and abnormal situation so that they can perceive the situation, comprehend it and finally anticipate the future status of the event.

**Key features of the verification process**

- The accident situation ergonomics has been validated and verified with V&V actions during the design stage and also with integrated sub-system validation, that was conducted in full-scale simulator. The normal operation ergonomics is validated with operational experience.
- As it is described above, new operator actions are created, some actions are eliminated, new dependencies are among operator actions.
- Iterative reviews of design requirements with input from operational experience, human factors specialists, and safety analyses. Verification based on NUREG 0700 and philosophies for the design of control rooms at the NPP. Task analyses and scenario-based testing in simulator and 3D-models.
- Not evaluated.
- The verification is based on the use of full-scale simulator and 3D-models, task analyses and operational experience.
<table>
<thead>
<tr>
<th>LUHS_1</th>
<th>LUHS_2</th>
<th>LUHS_3</th>
<th>LUHS_4</th>
<th>Conclusions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Adequacy of Verification</strong></td>
<td>In the design of the user interfaces the needs of the operators have been taken into account.</td>
<td>Adequate PSA approach for external events is used</td>
<td>The verification is seen as adequate.</td>
<td>Not evaluated.</td>
</tr>
<tr>
<td><strong>Proposals for Improvement</strong></td>
<td>None.</td>
<td>No improvement is needed.</td>
<td>None.</td>
<td>Not evaluated.</td>
</tr>
</tbody>
</table>

**BESEP requirement ID: BESEP_HFE_SAA_002**

The visual monitors or operating panels shall provide the operators a holistic view on the plant state and feedback from the course of event and effects from activations and passive or automatic functions.

| **Key features of the verification process** | In the design of user interfaces the tasks, requirements and experiences of the users are taken into account. The design aims to support safe and efficient operation. | HRA is performed within the PSA and the human–machine interaction is evaluated and implemented into the model | Parameters for assessing the plant state and feedback from the course of event are decided through DSA. Verification is based on philosophies for control room design at the NPP and operational experience. | Not evaluated. | Verification is based on philosophies for control room design at the NPP and operational experience. |

| **Adequacy of Verification** | The visual monitors and operating panels provide the operators a holistic view. | Adequate PSA approach for external events is used | The verification is seen as adequate. | Not evaluated. | The verification is seen as adequate. |
| **Proposals for Improvement** | None. | No improvement is needed. | None. | Not evaluated. | No improvement proposals. |

**BESEP requirement ID: BESEP_HFE_SAA_003**
Relevant information related to the procedures and guides shall be presented for the operators to assess the situation, to see the plant response to actions and to assess the progress of the plant state.

**Key features of the verification process**

<table>
<thead>
<tr>
<th>LUHS_1</th>
<th>LUHS_2</th>
<th>LUHS_3</th>
<th>LUHS_4</th>
<th>Conclusions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Procedure support displays support the operators in decision making and monitoring the situation in addition to the control panels. The displays and panels follow the rules given in style guide.</td>
<td>HRA is performed within the PSA and the human–machine interaction is evaluated and implemented into the model</td>
<td>See requirements BESEP_HFE_SA_001 and BESEP_HFE_SA-002.</td>
<td>High level description in EOPs and SAMGs; details in system specific OPs; measures to improve procedures.</td>
<td>Parameters for assessing the plant state and feedback from the course of event are decided through DSA. They are shown in procedure support displays and control panels, supported by procedures.</td>
</tr>
</tbody>
</table>

**Adequacy of Verification**

| All new panels and displays are verified to follow the rules given in style guide. | Adequate PSA approach for external events is used. | See requirements BESEP_HFE_SA_001 and BESEP_HFE_SA-002. | Adequate description in system operating procedures | Verification is based on style guide and evaluation of the description in system operating procedures. |

**Proposals for Improvement**

| None. | No improvement is needed. | None. | Develop an operational and transient mitigation strategy and specify the corresponding sequences of actions. | Develop an operational and transient mitigation strategy and specify the corresponding sequences of actions. |

**BESEP requirement topic:** Verification and validation (V&V) of design (SEP)

**BESEP requirement ID:** BESEP_SEP_VV_001

V&V shall demonstrate that the included areas, spaces, systems, structures and components, manual tasks and organizational conditions are working together as designed and meet the safety requirements set to them.

**Key features of the verification process**

<table>
<thead>
<tr>
<th>LUHS_1</th>
<th>LUHS_2</th>
<th>LUHS_3</th>
<th>LUHS_4</th>
<th>Conclusions</th>
</tr>
</thead>
<tbody>
<tr>
<td>The safety requirements related to LUHS have been validated from the PSA (risk distribution, CDF and LERF) and from the DSA (fuel and other)</td>
<td>The PSA is used to show that SSCs and HFE are working together as it is required.</td>
<td>See BESEP_SEP_VV_004.</td>
<td>Extensive tests were performed in order to verify the feasibility of implementing the external injection paths; these tests also served</td>
<td>Extensive tests were performed in order to verify the feasibility of the implemented safety functions. DSA demonstrates that the</td>
</tr>
</tbody>
</table>
## LUHS_1

boundary conditions, release). Also the human actions have been taken into account, the reliability part in PSA and the delays etc. in DSA.

## LUHS_2

the purposes of training the plant personnel.

## LUHS_3

plant copes with DBA event. PSA provides evidence on the SSCs operation.

## LUHS_4

### Conclusions

The safety requirements from authorities and legislation are met. Adequate PSA approach for external events is used. See BESEP_SEP_VV_004. Proper demonstration on the basis of tests and training. Proper demonstration on the basis of tests and training. Safety analyses demonstrate that safe state can be reached with sufficient reliability. The verification is seen as adequate.

### Proposals for Improvement

None. No improvement is needed. No improvement is needed. See BESEP_SEP_VV_004. The full path should be tested. It would be good to test the full path of operations needed for the initiating event.

### BESEP requirement ID: BESEP_SEP_VV_002

It shall be possible to trace the decisions made based on the results of V&V to safety design and safety requirements.

### Key features of the verification process

Based on possible V&V findings the need for design change is evaluated. If changed, the change is analysed before manufacturing and commissioning. PSA allows to trace the decisions made on the basis of V&V to safety design and requirements. Not possible to evaluate within BESEP. Not possible to evaluate within BESEP. Not evaluated. There exists a loop back to design from the V&V, and PSA allows to trace the decisions made on the basis of V&V.

### Adequacy of Verification

The change process is documented. Adequate PSA approach for external events is used. Not possible to evaluate within BESEP. Not evaluated. The possible change process is documented. The requirement is not
<table>
<thead>
<tr>
<th>LUHS_1</th>
<th>LUHS_2</th>
<th>LUHS_3</th>
<th>LUHS_4</th>
<th>Conclusions</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>evaluated within some case studies.</td>
</tr>
</tbody>
</table>

**Proposals for Improvement**

| LUHS_1 | LUHS_2 | LUHS_3 | LUHS_4 | No improvement is needed. | Not possible to evaluate within BESEP. | Not evaluated. | No improvement proposals. |

**BESEP requirement ID:** BESEP_SEP_VV_003

The procedures and guidelines shall be systematically validated and verified. Validation shall also address the role of human factors in the procedures and the correct signal generation under the conditions of external hazards.

**Key features of the verification process**

- **LUHS procedures** were systematically validated. Validation also involves the role of human factors under the conditions of external hazards.
- **EOPs and SAMGs** are systematically validated. The validation involves manual actions based on existing and newly developed procedures. V&V for procedures were based on input from PSA and DSA e.g., dependencies to other actions, timing requirements. Flex equipment were subject to hands-on tests at site with evaluation of results and feedback loop to improve the procedures.
- **HRA** was performed for manual actions based on existing and newly developed procedures.
- **Several measures** were aimed at making improvements to the procedures; the test and training programs reinforce their validation and verification too.
- **Tests and training programs** as well as the validation procedures provide a systematic validation and verification. Also, the role of human factors on manual actions and under the conditions of external hazards has been validated.

**Adequacy of Verification**

- The validation of the procedures for LUHS followed the normal plant instructions.
- Validation is performed using the plant simulator. This is adequate way for simulation.
- Flow of information between PSA and HF activities during the V&V.
- Systematic validation and verification of procedures during their review, test and training.
- The verification is seen as adequate as there is a systematic validation of procedures available, and full-scale simulator has also been used.

**Proposals for Improvement**

- None. No improvement is needed.
- None.
- None.
- None.
### LUHS_1

#### BESEP requirement ID: BESEP_SEP_VV_004

In the case of external hazards the NPP shall be safely shut down and kept in a subcritical state, the residual heat removal shall be ensured and the leakages of radioactive substances shall be kept below the specified limits.

<table>
<thead>
<tr>
<th>Key features of the verification process</th>
<th>LUHS_1</th>
<th>LUHS_2</th>
<th>LUHS_3</th>
<th>LUHS_4</th>
<th>Conclusions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Based on the thermohydraulic analysis (DSA) conducted, the NPP can be safely shut down to a subcritical state and kept in it so that the residual heat is removed in case of LUHS. There are no leakages of radioactive substances in this event, thus also these limits for the event are met.</td>
<td>The PSA results have shown negligible level of the risk. So the plant will be safely shutdown and kept in subcritical state.</td>
<td>DSA demonstrates that the plant copes with DBA event. For LUHS DSA demonstrates that ICCS and filtered venting of residual heat meets the conditions of the event. Cold shutdown is reached after 72 hours due to restoration of ordinary residual heat removal system. PSA demonstrates the reliability of the ICCS in the 72 hour case.</td>
<td>Assumption: all water intake facilities are lost simultaneously and recoverable LOOP occurs; justified that the capacity of the fire water system and AEFWS is sufficient.</td>
<td>DSA provides evidence on coping with initiating event within the regulatory limits. PSA results show negligible level of risk.</td>
<td></td>
</tr>
</tbody>
</table>

| Adequacy of Verification | Adequate PSA approach for external events is used | Safety analyses demonstrates that subcritical condition can be reached with sufficient reliability. The verification is seen as adequate. | Adequate, even though portable equipment and on-site fire brigade is considered. | Safety analyses demonstrate that safe state can be reached with sufficient reliability. The verification is seen as adequate. |

| Proposals for Improvement | None. | No improvement is needed. | PSA did not cover the transition from warm to cold shutdown in sequences with residual heat removal by filtered venting. | Installation of independent, stationary diesel generators to provide power supply to the well station pumps |

| Both method improvement (PSA for reaching cold shutdown by filtered venting) and plant design improvement |
**BESEP requirement ID**: BESEP_SEP_VV_005

The operability of systems, structures and components shall be demonstrated in their design basis external environmental conditions.

<table>
<thead>
<tr>
<th>Key features of the verification process</th>
<th>LUHS_1</th>
<th>LUHS_2</th>
<th>LUHS_3</th>
<th>LUHS_4</th>
<th>Conclusions</th>
</tr>
</thead>
<tbody>
<tr>
<td>The SSC existing in the NPP is classified to their design basis environmental conditions. According to the analysis conducted (PRA, DSA) the LUHS event does not provide environmental conditions exceeding the design basis conditions.</td>
<td>DSA results have shown that SSCs are able to withstand the design basis external events. HCLPFs are calculated to demonstrate it.</td>
<td>See BESEP_SEP_VV_004</td>
<td>Extensive tests were performed in order to verify the feasibility of implementing the external injection paths; these tests also served the purposes of training the plant personnel.</td>
<td>DSA results and extensive tests have shown that SSCs are able to withstand the design basis external events.</td>
<td></td>
</tr>
</tbody>
</table>

**Adequacy of Verification**

Analysis have been conducted according to normal plant procedures and they demonstrate the operability of SSCs in case of LUHS.

Adequate DSA approach for external events is used.

See BESEP_SEP_VV_004

Proper demonstration on the basis of tests and training.

Proper demonstration on the basis of analysis, tests and training.

**Proposals for Improvement**

None.

No improvement is needed.

See BESEP_SEP_VV_004

The full path should be tested.

Method improvement, i.e. PSA for reaching cold shutdown by filtered venting is seen possible. Additionally the whole path of needed actions should be tested.
D.2.6 Improvement proposals for the verification process

Some improvement proposals are given in the individual case study self-evaluations. For the requirement topic Functional separation to provide defence against failure propagation (DSA) it is seen, that the independence of power supply or the proof of independence could be improved, but otherwise there is no need for improvement in area of SSC interaction. Both NPP design and verification methods could be improved in the area of physical separation. Proof of independence could be complemented with input from PSA.

For the requirement topic Assessment of potential losses of safety functions (PSA) it is proposed, that when site specific data from the commissioned equipment is available, assumed failure data and probabilities for human actions should be re-evaluated. Further developing the initial sequence progression focusing on time dependencies as well as several follow-on analyses and actions are also possibilities for improvement. Human failure sensitivity studies and partly the human actions during longer time periods would provide some more evidence for the verification.

For the requirement topic Situation awareness and assessment (HFE) there are less improvement proposals. The only proposal is to develop an operational and transient mitigation strategy and specify the corresponding sequences of actions.

For the requirement topic Verification and validation (V&V) of design (SEP) it is proposed to test the full path of operations needed for the initiating event. Both method improvement (PSA for reaching cold shutdown by filtered venting) and plant design improvement (power supply) are seen feasible.

D.3 Safety Margins Assessment

D.3.1 Definitions of the safety margins used in LUHS_1 for PSA, DSA, HFE

Deterministic Safety Margin

Deterministic safety margin can be interpreted as a question what results of the event. Deterministic safety margin contains typically the phenomena and parameters listed in Chapter 4.2 of Deliverable 2.3. These are not repeated here.

In the event of LUHS there exists need to secure the heat removal. As there are both short term means (internal circulation, removal of the heat in steam via steam generators to the atmosphere) and long term means (using the cooling towers), the heat removal is secured during the whole event. This way it can be stated based on the DSA that as the cooling is secured, there exists no risk for core criticality or power increase, nor the possibility for fuel damage or barrier failure.

According to the national regulation there shall at maximum be radiological impact of 20 mSv. Based on the DSA no radiological release takes place in the event of LUHS, so the safety margin exists in the terms of radiological impact.

Probabilistic Safety Margin

Probabilistic safety margin can be interpreted as a question what leads to the event. The probabilistic safety margin is considered as the difference between the calculated core damage frequency and the predefined target of the core damage frequency.

For the LUHS event the share of the total CDF has been reduced by 4*10-6 after commissioning the cooling towers. The share of weather phenomena of the overall CDF in Loviisa NPP units is around 11%, and the share of the external events leading to LUHS is approximately 21% of the weather risks during power operation and approximately 34% during other operation modes. The total CDF of the plant fills the national CDF requirement.

Safety Margin for Human Actions
Safety margin for human actions can be interpreted as a question how is the event managed.

In the event LUHS the human risk analysis (HRA) has been used at least in recognizing the need of the blind operation (i.e. without support of displays or panels) of auxiliary emergency feedwater system and auxiliary residual heat removal system. Based on the analysis the operation procedure was created and thus the risk of the operation was reduced. Otherwise no safety margin for human actions is observed in the LUHS case study.

The safety margins for human actions could be defined better and taken more systematically into use.

D.3.2 Definitions of the safety margins used in LUHS_2 for PSA, DSA, HFE

**Deterministic Safety Margin**

Deterministic safety margin (SM) is considered for extremely low temperatures in the context of the margin to failure (see Figure D.1). This margin consists of the entire range between the operating point of a safety parameter and the failure point. Some of the margin is available to the licensee to allow the flexibility needed for safe and efficient plant operation, while additional margin comes about from regulations and requirements, including compliance with codes and standards that provide built-in margin to failure. SM is determined as HCLPF of the safety variable.

The deterministic SM is calculated using CDFM (Conservative deterministic failure margin). Inputs for CDFM is generated from the results of FEM calculations.

![Figure D.1: SM for extremely low temperatures.](image)

The parameters for extremely low air temperature fragility \( t_m \), \( \beta_R \) and \( \beta_U \) are estimated for different SSCs using finite elements model. The HCLPF is connected with the median temperature capacity using the following formula:

\[
HCLPF \approx t_m e^{-2.326 \beta_c} 
\]

where \( \beta_c = (\beta_R^2 + \beta_U^2)^{1/2} \) is the logarithmic standard deviation.

The deterministic parameter:

\[
HCLPF = t_m \exp(-1.65 (\beta_U + \beta_R)). 
\]

The HCLPF of the extremely low air temperature of the essential service water system is -31.16 °C. Conservative calculations of safety limits are performed. The value HCLPF = -31.16 °C is a conservative
value. If the conservatism of the finite element models is removed, the safety limit of the extremely low
temperature would be significantly decreased.

The definition of deterministic SM is in coincidence with definition in D2.3.

This is the state of the art. No proposal for improvement is needed.

**Probabilistic Safety Margin**

CDF of the plant for internal and external events (including seismic event and non-seismic external events) should be less than 1.0E-4/y for the plants in operation, including fuel damage frequency (FDF) in the spent fuel pool. CDF for the new plants should be 1.0E-5/y. LERF is one order of magnitude smaller (1.0E-5/y and 1.0E-6/y). The probabilistic SM should be less as the defined values.

In case of the LUHS_2 the CDF and LERF are negligible.

The interpretation of safety margins is in good agreement with the approach discussed in Chapter 4.3 of Deliverable 2.3.

This is the state of the art. No proposal for improvement is needed.

**Safety Margin for Human Action**

No human action SM is defined by the national Regulatory Authority. As it was already above described new human actions and new dependencies are defined in comparison with the internal event PSA. In general, the HEPs in the external events PSA are one order of magnitude larger as in the internal event PSA.

No specific approach presented in Deliverable 2.3 to interpret safety margins for human actions.

The safety margins for human actions should be defined in the future.

D.3.3 Definitions of the safety margins used in LUHS_3 for PSA, DSA, HFE

**Probabilistic safety margins**

*Definition*

The probabilistic safety margin is defined as the difference between the calculated core damage frequency and the predefined target of the core damage frequency (sometimes as regulatory requirement). A safety margin is also defined in similar way for the unacceptable release frequency. The targets are set for the plants total frequencies relating to core events. Safety margins for individual initiating events are not defined, but cutset lists and importance measures are studied for balance in contribution and identification of possible outliers, as well as plant barrier against core damage at the initiating event (Barrier=CDF/IE frequency).

![Figure D.2: Probabilistic Safety Margin in Case LUHS_3.](image-url)
Assessment

The exceedance frequency for defined values of low water temperature and on-shore wind was calculated based on local historical weather data and use of extreme value distributions. The assessment considered probabilities for multi-unit consequences and loss of offsite power. Automatic and manual plant responses were considered with regard to available time to meet success criteria of credited safety functions, e.g. core cooling and residual heat removal. HRA were performed for all credited normal and FLEX actions. The event sequences were modelled in the RiskSpectrum PSA model and calculation of frequencies and importance measures were performed individually and accumulated for all non-screened initiating events.

Evaluation

The assessment showed that the accumulated CDF and unacceptable release frequencies were well below adapted safety targets, and that the contribution from LUHS due to frazil ice was less than 1‰. The barrier against core damage were more than 5E-04 which shows that the plant has a strong defence against LUHS events.

Comparison of the Safety Margin Interpretation with Chapter 4 of Deliverable 2.3

The performed safety margin assessment is in large consistent with the definition in chapter 4 of deliverable 2.3, though the margin does not include parametric uncertainties.

Proposals for Improvement

Although parametric uncertainty analysis was performed no evaluation of safety margins considering uncertainties, e.g. 90-percentil of CDF, were performed.

Deterministic safety margins.

Definition

The deterministic safety margin perspective which is generally related to the different levels on defence-in-depth and event classes (frequency for events), is illustrated in the figure below.

![Figure D.3: Deterministic Safety Margin in Case LUHS_3.](image)

In this view the Safety margin against design base external events is realised by systems (independent core cooling system, ICCS) which are verified to withstand loads higher than the DBA load for external events. Therefore, there is a safety margin on plant level to withstand beyond-DBA without core damage occurring. If a complete loss of ultimate heat sink occurs the normal safety functions relying on the ultimate heat sink for cooling will not function, but the ICCS in combination with filtered venting will provide for the reactor reaching a subcritical state.
From another aspect, there is also a safety margin for the DBA event in the capacity of water heating dependant on the flow of water over the strainers, which gives a margin to either (or both) the water temperature and the required mass of water.

**Assessment**

The assessment is made by verifying the ICCS function for BDBA loads for external event such as LUHS for a prolonged mission time (72 h). The verification for the ICCS is made for a limited number of external events and with a realistic approach. The safety margin for the DBA event is assessed by mass flow calculations.

**Evaluation**

The verification of the ICCS showed that it can withstand more extreme events than the DBA event and gives a safety margin against core damage due to BDBA external events.

**Comparison of the Safety Margin Interpretation with Chapter 4 of Deliverable 2.3**

The type of deterministic safety margin described is not addressed in Chapter 4 of deliverable 2.3. The safety margin described in Figure 16 is related to a function/system and a specific parameter as the safety margin presented in the case study is related to different functions (diversity). One way to interpret figure 16 is to modify it according to the figure below.

![Figure D.4: Modified Deterministic Safety Margin of D2.3 chapter 4.](image)

**Proposals for Improvement**

The definition of safety margin could be improved. The two examples in this case study are not in agreement with the definition for deterministic safety margin according to Chapter 4 of Deliverable 2.3. Otherwise the safety margin described above is clearly defined by national authorities as the margin of the plan to withstand external events with higher magnitude than DBA-level.

**D.3.4 Definitions of the safety margins used in LUHS_4 for PSA, DSA, HFE**

**Probabilistic Safety Margin**

The difference between the frequency of loss of ESWS due to river contamination and the regulatory threshold for design basis natural external hazards may be regarded as a safety margin attribute. Besides, considering the fragility curves of the water intake facility, the margin can also be defined as the conditional failure or, more precisely, the conditional success probability at the design basis contamination density level, or as the difference between the median capacity and the design basis contamination density. Moreover, the risk attributable to riverine events indicates the adequacy of the safety margins.

Generally, the objective of hazard assessment for external events is to determine exceedance frequencies for various values of a parameter which represents best the load induced by an external hazard. Primarily, loss of ultimate heat sink due to river contamination was the subject of hazard assessment, as opposed to quantifying only the river contamination hazard itself. This consequence of the river contamination was taken into account as the initiating event in the analysis. The use of this approach was justified by the fact that Danube contamination can induce only one type of technological transient, namely loss of ultimate heat sink,
at the NPP. Moreover, identification and evaluation of a full spectrum of river contamination events did not appear feasible. The assessment was performed by simultaneously analysing the hazardous events and the effects of these events on the water intake system.

Consequently, the definition of the initiating event in question included a systematic search for all those external events and the associated event sequences that can induce inoperability of the water intake system due to river contamination processes. By reviewing these events and sequences, and taking the associated uncertainties into account, the frequency of water intake blockage was estimated.

The scenarios leading to partial or total loss of the water intake systems were determined by making use of invaluable contributions of experts in water management, environmental sciences and biology. In order to identify and evaluate possible endangering events

- an exhaustive list of external hazards was developed with the associated endangering events,
- dangerous substances were described in terms of chemical, physical and biological properties,
- those events were selected that needed detailed PSA modelling and risk quantification.

The frequency of the screened-in external events was determined by a combined use of statistical data analysis and expert judgment as deemed appropriate according to the type of an event. The quantitative results of hazard assessment include the frequency of loss of ESWS.

A PSA model has been developed for river contamination by applying the RiskSpectrum PSA programme. During risk quantification, the frequency of core damage sequences was determined and the most important risk contributors were identified. Point estimates of core damage risk were computed for each contamination type and for the four contamination types analysed in total. In addition, importance, sensitivity and uncertainty analyses were performed to gain further insights useful for a better characterization of risk and for recommending safety improvements.

If we designate river contamination as a natural hazard, the difference between the frequency of loss of ESWS due to river contamination (i.e. 5.25·10^{-5}/y) and the regulatory threshold for design basis natural external hazards (i.e. 10^{-4}/y) may be regarded as a safety margin attribute: 4.75·10^{-5}/y.

It was found unfeasible to quantify the occurrence frequency for different contamination densities (establishing a family of hazard curves) and to determine fragility curves (i.e. conditional failure probability of the water intake facility as the function of contamination density). Hence, the conditional success probability at the design basis contamination density level, and the difference between the median capacity and the design basis contamination density could not be determined.

According to the results of risk quantification, the point estimate for the annual probability of core damage attributable to river contamination is 9.44·10^{-7}/y. This figure is the cumulative frequency from all sources of contamination in all the plant operational states analysed. The results show that the risk from river contamination is moderate in comparison to the risk originated from other types of initiating events analysed in the PSA for the NPP. Moreover, it can also be concluded that the risk due to river contamination is not significant in comparison to the quantitative safety criteria, i.e. ·10^{-4}/y for core damage frequency. The latter finding further supports the conclusion that there is sufficient safety margin beyond the design basis river contamination.

The interpretation of safety margins presented in this document is in good agreement with the approach discussed in Chapter 4.3 of Deliverable 2.3. In this case study, the regulatory probabilistic safety criterion was compared to the calculated mean risk value, which is similar to the approach described in Deliverable 2.3. The only difference is that in Deliverable 2.3 the upper bound of the uncertainty range is applied instead of the mean value. Besides, the basis of the evaluation was the CDF value in this case study. However, Deliverable 2.3 addresses the evaluation of risk metrics for LERF too. Similarly to the approach presented in Deliverable 2.3, the relevant minimal cut sets as well as the importance measures related to random failures were assessed and evaluated. On one hand, it is to be noted that several aspects addressed in Deliverable 2.3 do not seem directly applicable to the present case study. On the other hand, use was made of the results of hazard assessment in determining safety margins in this case study, although it is not addressed in Deliverable 2.3.
It is emphasized that the results of the hazard assessment can be utilized in support of determining the safety margins if the loss of a safety function due to an external hazard is the subject of hazard assessment, as presented in this case study. This margin can be defined as the difference between the frequency of loss of a safety function due to a certain external event and the regulatory threshold for design basis external hazards.

**Deterministic Safety Margin**

From the point of view of hazard characterization and hazard assessment, a potential definition of deterministic safety margin could be the difference of the blockage potential of a design basis contamination event in terms of contamination density and the capacity of the filters in the water intake facility. Moreover, concerning plant response characterization (plant response analysis), the deterministic safety margin can be defined as the number of the different available mitigation systems in place to cope with the effects of river contamination.

As it was mentioned earlier, loss of ultimate heat sink due to river contamination was the subject of hazard assessment, as opposed to quantifying only the river contamination hazard itself. The use of this approach was justified by the fact that river contamination can induce only one type of technological transient, namely loss of ultimate heat sink, at the NPP. Moreover, identification and evaluation of a full spectrum of river contamination events did not appear feasible. However, the maximum probable density of the different types of characteristic river contamination have also been determined based on deterministic analyses, which served as input to defining the design basis of the water intake system.

The following water resources are available on-site for transient mitigation:

- demineralized water supply (6,960 m³ for the four units);
- water in the discharge water channel (4,2000 m³ for the four units);
- virtually unlimited supply of water from the fishing lakes and the well station.

If recovery of off-site power is successful, then the emergency and auxiliary emergency feed water systems can ensure residual heat removal until the demineralized water sources are used up in open loop heat removal. Taking the demineralized water supplies and the decrease of residual heat in time into account, safe cooling conditions can be ensured for up to 110 hours after reactor scram by means of this cooling configuration.

Motivated by the post-Fukushima Targeted Safety Reassessment, cross connection between the fire water system and the ESWS has been implemented. The characteristics of the different fire water subsystems (pump stations) were analysed and evaluated in detail by giving considerations to all the relevant technical factors including the adequacy of pump capacities at the different pump stations to satisfy the minimum necessary cooling water demand for all the units.

As described in Section 3 of the detailed case study descriptions, the fire water system can be connected directly to the condensers too. The capacity of the pump station is sufficient to provide the minimum necessary amount of cooling water for all the units. However, 24 hours of operation of the emergency or the auxiliary emergency feed water system is required in open heat removal mode in any case in order to reduce pressure and temperature in the condenser to enable injection of low pressure and low temperature water from the fire water system or to rearrange cooling system configuration in the secondary circuit by using the secondary decay heat removal system.

On one hand, a solid technical basis could not be established for quantifying the blockage potential in terms of contamination density, even though the capacity of the filters in the water intake facility had been analysed in detail. Hence, the hazard assessment did not allow a deterministically driven characterization of the safety margin or an assessment of the potential for cliff-edge effects.

On the other hand, it can be concluded that the number and the capacity of available safety systems, structures and components, including auxiliary or supporting systems thereof are sufficient, and theses plant items are protected from the effects of river contamination as well as from interaction with failed systems or components. It underpins the conclusion that there is a sufficiently high level of plant protection, hence an appropriate safety margins in place against the effects of river contamination, i.e.:

- four diverse and redundant water resources are available on-site for transient mitigation;
in full power operation five, in low power and shutdown states four redundant and, to a large extent, diverse pump stations (mostly fire water subsystems) are available to cope with loss of ultimate heat sink scenarios.

The deterministic analysis in this case study focuses on the feasibility of the potential mitigation measures including systems as well as interventions that are designed to cope with loss of ultimate heat sink scenarios, as this aspect is generally the most relevant concern when the protection against external events endangering water intake of the NPP is to be verified. Chapter 4.2 of Deliverable 2.3 deals mostly with physical phenomena and plant parameters that are to be assessed primarily by thermo-hydraulic and reactor physics calculations (see the listing at the end of the Chapter). Such assessments had also been performed during the design of the different mitigation systems prior to the analyses reported in this case study to justify that the mitigation actions can ensure a safe plant state if the necessary interventions are taken in a timely manner. For example, it was assessed whether forced pressure reduction at the secondary side and injection of low-pressure feed water into the steam generators could ensure a long-term safe, stable state of the plant or not. Consequently, it would have been feasible to assess the deterministic safety margins in this case study as it is interpreted in Deliverable 2.3; however, those aspects were not in the interest of the case study, as it is typically not a decisive factor when the protection against external hazards needs to be verified.

From the point of view of hazard characterization and hazard assessment, the difference of the hazard potential of a design basis external event and the capacity of the relevant plant SSCs could be interpreted as a safety margin attribute too. Moreover, concerning plant response characterization (plant response analysis), the deterministic safety margin can be defined as the number of the different available mitigation systems in place to cope with the effects of river contamination.

**Safety Margin for Human Actions**

An attribute of safety margins for human actions was defined as the conditional failure probability or, more precisely, the conditional success probability of recovery from loss of ESWS within the timeframe automatic actuations can ensure a safe stable state without the need for any operator interventions, if the off-site power is restored. Similarly, the difference between the time window automatic interventions can prevent core damage, if normal power supply is available and the mean time to recovery from loss of ESWS was considered as a relevant indicator of safety margins for human actions. Moreover, the Risk Increase Factor for all human actions beyond recovery from loss of ESWS was regarded as an additional attribute to safety margin, since it indicates core damage risk when all human actions fail and the role of human actions in such scenarios.

In addition to the human actions already modelled in the internal events PSA, eight human actions were identified and newly introduced into the model (beyond “recovery from loss of ESWS”):

- plant personnel install and start up the diesel-driven pump station for the discharge channel of the condensate cooling water system;
- operators set the path between the fire water system and the essential service water system, and close the paths to selected consumers of the essential service water system;
- on-site fire brigade ensures cooling water to the diesel generators from a fire hydrant;
- plant personnel transport diesel generators used for severe accident management to the well station on the river bank;
- on-site fire brigade provides water supply to the steam generators from the demineralized water tank;
- on-site fire brigade provides water supply to the steam generators from other sources;
- operators set the path between the fire water system and the steam generators;
- operators fill up the high boron concentrate tanks (TB) from the pure condensate tanks (TK);
- on-site fire brigade provides water supply to the SFP from the tank TB.

The Success Likelihood Index Method (SLIM) was used for quantifying the human failures to successfully perform the required actions listed above. The decision on using SLIM was driven by an expectation that this method can be used relatively flexibly and in a structured manner to incorporate expert opinion into the HRA quantification process so that the effects of key performance influences specific to the human actions in question can be readily and explicitly shown in the estimates of human error probability (HEP).
An expert group was set up to help quantify HEPs using SLIM. This group studied the required human interventions in detail, established a set of performance shaping factors (PSFs) based on an understanding of the conditions for human actions, assessed the relative weight of the different PSFs, calibrated the used factors and rated the interventions from the point of view of the PSFs. The following performance shaping factors (influences) were considered as the most important ones for the human actions and related human failure events assessed:

- environmental conditions;
- time constraint / emergency stressor;
- task complexity;
- human-machine interface;
- qualification and training;
- required level of team integration and team work to successfully perform the action;
- quality of procedures.

In addition to the human failure events quantified by using SLIM, recovery from loss of ESWS was also assessed in HRA. The recovery failure probability was quantified by assuming that time to recovery is a random variable predominantly characterised by the mean (average) recovery time, assessing the time window for recovery and evaluating the probability of failure on the basis of the probability distribution function considered relevant. A similar approach had been used for a limited number of recovery actions in the internal events PSA.

Expert judgment was applied to estimate the average time to recovery by giving considerations to task complexity, available means and available equipment for recovery, as well as the types and number of components affected by a given type of contamination. The quantitative results of hazard assessment include the average time to recovery from loss of ESWS for the different substances causing river contamination as follows:

- crude oil or oil by-products floating under water surface: 3 days;
- toxic substances (large scale fish devastation on the river): 2 days;
- grains that may cause filter clogging: 0.5 day;
- river vegetation that may cause filter clogging: 3 days.

According to the analysis results, the conditional success probability of recovery from loss of ESWS within the timeframe (110 hours) automatic actuations can ensure a safe stable state without the need for any operator interventions, if the off-site power is restored are as follows for the different contamination types:

- crude oil or oil by-products floating under water surface: 0.78;
- toxic substances (large scale fish devastation on the river): 0.90;
- grains that may cause filter clogging: 0.9999;
- river vegetation that may cause filter clogging: 0.78.

The difference between the timeframe automatic interventions can prevent core damage, if normal power supply is available and the mean time to recovery from loss of ESWS is expected to be:

- crude oil or oil by-products floating under water surface: 38 hours;
- toxic substances (large scale fish devastation on the river): 62 hours;
- grains that may cause filter clogging: 98 hours;
- river vegetation that may cause filter clogging: 38 hours.

According to the results of risk quantification, the Risk Increase Factor for all human actions beyond recovery from loss of ESWS is 1.8, hence the risk is around $1.8 \times 10^{-6}$/y in case no operator action is credited other than the recovery actions from loss of ESWS. This figure implies that the risk from river contamination is moderate in comparison to the risk originated from other types of initiating events analysed in the PSA for the NPP, even if these operator actions are not credited. Moreover, it can also be concluded that the risk due to river contamination is not significant in comparison to the quantitative safety criteria, i.e. $10^{-4}$/y for core damage frequency, even if these operator interventions are not successful.
Although there is no specific approach presented in Deliverable 2.3 to interpret safety margins for human actions, the analysis steps addressed in the report are also performed within this case study. The human actions were identified, and then analysed qualitatively and quantitatively, and the human failure events and their probabilities were built into the PSA. The qualitative and quantitative assessment was based on the identification of key influencing factors and the evaluation of the different operator actions, including recovery from loss of ESWS with considerations to the performance shaping factors determined.

Moreover, efforts were made in the case study to quantify the safety margin for human actions by assessing the conditional success probability of recovery from loss of ESWS within the timeframe automatic actuations can ensure a safe stable state without the need for any operator interventions, if the off-site power is restored. Similarly, the difference between the time window automatic interventions can prevent core damage, if normal power supply is available and the mean time to recovery from loss of ESWS was assessed as a relevant indicator to safety margins for human actions. Lastly, the Risk Increase Factor for all human actions beyond recovery from loss of ESWS was quantified as an additional attribute to safety margin.

Beyond the attempt made in the case study to quantify the safety margin for human actions as presented above, we propose to consider the difference between half an hour and the duration the operator intervention may still lead to a safe stable state as a further attribute to safety margin for human actions. The time window over half an hour is relevant, as it is required by national nuclear safety regulations that operator interventions within half an hour should not be credited. It is also emphasised to establish a more straightforward and traceable safety margin definition for human actions on the basis of applicable importance and sensitivity measures obtained from risk assessment. The interpretation and evaluation of such a safety margin should also be elaborated.

D.3.5 Comparison of the methods used for safety margin assessment

Comparison of the methods used for safety margin assessment described above is provided in Table D.2.
### Table D.2: Assessment of Safety Margins.

<table>
<thead>
<tr>
<th>LUHS_1</th>
<th>LUHS_2</th>
<th>LUHS_3</th>
<th>LUHS_4</th>
<th>Conclusions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Deterministic Safety Margins</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Definition</strong></td>
<td>What results of the event.</td>
<td>HCLPF</td>
<td>The safety margin is generally related to the different defence-in-depth levels and event classes (frequency for events). The ICCS is verified to withstand higher loads than the DBA load for external events.</td>
<td>number of the different available mitigation systems in place to cope with the effects of river contamination; (design basis contamination event in terms of contamination density and the capacity).</td>
</tr>
<tr>
<td><strong>Assessment &amp; Evaluation</strong></td>
<td>There exist diverse means to secure heat removal both in short and long term. Based on DSA there exists no risk for release in case of DBC or DEC LUHS. Allowed limit is 20 mSv, so decent safety margin exists.</td>
<td>CDFM and FEM</td>
<td>Verifying ICCS function for BDBA loads for a prolonged mission time (72 hours). This verification is done for a limited number of external events and with a realistic approach. The ICCS withstands more extreme events than DBA events and gives a safety margin against core damage for BDBA external events.</td>
<td>plant response analysis; the number and the capacity of available safety SSCs, including auxiliary or supporting systems thereof are sufficient, are protected from the effects of river contamination and from interaction with failed systems or component.</td>
</tr>
</tbody>
</table>
### APPENDIX D

**Comparison with D2.3**

<table>
<thead>
<tr>
<th>LUHS_1</th>
<th>LUHS_2</th>
<th>LUHS_3</th>
<th>LUHS_4</th>
<th>Conclusions</th>
</tr>
</thead>
<tbody>
<tr>
<td>The safety margin is in line with the Chapter 4.2 of Deliverable 2.3.</td>
<td>The definition of SM is in coincidence with definition in D2.3.</td>
<td>The safety margin in the case study is related to different functions (diversity).</td>
<td>physical phenomena and plant parameters in Ch. 4.2 of D2.3, not in the focus of the case study; focus on the feasibility of the potential mitigation measures including systems as well as interventions designed to cope with LUHS scenarios.</td>
<td>See Definition.</td>
</tr>
</tbody>
</table>

**Proposals for Improvement**

| None. | No proposal for improvement is needed. | The definition of safety margin could be improved. The definition of safety margin by the national authorities is the margin of the plant to withstand external events with higher magnitude than DBA-level. | the difference of the hazard potential of a design basis external event and the capacity of the relevant plant SSCs; define as: the number of the different available mitigation systems in place to cope with the effects of river contamination. | For LUHS_3 and LUHS_4 it is suggested that the definition of SM should be changed. LUHS_1 and LUHS_2 are consistent with the existing definition. |

**Probabilistic Safety Margins**

<table>
<thead>
<tr>
<th>Definition</th>
<th>Assessment &amp; Evaluation</th>
</tr>
</thead>
<tbody>
<tr>
<td>What leads to the event.</td>
<td>The plant reaches the CDF target set by the regulator.</td>
</tr>
<tr>
<td>Plants in operation:</td>
<td>The event share for the Level 1 PSA, CDF for internal and external events should be less than 1.0E-6.</td>
</tr>
<tr>
<td>total CDF &lt; 1.0E-4, total LERF &lt; 1.0E-5</td>
<td>Exceedance frequency of low water temperature and on-shore wind based on PSA for riverine events; initiating event = LUHS due to river contamination;</td>
</tr>
<tr>
<td>New plants:</td>
<td>All cases fulfil their respective goals for CDF. The specific IE</td>
</tr>
<tr>
<td>total CDF &lt; 1.0E-5, total LERF &lt; 1.0E-6</td>
<td></td>
</tr>
<tr>
<td>The difference between the calculated CDF and the predefined target of the CDF. No safety margins for individual IE are defined.</td>
<td>compare calculated risk to criteria; difference between the frequency of loss of ESWS due to river contamination and the design basis threshold for natural external hazards.</td>
</tr>
<tr>
<td></td>
<td>All definitions are consistent with deliverable 2.3 chapter 4.3.</td>
</tr>
<tr>
<td>LUHS_1</td>
<td>LUHS_2</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>LUHS event is not dominating in the total CDF.</td>
<td>4/y for plants in operation and less than 1.0E-5/y</td>
</tr>
<tr>
<td>For the case study of LUHS no specific PSA safety margin study was conducted.</td>
<td>LERF for new plant is one order of magnitude smaller.</td>
</tr>
</tbody>
</table>

**Comparison with D2.3**

- The safety margin in general level is in line with the Chapter 4.3 of Deliverable 2.3.
- The safety margin in general level is in line with the Chapter 4.3 of Deliverable 2.3.
- The safety margin assessment is consistent with the definition in chapter 4 D2.3. The assessment does not include parametric uncertainties.

in agreement, except:
- mean value vs. upper bound of uncertainty range;
- no LERF, only CDF;
- use of results of hazard assessment (not discussed in D2.3).

All cases are in general agreement. For LUHS_3 parametric uncertainties are not included. For LUHS_4 no LERF value was provided and use was made of the results of hazard assessment.

**Proposals for Improvement**

- None.
- No proposal for improvement is needed.
- Parametric uncertainty analysis was performed but no evaluation of safety margins considering uncertainties were performed.

probabilistic safety margin: the difference between the frequency of loss of a safety function due to a certain external event and the regulatory threshold for design basis external hazards.

LUHS_1 and LUHS_2 are consistent. LUHS_3 highlights that evaluation of SM considering uncertainties is beneficial. LUHS_4 stress that regulators can have thresholds for DBEH the difference therefrom could provide a specific PSM.

<table>
<thead>
<tr>
<th>Safety Margins for Human Actions</th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>LUHS_1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LUHS_2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LUHS_3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LUHS_4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Definition</td>
<td>LUHS_1</td>
<td>LUHS_2</td>
<td>LUHS_3</td>
<td>LUHS_4</td>
<td>Conclusions</td>
</tr>
<tr>
<td>------------</td>
<td>--------</td>
<td>--------</td>
<td>--------</td>
<td>--------</td>
<td>-------------</td>
</tr>
<tr>
<td>How the event is managed.</td>
<td>No exact definition.</td>
<td>No definition.</td>
<td>conditional success probability of recovery from loss of ESWS within the timeframe automatic actuations can ensure a safe stable state (no operator action); the difference between the time window automatic interventions can prevent core damage (if NPS available) and the mean time to recovery from loss of ESWS: 38, 62, 98, 38 hours for different contamination types;</td>
<td>No safety margin for human actions can be found within the cases regarding HFE. All cases mention HRA. To some extent it is arguable that some attention towards safety margins for human actions have been incorporated to the probabilistic and deterministic safety margins.</td>
<td></td>
</tr>
</tbody>
</table>

<p>| Assessment &amp; Evaluation | The need for procedure for blind operation of AEFWS and ARHRS was recognised in HRA. Otherwise no safety margin for human actions is observed in the LUHS_1 case study. | HEP &lt; 1.0E-5 are not considered in the PSA. | No assessment for safety margin within HFE. | HRA (using SLIM and engineering judgement); conditional success probability of recovery from loss of ESWS within the timeframe automatic actuations can ensure a safe stable state (no operator action): 0.78, 0.90, 0.9999, 0.78 for different contamination types; the difference between the time window automatic interventions can prevent core damage (if NPS available) and the mean time to recovery from loss of ESWS: 38, 62, 98, 38 hours for different contamination types; | Either no assessment and therefore no evaluation of human actions are made in the cases or human actions with a sufficiently low probability of error are not considered. |</p>
<table>
<thead>
<tr>
<th>LUHS_1</th>
<th>LUHS_2</th>
<th>LUHS_3</th>
<th>LUHS_4</th>
<th>Conclusions</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>If all human actions are failed, the risk is still well below the risk criteria.</td>
</tr>
<tr>
<td><strong>Comparison with D2.3</strong></td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>analysis steps addressed in the report are also performed; additional efforts, see the definition cell.</td>
</tr>
<tr>
<td><strong>Proposals for Improvement</strong></td>
<td>The safety margins for human actions could be defined better and taken more systematically into use.</td>
<td>To remove conservatism from FEM analyses. The safety margins for human actions should be defined in the future.</td>
<td>Better definition of safety margins for human actions.</td>
<td>difference between half an hour and the duration the operator intervention may still lead to a safe stable state; establish a more appropriate safety margin definition for human actions on the basis of importance and sensitivity measures from PSA.</td>
</tr>
</tbody>
</table>
The safety margin definition for DSA used in LUHS_1 and LUHS_2 is in line with the DSA safety margin definition given in Chapter 4.2 of BESEP Deliverable 2.3. LUHS_2 used CDFM to calculate the safety margin for DSA. In LUHS_3 the safety margin determination is done through verifying that the ICCS and filtered venting necessary to take the plant to a subcritical state in the case of LUHS can withstand loads more severe than the DBA loads. The approach in LUHS_3 follows the national regulatory environment where the requirements regarding frequency for events to be considered in the design basis and beyond are met through defence-in-depth for a limited number of external events with a realistic approach. Physical phenomena and plant parameters, the definition is related to, were not in the scope of LUHS_4. In LUHS_4 it would have been feasible to assess the deterministic safety margins as it is interpreted in Deliverable 2.3; however, those aspects were not in the scope of the case study.

The safety margin definition for PSA used in LUHS_1, LUHS_2, LUHS_3 and LUHS_4 are in line with the PSA safety margin definition given in Chapter 4.2 of BESEP Deliverable 2.3. LUHS_3 provides a safety margin that does not include parametric uncertainties. In LUHS_4 safety margin was also used as the difference between the frequency of loss of ESWS due to river contamination and the design basis threshold for natural external hazards.

For human actions the safety margin definition is less exact as for PSA and DSA also in Chapter 4.2 of BESEP Deliverable 2.3. For the HFE methods and approaches, in LUHS_1 only human reliability analysis (HRA) has been used in recognizing the need of the blind operation (i.e. without support of displays or panels) of auxiliary emergency feedwater system and auxiliary residual heat removal system. Based on the analysis the operation procedure was created and thus the risk due to operation was reduced. For LUHS_2 no HFE method is used. In LUHS_3 the safety margin for human actions is handled as a part of the deterministic safety margin and the probabilistic safety margin using HRA. Within the HFE-process for LUHS_3 there are no requirements for safety margins for human actions but the different steps in the process aims at ensuring the possibility to the operators to perform their actions within the respective timeframes. LUHS_4 defined the safety margin as the conditional success probability of recovery from loss of ESWS within the timeframe automatic actuations can ensure a safe stable state without the need for any operator interventions, if the off-site power is restored. Similarly, the difference between the time window automatic interventions can prevent core damage, if normal power supply is available and the mean time to recovery from loss of ESWS was considered as a relevant indicator of safety margins for human actions. Moreover, the Risk Increase Factor for all human actions beyond recovery from loss of ESWS was regarded as an additional attribute to safety margin, since it indicates core damage risk when all human actions fail and the role of human actions in such scenarios.

As stated above the cases LUHS_1 and LUHS_2 is in line with the definition for deterministic safety margin in Chapter 4.2 of BESEP deliverable 2.3. For case LUHS_3 and LUHS_4 the demonstration of safety margin is in line with this definition for the DBA events but for the beyond design basis external events other but still similar methods are applied. LUHS_3 uses a realistic approach to demonstrate the plants safety margin in terms of response to the event. LUHS_4 demonstrates the plant response to beyond design basis external events through the number of available mitigation systems as the safety margin. Two of the cases describe a different approach for the demonstration of deterministic safety margin beyond design basis external events.

Probabilistic safety margin is used in the same way in the different case studies.

Safety margins for human actions have not been identified in any of the cases.

D.3.6 Improvement proposals

Concerning plant response characterization (plant response analysis), the safety margin for DSA could be defined as the number of the different available mitigation systems in place to cope with LUHS situations.

Probabilistic safety margin, i.e. the safety margin for PSA: the difference between the frequency of loss of a safety function due to a certain external event and the regulatory threshold for design basis external hazards, can be regarded as an adequate evaluation approach when analysing the external hazards, their effects and risks.

The safety margins for human actions could be defined better and taken more systematically into use than the state-of-practice. The safety margin for human actions may be better linked with training of the operators and
the plant staff. This would be an interesting goal for a living PSA. For example, the results from scenarios that can be trained in the simulator can possibly be incorporated into the safety assessment for the specific actions that could provide updates to the PSA model. The same could be done for scenarios that can’t be trained in the simulator. It is interesting to assume that the ongoing retraining of the staff at the plant could provide both quantitative and qualitative input to safety margin assessment. To be able to observe eventual changes in performance over time could also be beneficial for effectiveness in training schedule. In accordance with one of the cases it is possible to evaluate safety margins for beyond design basis accidents with realistic methods which would include this type of human actions handling.

D.4 Interactions between DSA, PSA and HFE

D.4.1 Description of the interactions in LUHS_1

The interactions between DSA, PSA and HFE have been defined for case LUHS_1 in the point of view of developing the strategy against LUHS. During long-lasting development several interactions existed between PSA, DSA and HFE. The estimation of the IE frequency comes from the PSA and this information is used as a basis for selecting the analysis cases e.g. for thermohydraulic safety analyses. (PSA -> DSA)

The need for the cooling towers was originally discovered in PSA for the SBO event, but the towers do minimize the risk also in LUHS (PSA -> DSA). The commissioning of the cooling towers leads to changes in strategy to manage the LUHS event (PSA/DSA -> HFE/SEP). In the design of the tower’s PSA related information of the environmental conditions was also needed. The human limitations of work found out in SBO analysis led to the implementation of the blind operation procedure for auxiliary residual heat removal system and auxiliary emergency feedwater system (HFE/PSA -> DSA).

Also, in the DSA and in the procedures the human action times, reaction times and operational limits are taken into account (HFE -> DSA/HFE).

There are no differences in interactions between analyses for DBC and analysis for DEC.

The interactions between DSA, PSA and HFE could be made more streamlined and such that each party (or discipline) would be more aware of the needs and means of the others. This could be reached by better describing the interactions in internal procedures.

D.4.2 Description of the interactions in LUHS_2

DSA is used to generate HCLPF for PSA. Using the HCLPF and the uncertainty parameters (the formula is described above) the fragility curves for SSCs are constructed. Failure probability of SSCs can be calculated after implementation of hazard curves and fragility curves to the HAZARDLITE module of the RiskSpectrum code. HAZARDLITE performs convolution of the hazard curves and fragility curves and SSC failure probabilities are calculated.

No HFE is involved in DSA. Human error probabilities (HEP) are implemented into the external event PSA. Only HRA activities are considered.

DEC analyses are not performed because the negligible CDF the extremely low temperatures are screened out as practically eliminated events.

DSA are providing inputs for PSA. This interconnection is the only way for calculation of CDF, FDF and LERF for the plant within a PSA project. Alternatives exist only in the form of DSA, however, the most acceptable results for the regulatory body are to have conservative results.

The above described approach is the good practice and state of the art.
D.4.3 Description of the interactions in LUHS_3

The interactions between the different analyses are described on a high-level in the case study description, a more detailed description is given in the following section together with graphical presentations in Figure 4 and 5. The interactions between the safety analyses are a part of the SEP which in the next section is described by using the V-model. The description in this section includes both the interactions between the analyses and the interaction between requirements, safety analysis and plant design.

On an overview level the green boxes represent requirement related steps in the process, the different blue boxes represent safety analyses related steps and the purple represent plant design steps. The interactions can be divided into three different levels:

- Level 1: Interaction between safety requirements, safety analysis and plant design
- Level 2: Interactions between different safety analyses
- Level 3: Interactions within a safety analysis

Step 1-3 describes the SEP in a level 1 perspective connecting safety requirement, safety analyses and plant design, in Figure D.5 for the DBA and in Figure D.6 for the BDBA and the design of the independent core cooling system (ICCS). Step 2 contains all relations and interconnections between the safety analyses and is a combined description of SEP level 2-3. It should be noted that the process related to external events have been going on for more than 15 years at the NPP and that many different projects have been involved in the process. Hence, the process has been complex and is not easy to describe.

In the end when all the process steps have been performed the Safety Analysis Report (SAR) was up-dated (re-constructed UHS and construction of ICCS). The updated SAR describes the new requirements, the new design and the new analyses on how the design fulfills the new requirements. Hence, the up-date of SAR is the final step in the V-model related to the Safety Engineering Process describing the new plant configuration as built.

Figure D.5: SEP of DBA in Case LUHS_3.
SEP Level 1, Figure 4:

Step 1a: Operational experience from incidents at similar plants showing that existing design does not meet the requirements. Flow A gives the input to Step 3a that the set point for switch-over to recirculation of heated outlet water needs to be re-evaluated.

Step 1b: Issuing of new requirements from the authority which clearly states that all possible external events should be considered and analysed. Moreover, the return frequency is given to 10-4-10-6/year for design base accidents and is applicable for external events. Flow B gives the input to Step 2.2a in the safety analyses that all external events are to be analysed.

Step 1c: The Fukushima event led to requirements on performing the ENSREG Stress Tests to analyse the plant design for design base and beyond design base external events. Flow C is the requirement on how to perform the stress test which is used in the analysis in Step 2.1a.

Step 2: This step contains all the safety analysis which have been performed. The step is described in more detail in the SEP Level 2-3 below. Flow L is information on the FLEX strategies to be implemented in order to strengthen the ultimate heat sinks ability to cope with external events used as input in Step 3.

Step 3: Represent the process step of design and construction work to support the proposed FLEX strategies. Flow M is information on design given in the different project stages, and also results of performed V&V activities, which is fed back to Step 2.3a.

SEP Level 2-3, Figure 4:

Here the details of Step 2 are described to highlight the interconnections and interactions of the safety analyses within the SEP. It should be noted that the figure and description try to capture the most important steps and flows of the SEP. More step and flow could be added but then the figure would be too complicated and difficult to use within the BESEP project.

Step 2.1a: After the Fukushima event the stress test were performed based on requirements from ENSREG (Step 1c and Flow C). Results of the stress tests were used as input for benchmark against existing safety analyses and then updated identification and screening of external events in Step 2.2a, shown by Flow D. Results of the stress test was also fed into Step 2.2b and Step 2.3a (flow not shown in the figure) were alternative FLEX actions to cope with all identified external events were identified, and then in Step 2.2b analysed and screened, shown by Flow G.

Step 2.1b: The deterministic analysis was updated with information on external events and return values fed from the PSA in Step 2.2a indicated by Flow F. Determination of load values for the deterministic analysis was performed in this step and it was also determined that the design base value for external events should correspond to a return frequency of \(10^{-5}\)/year.

Step 2.2a: Updated identification and screening of external events was made in this step first based on new requirements shown by Flow B, and then as a result of the stress test in Step 2.1a. Through Flow E the identified external events fed into the PSA-study. The identification and screening of external events within the PSA formed the bases for the deterministic approach as given by Flow F which basically consisted of the total list of identified site-specific external events and their calculated return frequencies.

Step 2.2b: In this step the results of the stress tests, Step 2.1a, were used as input for probabilistic evaluation of possible FLEX actions to cope with all identified external events, as shown by Flow G. The step identified, evaluated and screened FLEX strategies in an iterative manner with HF, Step 2.3a. Development of FLEX strategies, shown by Flow H and I and K. Also, from the HRA activity of the PSA, input was given to HF on the need for development of existing emergency operating procedures in order to fit/connect with the new FLEX procedures. Results from V&V activities were also fed back to the HRA in the PSA as indicated by Flow M and K. The results of Step 2.2b, i.e. equipment, procedures, timing and manning, were finally fed to the PSA as indicated by Flow N.
Step 2.2e: The update of the PSA-study included in the SAR is illustrated with this Step, though the PSA-model itself was also utilized in Step 2.2b.

Step 2.3a: In this step FLEX strategies were developed based on the results from the stress test and input on risk importance measures from the PSA, Step 2.2b. The requirement for procedures were fed to Step 2.3b by Flow J. Development of strategies were performed in an iterative manner between PSA and HF as indicated by Flow H and I. Information on selected strategies, Flow L, were given as input to the design stage in Step 3a and results of design and V&V activities were fed back as indicated by Flow M.

Step 2.3b: In this step new procedures were developed and existing procedures were updated in order to support FLEX strategies. Input was also given from the HRA-activities in Step 2.2b (indicated by Flow H) concerning improvements of procedures based on risk importance measures (i.e. suggestions for improvement of the reliability of a certain manual action). The results of the step were fed to the PSA by Flow K.

Figure D.6: SEP of BDDBA in Case LUHS_3.

Evaluation of Adequacy

The interactions between the analyses are:

- Input of loads and frequencies for external events (PSA->DSA)
- Plant response analysis (PSA <-> DSA)
- Stress test leads to FLEX strategies and manual actions (PSA/DSA->HF)
- Evaluation of FLEX strategies and procedures (PSA<->HF)

Interactions between DSA and PSA/HF were performed in possible extent with regard to the differences in prerequisites between the analyses, while the interactions between HF and PSA were systematic, continuous and dynamic through the process.

Proposals for Improvement

Improved dynamic interaction between DSA and PSA/HF would be beneficial and lead to better risk informed strategies, better compliance between DSA/PSA and more cost-effective SEP.
D.4.4 Description of the interactions in LUHS_4

Hazard assessment for river contamination was performed using a combination of deterministic and probabilistic analyses. The assessment was made jointly by water management experts (i.e. experts in water management, environmental sciences and biology) and PSA analysts. Consequently, hazard assessment is a manifestation of an integrated approach, considering deterministic, probabilistic, as well as human factors engineering aspects simultaneously. Concerning HFE, the potential to prevent the blockage of the water intake facility by removing the contamination from the cooling water channel was considered.

Amongst others, the stress test of the NPP focused on the analysis of plant response to a loss of ultimate heat sink scenario and on the evaluation of preparedness for such an event. Earlier, loss of cooling by the river as the ultimate heat sink had been screened out from situations that should be considered in the design basis or beyond, as no external or internal hazards had been identified that might cause such a situation with a non-negligible occurrence frequency. The results of the stress test triggered the implementation of safety measures in order to improve the effectiveness of coping with loss of ultimate heat sink scenarios. Accordingly, plant response analysis was performed deterministically first, considering HFE aspects too. Later on, when most of the safety enhancement measures defined during the stress test were implemented, it was found that riverine events would need to be the subject of detailed risk assessment. Hence, PSA for riverine events was performed after the completion of and utilizing the lessons learned from deterministic plant response analysis and the necessary system modifications. Moreover, during the development of the PSA, HFE aspects addressed in the post-Fukushima measures were taken into account. HFE activities and HRA within PSA mutually supported each other during safety analysis.

Hazard assessment was performed in an integrated manner, considering DSA, PSA and HFE aspects simultaneously, that may be regarded as an adequate and mature approach. However, plant response analysis, including the elaboration of several safety measures in order to improve the effectiveness of coping with loss of ultimate heat sink scenarios, was initially based on deterministic analysis, considering HFE aspects, but neglecting probabilistic assessments. PSA was used to review the adequacy of the newly implemented safety measures from risk point of view. This interaction (evolution) of the safety analyses is not preferred in state-of-practice safety engineering processes and should be avoided. The results of DSA and HFE were used in PSA, as far as it was seen practicable and feasible. This interaction and interfacing can be regarded as adequate too.

It is seen advantageous and advisable to utilize PSA and PSA insights as an integral part of determining the implementation of safety measures for coping with external events, as opposed to making use of risk insights in a follow-on manner, i.e. mostly for the purposes of reviews. Such uses of risk assessment and risk insights can help establish the basis of plant modifications, operational and mitigation strategy including the identification of the most important cornerstones, rather than making adjustments to the available strategy as well as SSC design laid down previously by using deterministic considerations only. In summary, DSA, PSA and HFE should be performed simultaneously, interacting actively, so that PSA insights can be used to underpin safety measures including plant modifications.

D.4.5 Comparison of the interactions

Comparison of the interactions between DSA, PSA and HFE described above is provided in Table D.3.
<table>
<thead>
<tr>
<th>Interactions between DSA, PSA and HFE</th>
<th>LUHS_1</th>
<th>LUHS_2</th>
<th>LUHS_3</th>
<th>LUHS_4</th>
<th>Conclusions</th>
</tr>
</thead>
<tbody>
<tr>
<td>PSA provides IE frequencies for DSA case selection. The need for cooling towers was discovered in PSA, that affected then the DSA and HFE. Human limitations of work in HFE/PSA lead to procedure improvement that was also taken into account in DSA.</td>
<td>DSA is used to generate HCLPF for PSA. Using the HCLPF and the uncertainty parameters the fragility curves are constructed. The HAZARDLITE code performs convolution of the hazard curves and fragility curves and SSC failure probabilities are calculated. These are inputs into PSA. HRA also provides inputs into PSA as HEPs.</td>
<td>DSA results from stress tests is input to PSA. Including input for probabilistic evaluation of FLEX actions including human actions. Results from this was fed back into the PSA model for EE. DSA updated with information on external events and return values from PSA:</td>
<td>hazard assessment: considering deterministic, probabilistic and HFE aspects simultaneously; deterministic plant response analysis considering HFE aspects too; deterministic plant response analysis input to PSA for riverine events; HFE activities and HRA within PSA mutually supported each.</td>
<td>IE frequencies from PSA is used as input to the DSA; Need for cooling towers evaluated in PSA used as input to DSA and HFE; DSA used to generate HCLPF for PSA; DSA stress test input to PSA; evaluation of FLEX strategies with HFE input to PSA; deterministic plant response input to PSA; HFE and HRA within PSA supported each.</td>
<td></td>
</tr>
<tr>
<td>Evaluation of Adequacy</td>
<td>Adequate DSA and PSA approach for external events is used. Interactions between HF and PSA were systematic, continuous and dynamic through the process.</td>
<td>Integrated hazard assessment (adequate); no PSA input to DSA and plant modifications; use of PSA only to review safety measures; DSA and HFE considered in PSA (adequate).</td>
<td>Interaction between HFE and PSA; PSA used to review safety measures; DSA and HFE considered in PSA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Proposals for Improvement</td>
<td>The interactions between DSA, PSA and HFE could be made more streamlined. This could be reached by better describing the</td>
<td>Improved dynamic interaction between DSA, PSA and HFE should be performed simultaneously, interacting actively, use</td>
<td>Better internal procedures for interactions between DSA, PSA and HFE</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table D.3: Interactions between DSA, PSA and HFE.
<table>
<thead>
<tr>
<th>LUHS_1</th>
<th>LUHS_2</th>
<th>LUHS_3</th>
<th>LUHS_4</th>
<th>Conclusions</th>
</tr>
</thead>
<tbody>
<tr>
<td>interactions in internal procedures.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LUHS_1</td>
<td>LUHS_2</td>
<td>LUHS_3</td>
<td>LUHS_4</td>
<td>Conclusions</td>
</tr>
<tr>
<td><em>Interactions between DSA, PSA and HFE</em></td>
<td>PSA provides IE frequencies for DSA analysis case selection. The need for cooling towers was discovered in PSA, that affected then the DSA and HFE. Human limitations of work in HFE/PSA lead to procedure improvement that was also taken into account in DSA.</td>
<td>DSA is used to generate HCLPF for PSA. Using the HCLPF and the uncertainty parameters the fragility curves are constructed. The HAZARDLITE code performs convolution of the hazard curves and fragility curves and SSC failure probabilities are calculated. These are inputs into PSA. HRA also provides inputs into PSA as HEPs.</td>
<td>DSA results from stress tests is input to PSA. Including input for probabilistic evaluation of FLEX actions including human actions. Results from this was fed back into the PSA model for EE. DSA updated with information on external events and return values from PSA:</td>
<td>hazard assessment: considering deterministic, probabilistic and HFE aspects simultaneously; deterministic plant response analysis considering HFE aspects too; deterministic plant response analysis input to PSA for riverine events; HFE activities and HRA within PSA mutually supported each.</td>
</tr>
<tr>
<td>Evaluation of Adequacy</td>
<td>The interactions used in developing the LUHS strategy are adequate.</td>
<td>Adequate DSA and PSA approach for external events is used.</td>
<td>Interactions between HF and PSA were systematic, continuous and dynamic through the process.</td>
<td>integrated hazard assessment (adequate); no PSA input to DSA and plant modifications; use of PSA only to review safety measures; DSA and HFE considered in PSA (adequate).</td>
</tr>
</tbody>
</table>

Interaction between HF and PSA; PSA used to review safety measures; DSA and HFE considered in PSA.
<table>
<thead>
<tr>
<th>Proposals for Improvement</th>
<th>LUHS_1</th>
<th>LUHS_2</th>
<th>LUHS_3</th>
<th>LUHS_4</th>
<th>Conclusions</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The interactions between DSA, PSA and HFE could be made more streamlined. This could be reached by better describing the interactions in internal procedures.</td>
<td>No improvement is needed.</td>
<td>Improved dynamic interaction between DSA and PSA/HF would be beneficial.</td>
<td>DSA, PSA and HFE should be performed simultaneously, interacting actively, use PSA insights to underpin safety measures.</td>
<td>Better internal procedures for interactions between DSA, PSA and HFE;</td>
</tr>
</tbody>
</table>
PSA provides input to DSA in LUHS_1 in the form of IE frequencies. In LUHS_2 DSA provides support to PSA in generating the HCLPF. In LUHS_3 information from deterministic stress tests were used as input to EE data analysis and evaluation of FLEX strategies within PSA. Information on external events from the PSA was then fed back into the DSA. In LUHS_4 the hazard assessment using PSA, DSA and HFE was conducted simultaneously, but also DSA provided input to PSA regarding plant response analysis. The interconnection between PSA and DSA is in all cases mostly formalised, but in LUHS_4 also partly tailored for the case. HFE is involved in DSA via finite element modelling in LUHS_2. Also, the human error probabilities have been implemented in external event PSA. In LUHS_4 the human potential in preventing the blockage and removing contamination was taken into account. In plant response analysis (DSA) the HFE aspects were considered. This is the case also in LUHS_1. In the development of PSA the HFE aspects were considered in LUHS_1 and LUHS_4. In LUHS_1 the human limitations of work lead to implementation of new procedure for blind operation. In LUHS_3 FLEX strategies were identified and evaluated in an iterative manner with human factors resources. The HRA activities within the PSA were also used as input to human factors engineering on the need for development of existing EOPs to fit the new FLEX procedures.

For LUHS_1 there are no differences in interactions between DBC and DEC analyses. In LUHS_2 no DEC analysis haven been conducted due to negligible CDF. In LUHS_3 the interactions between analyses have mainly been the same with the addition of input to DSA from PSA in terms of reliability of the ICCS. This is because requirements for deterministic analyses of DEC event LUHS is allowed to include realistic methods.

The ways of interaction vary between the LUHS case studies so no exact strengths or possible alternative interactions can be identified. However, it is seen common to provide PSA input to plant response analysis and DSA input on the plant response to PSA. It would be very important to discover the limitations and possibilities of human actions in PSA and DSA already at the early stages of a modification or analysis.

It is seen advisable to apply PSA and DSA insights as an integral part of determining the implementation of safety functions for managing external events. DSA, PSA and HFE should be performed simultaneously, interacting actively, so that PSA insights can be used to underpin safety measures including plant modifications. Additionally, DSA can be used in supporting the design of the modifications. For DEC external events the plant response almost always includes several human actions. These human actions are considered in the PSA and the DSA and require qualitative analysis methods. The elements in the HFE process increase the reliability of the design. By giving more attention to HFE safety improvements could also be reached.

### D.4.6 Improvement proposals

The interactions between DSA, PSA and HFE could be made more streamlined and such that each party (or discipline) would be more aware of the needs and means of the others. This could be reached by better describing the interactions in internal procedures and guidelines.

When the scope of the analyses and their interconnections are defined in due time before the actual commissioning, there is a possibility to have a feedback loop between the analyses and the actual design process.

### D.5 Overall Safety Engineering Process

#### D.5.1 Description of the overall SEP and the flow of information in LUHS_1

In general the overall safety engineering process covers the whole project/ product life-cycle. It is visualised in the following Figure. The process is similar with the process described in Figures 12 and 13 in deliverable 2.
Figure D.7: Overall SEP of LUHS_1.

In all stages the previous stage design is verified to confirm that the transformation of inputs (= requirements) to outputs (design and/or requirements for the subsequent stage) has been done according to requirements and that no errors or faults have been introduced. In realisation and implementation phases verification is performed for example in integration and factory tests to confirm that the implemented system fulfils its specified requirements.

For the LUHS event management these steps have been followed in the later development stage where the blind operation of the auxiliary residual heat removal system and auxiliary emergency feedwater system in case of SBO and LUHS was instructed, and also in the cooling tower project.

Before entering the SEP for cooling tower project, the need was revealed by a normal regulatory required PRA. After pre-studying the different ways to manage the deficiency an implementation solution was selecting. Already during the pre-study phase the stakeholder requirements were collected and evaluated. For the solution options preliminary thermohydraulic analysis (DSA) as well as preliminary PRA were conducted. Based on these analyses amongst other the implementation solution was chosen. In the beginning of the implementation project the stakeholder needs and requirements were collected and evaluated again. With DSA and PRA it was verified that the cooling tower design fulfils the requirements. On a general level this process flow is illustrated in the following Figure.

Figure D.8: Process flow for LUHS_1.
The overall safety engineering process is based on the safety requirements and on their management. Safety requirements are formed based on the stakeholder interests. Stakeholders include the national regulatory, plant personnel etc. The national requirements are the basis for the requirements, but as the national legislation and the regulatory requirements are extensive and complex, they are used as input while forming the requirements for the overall safety engineering process. This way also the interpretation of the original requirement as well the demonstration of the requirement fulfilment (V&V) are taken into account already in the requirement design stage.

The safety engineering process focuses on the first hand to provide evidence for the licensing process. I.e. if the safety requirements are fulfilled it can be assumed that the plant is licensable.

Safety analyses are conducted in all stages of design. As the plant is operable, in the regular periodic safety reviews also safety analyses shall be renewed. When plant modifications are planned the potential changes are preliminarily analysed using appropriate methods like probabilistic safety analysis and deterministic safety analyses. When the design is ready the analyses are repeated for the relevant parts. If analyses in these stages show any weaknesses or faults in the design, the design is renewed and then the analyses are renewed.

Sometimes the need for plant modifications is found based on PSA results. Also changes in authority requirements or new operating experience can initiate plant modification (including just improvement of guidelines or procedures). In all these cases the analyses are used to support and validate the design and the requirement fulfilment.

For the LUHS event the plant design has been improved with several technical updates, the cooling towers as the latest improvement.

The overall safety engineering process could be improved to contain a wider view on safety in addition to the licensing stream. The flow of requirements and information could be described and followed more consistently.

**D.5.2 Description of the overall SEP and the flow of information in LUHS_2**

Plant response and fragility analyses are performed in all case studies within DSA. External event PSA is developed in the case studies. HRA is performed for human actions, evaluation of adequacy of modelling from the plant safety point of view is performed in all case studies.

In our understanding the HCLPF calculation is an adequate approach for interconnection of PSA and DSA. For comparison with other methods there is not enough information in the case studies.

**D.5.3 Description of the overall SEP and the flow of information in LUHS_3**

The safety engineering process (SEP) is not described in the detailed case study, it is only the flow of information between the safety analyses that are described.

The case study describes a process that has been ongoing for a long time period, initiated in part by actual events on similar designs, stress tests following the Fukushima accident, and in part by new regulations from the national authorities stating that external events should be considered in design. Therefore, re-qualification for fulfilment of the new regulations were initiated including the plants defences against LUHS events. The project followed the engineering process at the NPP used for plant modifications. The SEP is an integrated part in the engineering process, as described in the figure below.
The engineering process for plant modifications is based on the classical V-model as described in Deliverable 2.3. The SEP is integrated in the engineering process and is highlighted in the green boxes in the figure. An important phase is the iteration between incoming plant design/requirements, system design and safety assessment which is like the process described in figure 2 in Deliverable 2.3. The process described in the figure above in combination with the process of interactions between the different analyses forms the SEP. Since the SEP is not described in detail in the detailed case study description the case study will be updated with a description of the SEP.

**Safety requirements**

The incoming safety requirements in the case study is the requirement that SSC relevant for safety should be protected against external events including events with a frequency of $10^{-5}$/year.

**Supporting safety analyses**

The supporting analyses are described in the case study description and in the verification of requirements section above.

**Related plant design**

Based on the safety requirement and the supporting analyses the decision was to install the ICCS and to add certain FLEX equipment and procedures.

**D.5.4 Description of the overall SEP and the flow of information in LUHS_4**
Similarly to all operating Nuclear Power Plants in the European Union, a Targeted Safety Reassessment (so-called “stress test” (see IIb)) was performed for the NPP after the Fukushima nuclear accident in 2011. The national Nuclear Safety Code (Ia) and the ENSREG requirements (Ib) were taken into account (1a and 2a) in the stress test. Amongst others, the stress test focused on the analysis of plant response to a loss of ultimate heat sink event and on the evaluation of preparedness for such an event. Earlier, loss of cooling from the river as the ultimate heat sink had been screened out from those events that should be considered in the design basis or beyond, as the occurrence frequency of this event had been assessed as negligible due to either external or internal hazards. Accordingly, plant response analysis was performed (3a) deterministically first (IIc) by considering (6a) HFE (IId) aspects too. The analysis identified (5a and 6d) the need for introducing, amongst others, 9 safety enhancement measures (IIIa and IIIb) to successfully cope with loss of ultimate heat sink situations. These measures have been implemented since then.

All the measures related to providing direct water injection into the steam generators, the essential service water system as well as the spent fuel pools from external, low pressure water sources using mobile equipment with the support of the on-site fire brigade of the NPP were evaluated in the case study. It was examined whether these measures can effectively serve the purposes of accident mitigation in such situations. This analysis also supported (6c) the development of a detailed operational and transient mitigation strategy (IIIc) that should be followed in case of loss of ESWS. This strategy is being developed.

During the Periodic Safety Review (IIa) for the NPP, performed in agreement with the requirements of the Nuclear Safety Code (Ib), it was found that available hazard analyses did not enable a well-grounded conclusion whether events that can lead to loss of the ultimate heat sink due to the discharge of dangerous or harmful substances into the river could be screened out from hazards that needed to be considered in the design and that needed to be subject to detailed analysis to quantify risk or not. Additional hazard assessment (IIe1) for external events endangering the intake of cooling water from the river was performed using deterministic and probabilistic analyses in combination in order to better examine this issue (4a). The assessment was made in co-operation of water management experts (i.e. experts in water management, environmental sciences and biology) and PSA analysts. Consequently, hazard assessment is a manifestation of an integrated approach, considering deterministic, probabilistic, as well as HFE aspects simultaneously. With respect to HFE, the possibilities and conditions for preventing the blockage of the water intake facility by removing the harmful substances from the cooling water channel were considered (6b). The hazard assessment has resulted in a higher frequency for the occurrence of river contamination than the threshold of $10^{-7}/\text{y}$ set as a criterion for probabilistic screening used in the safety analyses of the plant.

Risk assessment (IIe) was performed for events that can cause loss of the ultimate heat sink due to the discharge of dangerous substances into the river. Plant response and fragility analysis was performed by making use of the findings of the deterministic plant response analysis (5b). PSA model development (IIe3)
built upon the results of hazard assessment (7a), and plant response and fragility analysis (Ile2; 8a) by exercising the commonly known tasks: event sequence modelling, fault tree analysis, human reliability analysis and input data assessment. As noted before, HRA within PSA and HFE in the overall safety analysis were largely interrelated activities (6e) during the development of PSA. The core damage risk attributable to external events endangering water intake was quantified and the main risk contributors were identified. Based on the quantified risk measures and risk contributors, some plant vulnerabilities were revealed and safety concerns were reported. The results and findings of the risk assessment can help further underpin the development of the strategy for coping with river contamination hazards (9a).

**Evaluation of Strengths and Weaknesses**

It can be concluded that the safety engineering practice was initiated by the conclusions of a periodic safety review and, indirectly, the stress test for the NPP. The relevant requirements were in the forefront of the analyses. The plant design was modified on the basis of deterministically driven plant response analysis. At a high level, the interrelationship of safety requirements, supporting analyses and related plant design may be regarded as acceptable. However, the scope of supporting analyses was less than complete when safety enhancement measures to better cope with loss of ultimate heat sink situations were identified and implemented. It was not foreseen at the beginning that all disciplines (i.e. DSA, PSA and HFE) should be addressed in the verification of the fulfilment of the relevant requirements. On one hand, hazard assessment had not been performed as a first step that would have underpinned the need for preparedness against such events. On the other hand, the process cannot be considered as a truly risk-informed approach as far as the use of PSA information is concerned because PSA insights had not been considered during the specification of the plant modification. PSA was performed only after implementing most of the proposed plant modifications. Moreover, there was no integrated, unified process or approach used when justifying the fulfilment of the relevant, multi-disciplinary requirements. It is noted that even though the plant modifications were identified on the basis of deterministic plant response analysis, further assessments, including hazard assessment and PSA for riverine events, verified the need and the sufficiency of the plant modifications implemented earlier. To sum up, it was a weakness in the safety engineering process that the different types of analyses pursued and the plant modifications made to verify the requirements were not performed in an integrated manner, and by considering the different aspects in combination and in parallel.

**Proposals for Improvement**

During the identification and implementation of safety enhancement measures to successfully cope with external hazard induced scenarios not considered originally in the design of an NPP, an action plan and a road map should be developed that integrates the various analysis types necessary for verification. Of particular importance is planning of the interconnections among the different types of analyses and analysis steps, including the definition of milestones, application of unified input data, scheduling meetings to be organised to inform each other on intermediate or final results of a certain analysis type. A generalist expert should be nominated to be responsible for task coordination and follow up. A reasonable order of work should be determined among the areas of DSA, PSA and HFE. Plant modifications and requirement justification should consider the results from all the analysis areas in an integrated manner (i.e. no plant modification is allowed until all the analyses are completed). System modifications should be designed by considering both deterministic aspects and PSA insights. This approach seems much more effective than subsequent system modifications based on the DSA and PSA results separately. Similarly, all the insights obtained from HFE and PSA should be taken into account when developing operating procedures, elaborating training programmes, defining the appropriate tools and equipment, etc. related to the use of portable equipment. This would ensure better risk-informed decision making and better substantiated plant modifications, as opposed to considering the findings from different types of assessment separately.

**D.5.5 Comparison of the overall safety engineering process**

Comparison of the overall safety engineering process described above is provided in Table D.4.
### Table D.4: Characterization of the Overall Safety Engineering Process.

<table>
<thead>
<tr>
<th>LUHS_1</th>
<th>LUHS_2</th>
<th>LUHS_3</th>
<th>LUHS_4</th>
<th>Conclusions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Overall approach and steps of the SEP</strong></td>
<td>Plant response and fragility analyses are performed in all case studies within DSA. External event PSA is developed in the case studies. HRA is performed for human actions, evaluation of adequacy of modelling from the plant safety point of view is performed in all case studies.</td>
<td>Initiation of the case study is operation experience from similar designs, stress tests following the Fukushima accident, new regulations from Swedish authorities. The steps of the SEP are as described in Figure D.9.</td>
<td>National regulatory and ENSREG requirements -&gt; Stress test and PSR -&gt; safety analyses (DSA, PSA, HFE) -&gt; plant design (technical measures, operating procedures; operational and transient mitigation strategy). Safety analyses: 1. Deterministic plant response analysis (DSA); 2. Human Factors Engineering (ensure adequate contamination removal); 3. PSA (hazard assessment, plant response and fragility assessment, PSA model development, risk quantification and interpretation of results).</td>
<td>New or modified requirements (regulatory requirements, experienced initiating events on similar plants etc.) trigger the SEP. The needs of the analyses and their interconnections are defined in the early stage.</td>
</tr>
<tr>
<td>- Objective definition at the preparation phase,</td>
<td>- Collecting stakeholder requirements</td>
<td>- Defining the concept and architecture of the design</td>
<td>- Basic and detailed design</td>
<td>- Manufacturing</td>
</tr>
<tr>
<td>- Elaborating system requirements</td>
<td>- Verification of all design steps</td>
<td>- Integration and factory tests, also provide verification of the system requirements</td>
<td>- Installation tests, also provide validation of the stakeholder requirements</td>
<td>- Commissioning tests</td>
</tr>
<tr>
<td>- O&amp;M (&amp;Decom)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Interrelationship among the Steps</td>
<td>LUHS_1</td>
<td>LUHS_2</td>
<td>LUHS_3</td>
<td>LUHS_4</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>--------</td>
<td>--------</td>
<td>--------</td>
<td>--------</td>
</tr>
<tr>
<td>In all stages the previous stage design is verified to confirm that the transformation of inputs (= requirements) to outputs (design and/or requirements for the subsequent stage) has been done according to the requirements and that no errors or faults have been introduced.</td>
<td>In our understanding the HCLPF calculation is an adequate approach for interconnection of PSA and DSA. For comparison with other methods there is not enough information in the case studies.</td>
<td>See Table 3.</td>
<td>See Table 3; technical measures based on deterministic plant response analysis and HFE (PSA only for verification purposes); PSA insight: develop a strategy for coping with river contamination hazards.</td>
<td>Verification throughout the process connects the steps; the HCLPF is adequate for the connection between PSA and DSA; PSA only used for verification – could be used to provide insights for developing strategies.</td>
</tr>
</tbody>
</table>

--> Every SEP step verifies the design of the preceding step.

| Strength of the SEP | Defined, streamlined and transparent approach | A very widespread method and the software is available for application. | The process describes the relation between requirements, safety analyses and plant design. | Defined and transparent; describing relation between safety requirements, safety analyses and plant design |

[945138] BESEP – Benchmark Exercise on Safety Engineering Practices  Page 139/214
<table>
<thead>
<tr>
<th>Weaknesses of the SEP</th>
<th>LUHS_1</th>
<th>LUHS_2</th>
<th>LUHS_3</th>
<th>LUHS_4</th>
<th>Conclusions</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>For smaller projects/tasks, full scope SEP is too heavy, but on the other hand, the SEP can be down-scaled.</td>
<td>Conservative results to confirm the safety of the plants.</td>
<td>Graded approach towards size of the project is difficult.</td>
<td>the different types of analyses pursued and the plant modifications made to verify the fulfilment of the requirements are not the result of a fully and properly integrated approach/framework and thus there is a lack of systematic considerations to the different aspects in combination and in parallel.</td>
<td>Scaling the scope of the SEP; it gives conservative results; systematic consideration of the different aspects in combination and in parallel is required for an integrated approach.</td>
</tr>
<tr>
<td>Proposals for Improvement</td>
<td>SEP could include better description or definition on the cross-connections for the different kind of analysis conducted on the different SEP steps.</td>
<td>To remove the conservatism from FEM analyses.</td>
<td>During the early steps of the process, it is beneficial to investigate operational experience, what resources in terms of already performed analyses are there, and are there any important human actions.</td>
<td>an action plan (including a road map) should be developed that integrates the various types of analysis necessary for verification; planning of the interconnections between the different types of analyses and analysis steps; plant modifications and requirement justification should consider the results from all the analysis areas in an integrated manner.</td>
<td>Better definition on cross-connections for analyses performed in different SEP-steps; remove conservatism from FEM analyses; an action plan for integrating the various analyses necessary based on operational experience, already performed analyses and important human actions, the results from analyses should be linked to plant modification and requirements.</td>
</tr>
</tbody>
</table>
Based on the self-evaluations of LUHS_2 and LUHS_4 it can be concluded that SEP approach is case-dependent for these cases. No common pattern or general guideline exists. In the LUHS_1 case a general SEP approach has been described. The safety engineering practice defined for LUHS_4 follows the similar steps and information flows as for LUHS_1. LUHS_1 SEP is based on requirements, management of them as well as verification and validation of the design based on the requirements. The safety engineering process focuses on the first hand to provide evidence for the licensing process. I.e. if the safety requirements are fulfilled it can be assumed that the plant is licensable.

In LUHS_1 the (changed/ updated) stakeholder requirements are one of the triggers for the SEP. In LUHS_4 triggers are the need to conduct stress test or the periodical safety review. In LUHS_3 the triggers have during a longer time period been actual events on similar plant designs, need to conduct stress test and new regulatory requirements. These can be interpreted as stakeholder requirements, so the starting point of SEP is similar. For LUHS_2 no specific starting point for SEP has been described.

For LUHS_1 and LUHS_3 it is common, that as the case studies describe a set of analyses and improvements conducted during a longer time period and based on multiple triggers, the SEP described in them is rather a generalized description of the process applied than an exact description of the process defined for the case study. LUHS_1 and LUHS_3 follow the basis of the classical V-model as described also in Figure 2 in Deliverable 2.3. SEP is an integrated part of the engineering process, as defined also for LUHS_4.

The described flow of information in LUHS_1, LUHS_3 and LUHS_4 is identical. Requirements initiate the safety analyses, analyses provide input for other analyses and for plant, strategy or procedure modification. Also the flow in LUHS_2 follows the same pattern, but in more detail, as LUHS_2 is more of a PSA case than the other case studies, it contains larger variety of analysis methods.

Strength in the SEP process of LUHS_1 is the transparency of the flow of requirements. Strength is also, that SEP provides direct support to licensing the plant/ modifications. Weakness in the SEP approach used in LUHS_1 is that concentrating on the licensing other safety or usability related issues as well as the effects of human performance may get passed by.

SEP for LUHS_2 concentrates on the PSA side of the process. It is sufficient for the case study, but other cases would need more comprehensive SEP approach that is not described in LUHS_2, so no evaluation on the SEP process outside PSA can be provided.

The SEP in LUHS_3 is initiated by actual events on similar designs, stress tests following Fukushima, new regulations from the national authorities.

SEP for LUHS_4 was initiated by the conclusions of a periodic safety review and, indirectly, the stress test for the NPP. Weakness in the selected/ defined SEP in LUHS_4 was that it was not foreseen at the beginning that all disciplines (i.e. DSA, PSA and HFE) should be addressed in the verification of the fulfillment of the relevant requirements. PSA was performed only after implementing most of the proposed plant modifications even though it would better support safety when performed also for the design. Also, lack of integrated, unified process or approach used for justifying the fulfillment of the relevant, multi-disciplinary requirements should be cleared.

D.5.6 Proposals for improvement

Safety Engineering Process should be defined in general for the design and safety engineering organisations. When identifying a need for an improvement or study, the general SEP should be taken as a basis and then modified to fit to the improvement or study identified. As learned in the case studies, during the identification and implementation of safety enhancement measures to successfully cope with external hazard induced scenarios not considered originally in the design of an NPP, an action plan and a road map should be developed that integrates the various analysis types necessary for verification. Also it should be defined beforehand, what evidence is needed to fulfill the requirements and how that is reached, by considering and addressing all disciplines (i.e. DSA, PSA, HFE).

Information flows should be addressed and it should made visible or at least taken into account in the process how the changes at the upper level would be implemented in a way that it includes all disciplines.
Also, in the case studies the HFE area has been in a minor role. A further improvement for SEP would be a more in-depth application of HFE. The scope of a project should include operational experience and should account for the important human actions affected by the possible design change.

The overall safety engineering process could be improved to contain a wider view on safety in addition to the licensing stream or PSA. The flow of requirements and information could be described and followed more consistently.

D.6 Key success factors for an efficient and integrated SEP

Based on the conclusion and comparison of the group LUHS case studies, the following key success factors for an efficient and integrated SEP can be defined:

- the preferred main flow of information and actions: hazard analysis -> plant response analysis -> PSA model -> plant design
- the safety analyses and their interconnections should be defined,
- analyses should provide feedback to the design process and the modified design should be again analysed,
- a safety graded approach should be applied by defining how deep the analysis should be and what analysis are the most important,
- evidence of the safety requirement fulfilment should be established via the pre-defined analyses and their interconnections.

The generalized safety engineering process for the group LUHS reflects all the key success factors described above. Three levels are defined in the SEP:

- level 1, the interactions between (safety) requirements, analyses and plant design
- level 2, the interactions between DSA, PSA, HFE
- level 3, the interactions within DSA, PSA or HFE analyses.

On level 1, new or modified regulatory requirements, changes in operating environment or in the scope of occurred events at other NPPs trigger the start of the SEP. After evaluating the trigger new requirements shall be elaborated for the systems or analyses. Plant modifications and requirement justification should consider the results from all the analyses in the three disciplines (DSA, PSA, HFE) in an integrated manner (i.e. no plant modification is allowed until all the analyses are completed and verified). This is again part of level 1 SEP as defined above. System modifications should be designed by considering both deterministic aspects/reasoning and PSA insights. This approach is seen superior to planning system modifications based on the separate uses of DSA and PSA results. In defining and conducting the analysis due consideration shall be given to the actual need or problem, not to gaining the solution as fast as possible. Sometimes the ideal solution can be discovered after investigating the original problem better.

Similarly, all the insights obtained from DSA, HFE and PSA should be taken into account when developing operating procedures, elaborating training programmes, defining the appropriate tools and equipment, etc. related to the use of special-purpose means of accident mitigation or management (most importantly, portable equipment) and dedicated human resources. This would ensure better risk-informed decision making and better substantiated plant modifications, as opposed to considering the findings from the different types of safety analyses one by one.

The common flow of information and actions follows the line hazard analysis -> plant response analysis -> PSA -> plant design, but there can and also should exist connections and back-loops between the parts.

On level 2 of the SEP, an action plan and a road map should be developed to integrate the various types of analyses within the three analysis disciplines (DSA, PSA, HFE) to be performed in support of the verification. Careful planning of the interconnections among the different types of analyses and analysis steps including the definition of milestones, application of unified input data, scheduling and organizing meetings for information exchange on intermediate or final results of a certain type of analysis type is of utmost importance. A generalist expert should be nominated to bear the responsibility of task coordination and follow up. The order of work and sub-tasks should be determined for DSA, PSA and HFE, respectively. Figure D.11 illustrates the
engineering process used in LUHS_3, which is a good basis also for the generalised SEP. SEP level 1 and partly 2 are visible in the Figure.

**Figure D.11: Engineering process for generalised SEP**

On level 3 of the SEP, one important process is the safety graded approach. It is conventionally seen as a part of HFE but it is very useful for DSA and PSA too for defining the scope and methods, i.e. the resources used for the analyses. With graded approach it can be defined whether using engineering judgement is sufficient or are exact (and often time consuming) calculations and numeric analyses necessary.

Figure D.12 presents the PSA-based view on the generalised SEP for the LUHS case study group based on case study LUHS_2. In the upcoming work, this SEP will be supplemented with more viewpoints on other analysis disciplines (DSA, HFE) and other information interconnections between analyses.
Figure D.12: SEP for the generalized case study

For the HFE process for design considering DEC external events the process element of important human actions (IHA) is prominent. During this step it should be iterated over the safety analyses what are the intended human actions. When the intended human actions are identified the HFE process aims to ascertain that the human actions can be performed by the operators. This step is perhaps the most important when it comes to the interaction between the HFE process and safety analyses. When considering the SEP for cases with possible change in the design for DEC external events it would be beneficial for the development of the safety analyses that the operational experience review is performed as a part of screening steps in PSA and DSA. It is to ensure that the effects the change has on the operating personal are properly addressed.

One interpretation of safety margin is given in Figure D.13. It is defined as a margin of failure between the operating point and the failure point. It consists of the margin available to licensee, the value between operating point and safety limit, and of the margin established by regulations/requirements, the value between safety limit and failure point. Depending on the case, the safety margin can be based on expert judgement instead of direct calculations. The safety margin can also be interpreted e.g. as availability or reliability of the countermeasures instead of the pure size or magnitude of the initiating event. It is also possible, that the safety margin is just one frequency for the probability of the initiating event group.
One further possible development issue in generalised SEP or SEP in general is the need of analyses also before the so called pre-study phase, i.e. before actually any development or upgrade decision exists. It would be helpful to have a guideline or general instructions how to plan the analyses and their interconnections also in these cases.
APPENDIX E: CROSS-CASE COMPARISON IN CASE STUDY GROUP PVES

E.1 General information

Responsible Organization(s): NUBIKI, Risk Pilot, UJV

Case Study Group Identifier: PVES

Date: 23/09/2022

Case Study Titles:
- Snow and Wind Affecting Diesel Generators (PVES_1)
- Protection of the Reactor Hall from the Effects of Extreme Snow (PVES_2)
- Analysis of Extreme Snow Risk (PVES_3)

E.2 Fulfilment of BESEP Safety Requirements

The responsible organizations of the PVES (Plant Vulnerability to Extreme Snow) case study group agreed on focusing the comparative assessment regarding the fulfilment of BESEP safety requirements to a limited number of requirements, namely on those that seemed the most relevant ones to each case study and may serve as a good basis for benchmarking. In order to enable a thorough review that adequately considers the specifics of each case study in this case study group, each partner updated their self-evaluations by addressing all of these BESEP requirements. Hence, the fulfilment of the following BESEP safety requirements was addressed in every case:

- Physical separation and structural integrity (DSA):
  - **BESEP_DSA_PSEP_002**: The systems, structures and components, including auxiliary or supporting systems thereof shall be protected from the effects of external hazards as far as reasonably practicable.

- Justification of the engineering assumptions used in analysis (DSA):
  - **BESEP_DSA_JEA_001**: The engineering assumptions applied in conducting the deterministic safety analysis shall be appropriately justified.

- Support to developing abnormal and emergency operating procedures and severe accident management guidelines (PSA):
  - **BESEP_PSA_EOP_001**: PSA shall be used to support the development of abnormal and, emergency operating procedures and severe accident guidelines considering aspects that may influence the activities and performance of operating personnel.

- Guidance selection, decision making and intelligent use of guidance (HFE):
  - **BESEP_HFE_GS_001**: The procedures and guides designed for any event shall be easy to identify and select during the event.
  - **BESEP_HFE_GS_002**: The procedures and guides shall be designed to support the human performance in decision making.
  - **BESEP_HFE_GS_003**: The procedures and guides shall be designed taking into account the human capabilities and limitations and the human reliability analyses.

- Safety design and requirement management for external hazards (SE):
  - **BESEP_SEP_SDRM_003**: The design basis hazard factors shall be selected based on site-specific analysis. They shall be specified based on the hazard curve, taking into account the screening criterion applicable to the given hazard factor. The analysis shall be performed by deterministic methods, and based on the state-of-the-art results of science and technology by probabilistic methods.
  - **BESEP_SEP_SDRM_007**: The decision whether a given hazard of low probability is relevant for the nuclear safety of the power plant, shall be based on engineering judgement, for example using fragility curves.
  - **BESEP_SEP_SDRM_010**: The applicability of the standards selected for the design process shall be justified.
The fulfillment of these requirements was subject to comparative assessment as follows.

Requirement No. 1. – BESEP_DSA_PSEP_002: The systems, structures and components, including auxiliary or supporting systems thereof shall be protected from the effects of external hazards as far as reasonably practicable.

Summary of the Verification Process

To justify the protection of the relevant building structure(s) of an NPP against the effects of extreme snow, an evaluation was made in each case study whether the structure(s) can reassuringly withstand the design basis as well as the beyond design basis snow load or not. The requirement in question was verified primarily on the basis of the structural strength analysis. This corresponds to a traditional deterministic safety analysis belonging to structural engineering. The analyses were based on widely accepted standards (e.g. Eurocode) or on well-elaborated methods that can be regarded as state-of-practice for structural strength verification of buildings.

The steel superstructure of the reactor hall is in the focus of one of the case studies. The results of the detailed structural re-analysis confirmed that each structural element meets the Eurocode requirements, except for two top chord members. It was concluded that strengthening these two chord members were needed to ensure appropriate protection against design basis loads. Subsequently, a detailed design of structural reinforcement was developed and plant modifications were implemented accordingly. Fragility analysis of the reactor hall was also performed to further underpin the protection against beyond design basis loads. This analysis was based on structural strength as well as structural reliability analyses. As a result, it could be concluded that the reactor hall steel superstructure can withstand the design basis loads, and safety margins beyond the design basis loads exist, as ensured by fulfilling the Eurocode requirements. In another case study, a similar structural reinforcement was performed on the emergency diesel generators building to ensure adequate protection against design basis snow loads. Moreover, the protection of combustion air intake from the effects of snow was analysed and evaluated to verify the operability of the emergency diesel generators during extreme snow storm. The third case study included a consequences assessment of roof collapses by determining the loss of systems and components located in the different buildings. Structural strength analyses were performed and fragility curves were developed for each safety related building in this case study.

Adequacy of Verification

The development of a detailed finite element structural model and the application of widely accepted standards are regarded as the state-of-practice for verifying the structural strength of a building. Structural reinforcement was made in two case studies by following commonly accepted civil engineering practices. Moreover, fragility curves were also established in two of the case studies based on state-of-the-art approaches to ensure sufficient protection against beyond design basis loads. In one of the case studies, the blockage of the air intake system was evaluated in a qualitative manner for the diesel generator building.

Overall, it can be concluded that the fulfillment of the given requirement can be considered complete with high technical quality in each case study.

Proposals for Improvement

As described above, the requirement in question should be verified primarily on the basis of the structural strength analysis of the affected building structures, i.e. a traditional deterministic safety analysis belonging to structural engineering. Fragility analysis should also be performed to further underpin the protection against beyond design basis loads. In one of the case studies, it was stated that these two different tasks were performed independently of each other. The process of verifying the fulfillment of the given requirement could have been refined by performing the two types of analysis in combination and by the same expert group, as several clarifications and time consuming technical discussions were needed when performing fragility assessment on the basis of the structural analyses. In another case study, the fragility curves have not been elaborated so far; however, it could further underpin the protection of the building in question against beyond design basis loads. In the third case study, the conservatism in the assessment needs to be decreased by means of additional structural analyses.
Requirement No. 2. – BESEP_DSA_JEA_001: *The engineering assumptions applied in conducting the deterministic safety analysis shall be appropriately justified.*

**Summary of the Verification Process**

Structural strength analysis was the primary deterministic safety analysis in the different case studies. The analyses were based on widely accepted standards (e.g. Eurocode) or on well-elaborated methods that can be regarded as state-of-practice for structural strength verification of buildings. The self-evaluation sheets do not specify the justification aspects of engineering assumptions applied in the analyses; however, it is stated that these assumptions are described and justified in sufficient detail in all cases. It was also mentioned in one case that engineering assumptions were implicitly included in the calculations via the relevant standards that can be regarded as widely accepted and justified. One case study regarded the vulnerability assessment of indoor safety systems and components due to roof collapse as an additional deterministic analysis. In this analysis, engineering judgement was applied taking into consideration, amongst others, general vulnerability characteristics and location of components.

**Adequacy of Verification**

According to the self-evaluations, the verification processes of the given requirement applied in the different case studies can basically be considered adequate for structural strength analyses. The verifications are based on the fact that the relevant standards and methods used rely on justified assumptions. In one case study, the vulnerability assessment of safety systems and components due to the collapse of the roof was regarded as a deterministic analysis, where some further improvements seem necessary to fully verify the requirement. Although, good practices for justification of engineering assumptions are not presented in the self-evaluation sheets, it is seen essential to describe all engineering assumptions applied in the deterministic safety analyses in the analysis documentation and to justify the assumptions as thoroughly, as possible.

**Proposals for Improvement**

Ideally, to verify the fulfilment of the given requirement, all applied engineering assumptions should be listed and justified. Although it may not fully be feasible, it is essential to describe each and every engineering assumption in sufficient detail and substantiate their selection and application as much as possible. Justification of engineering assumptions may be based on substantially different approaches depending on the type of the assumption in question as well as on the available methods and information. Experimental data, relevant literature, and validated and verified targeted assessments should be aimed at; however, it may not always be realistically feasible to meet all these conditions. The application of reasonably conservative assumptions and addressing the aspects and information that have been taken into account can be an acceptable verification process to fulfil the BESEP requirement in question.

Requirement No. 3. – BESEP_PSA_EOP_001: *PSA shall be used to support the development of abnormal and, emergency operating procedures and severe accident guidelines considering aspects that may influence the activities and performance of operating personnel.*

**Summary of the Verification Process**

It was recognized in each case study that the occurrence of snow-induced transients can be prevented, if snow is removed from the affected plant areas, important to plant safety, in a timely manner. In one case study, PSA was not applied to support the development of any operating procedures or severe accident management guidelines related to extreme snow situation; PSA identified only the need that some procedures or guidelines should address extreme snow situations. In the other two cases, the snow PSA included detailed human reliability assessment. Based on the lessons learned from the analysis, a proposal was developed on how to modify the available procedures and guidelines to ensure more reliable snow removal or accident mitigation. Attempts were made to identify and evaluate the key influences on snow removal activities and on the associated success rate to substantiate the proposals for procedure improvements. In one of the self-evaluation sheets the key analysis steps to underpin the proposals for safety enhancement are also presented.
Adequacy of Verification

In one of the case studies, PSA was not applied to support the development of any operating procedures or guidelines related to extreme snow situation. Regarding the other two case studies, the relevant operating procedures and guidelines related to snow removal or accident mitigation had been elaborated before the snow PSA was completed. Consequently, PSA was applied to review and to further improve the relevant operating procedures and guidelines, since the strategy had originally been developed without giving explicit considerations to risk aspects. However, the risk-informed review can be considered a sufficiently detailed evaluation that included the elaboration of new approaches.

Proposals for Improvement

It is seen advantageous to utilize PSA and PSA insights as an integral part of developing operating procedures for coping with external events, rather than making use of risk insights in a follow-on manner, i.e. mostly for the purposes of reviews. This finding is well supported by the fact that external hazards are generally important contributors to plant risk. Such uses of risk assessment and risk insights can help establish the basis of the operational and mitigation strategy including the identification of the most important cornerstones, instead of making only adjustments to the available strategy laid down previously by using deterministic considerations only.

In case of a risk-informed review, the following key analysis steps can usefully underpin the proposals for procedure improvement:

- identification of the most important performance shaping factors relevant to the success of snow removal;
- review of the snow removal strategy;
- evaluation of the plant procedures and associated arrangements in place for snow removal with considerations to the influencing factors identified in the first step;
- quantification of failure to remove snow from the roofs based on an evaluation of the applicable plant procedures and other relevant influences on performance.

Requirement No. 4. – BESEP_HFE_GS_001: The procedures and guides designed for any event shall be easy to identify and select during the event.

Summary of the Verification Process

There is a dedicated operating procedure in place at each plant addressed in the case studies that controls, amongst others, snow removal activities. This procedure is generally applied in case of various external events where preparatory actions are feasible. Extreme snow can be forecasted a few days in advance, hence there may be sufficient time to take such actions. In one case, the actions specified in the procedure depend on the severity of warning of the national meteorological institute. As there is enough time to start snow removal from the roofs of safety related buildings, the identification and selection of the relevant procedure can be considered simple and straightforward in all cases. Moreover, if a certain initiating event occurs due to extreme snow, the relevant emergency operating procedure should be followed by the control room crew in the main control room. These procedures are self-evidently easy to be identified and selected in a transient situation.

Adequacy of Verification

Even if no detailed, targeted assessments were performed, the verification process can be regarded as adequate in each case study. The identification and selection of the relevant procedures and guides to be applied during heavy snowfall are ensured. This statement can be well supported by the fact that these procedures have already been efficiently used many times in harsh weather conditions, including extreme snow too, in one case. It is noted that the evaluation of identifying and selecting the snow removal procedure was in the focus of the case studies; the usability of the whole set of procedures, as well as specific methods to verify the usability were not addressed.

Proposals for Improvement
No detailed justification seems necessary to verify the fulfilment of the given BESEP requirement, as there is sufficient time to start snow removal from the roofs of safety related buildings, and the identification and selections of the relevant procedures or guidelines can be considered self-evident in such situations. This statement can be well supported by the fact that these procedures have already been efficiently used several times in harsh weather conditions including extreme snow. It may be reasonable to extend the scope of the requirement verification by addressing the usability of the whole set of procedures, as well as specific methods for the verification of the usability of plant procedures.

Requirement No. 5. – BESEP_HFE_GS_002: The procedures and guides shall be designed to support the human performance in decision making.

Summary of the Verification Process

There is a dedicated operating procedure in place at each plant addressed in the case studies that controls, amongst others, snow removal activities. Two of the case studies deal with the verification of requirement fulfilment from the point of view of this operating procedure, whilst the third one focuses on emergency operating procedures to be used by the control room crew in general, regardless of the underlying initiating event or external hazard. It seemed reasonable to concentrate the comparative analysis presented hereby on those case studies that address the procedures that control snow removal activities. In one of these case studies, the main decision points during the whole snow removal process are identified as follows:

- preparation for timely snow removal activities;
- starting the snow removal activities in time, criteria to begin work;
- selection and prioritization of buildings to be protected;
- permanent disposition of removed snow.

The potential support provided by procedures to these decision points is identified and evaluated too.

According to the other relevant case study, preparation for timely snow removal is initiated on the basis of warnings by the national meteorological institute. The procedure that controls snow removal gives information on how to prioritise snow removal activities and when to start them.

Adequacy of Verification

The operating procedure that controls snow removal activities is designed to support various aspects of the decision making, e.g. starting snow removal activities in time and criteria to begin work. An evaluation of the support provided by the procedures to the main decision points should be the basis of verification. In one of the case studies, some areas were identified in the procedures in place that cannot be regarded as comprehensive or sufficiently detailed. These deficiencies should be removed. In the other relevant case study, it is stated that no dedicated assessment has been performed to verify the fulfilment of the given requirement.

Proposals for Improvement

In one of the case studies, it is stated that the organisations’ capabilities to follow the procedures could theoretically be assessed, but seems unfeasible. In another case study, the need for safety enhancement with respect to improving human performance in decision making was summarized as a proposal for improvement to the current practice.

In summary, to verify the fulfilment of the given requirement, the support provided by the relevant procedures to the following main decision points during the snow removal process should be evaluated and its adequacy justified:

- preparation for timely snow removal activities including measures to ensure the availability of tools and equipment;
- starting the snow removal activities in time, criteria to begin work;
- selection and prioritization of buildings to be protected;
- permanent disposition of removed snow.
Requirement No. 6. – BESEP_HFE_GS_003: *The procedures and guides shall be designed taking into account the human capabilities and limitations and the human reliability analyses.*

**Summary of the Verification Process**

Similarly to the verification of requirement no. 5, one case study focused on the evaluation of the control room crew activities not the snow removal from the roofs; hence it was not found reasonable to include the verification process of this case study in the comparison. In one of the self-evaluation sheets it was described that the feasibility to perform the actions prescribed in the procedures has not yet been fully verified with respect to the capability and availability of personnel during an extreme snow event. The verification so far considered mainly the availability of pre-warnings and relevant equipment.

In another case, an attempt was made to identify and evaluate the key influences on snow removal activities and on the associated success rate to substantiate the proposals for procedure improvements. The key analysis steps to underpin the proposals for safety enhancement are also presented in the corresponding self-evaluation sheet. It is highlighted that the following influencing factors were also found important to successful snow removal:

- environmental conditions induced by extreme snowfall, physical circumstances of task execution
  - accessibility;
  - persistent snowfall (possibly snowstorm) and performance aggravating effects due to accumulated large amount of snowpack;
- organizational conditions, resources of staff and equipment
  - organizational conditions;
  - assurance of standby staff for snow removal – manpower and fitness for duty;
  - equipment needs.

Consequently, human capabilities and limitations including also the physical circumstances of task execution were considered and use was made of human reliability analysis during a risk-informed review of the operating procedures. Based on the output of the evaluation, an increase in the number of persons to remove snow seemed necessary at least by involving additional plant staff. It was found of high importance to incorporate training on the use of the relevant organizational plan into the training program of all the plant staff involved in snow removal.

**Adequacy of Verification**

In one of the case studies, the feasibility to perform the actions prescribed in the procedures was not fully verified with respect to the capability and availability of personnel during an extreme snow event. Human capabilities and limitations were evaluated and human reliability analysis was performed in the other relevant case study to identify and evaluate the key influences on snow removal activities and on the associated success rate. Due to significant limitations in applicable data, expert judgement played an important role in human reliability analysis. The organizational plan was studied and evaluated by making use of the HRA findings and performing targeted qualitative evaluations.

**Proposals for Improvement**

In one of the case studies, it is stated that the organisations’ capabilities to follow the procedures could theoretically be assessed, but seems unfeasible. In another case study description, it is highlighted that when developing procedures for local actions of plant crew, multi-unit aspects need to be considered in the assessment of human capabilities and limitations. An alternative approach to verify the fulfilment of the requirement could be to quantitatively assess human capabilities and limitations with respect to snow removal, i.e. to assess the amount of snow that may be removed by an individual during a single shift. In addition, the amount of snow that needs to be removed from the roofs of all safety related buildings could be assessed too, considering different snowfall intensities and durations. A comparative analysis can refine the expert judgement that determines the manpower necessary for successful snow removal.

Requirement No. 7. – BESEP_SEP_SDRM_003: *The design basis hazard factors shall be selected based on site-specific analysis. They shall be specified based on the hazard curve, taking into account the screening...*
criterion applicable to the given hazard factor. The analysis shall be performed by deterministic methods, and based on the state-of-the-art results of science and technology by probabilistic methods.

Summary of the Verification Process

The objective of hazard assessment for extreme snow is to determine exceedance frequencies for different magnitudes of the parameter that represents best the load induced by extreme snow. In each case study, hazard assessment was based on the data collected by the national meteorological service at a station near the NPP during the past few decades (in one of the case studies the data for snow was estimated based on site specific data on rain since no data specific for snow was available). The main difficulty in determining the occurrence frequency of extreme snow is the lack of observations for the events that should be subject to statistical estimation, since data samples from experience are available for a relatively short period only. The results are subject to significant uncertainty, whatever computational method is applied. In accordance with the international practice of climatological applications, use was made in each case study of the extreme value theory to characterize and quantify the extreme snow hazard. The national nuclear safety regulations prescribe the exceedance frequency of loads that should be considered in design basis for loads from natural external hazards, hence the plant design basis value needs to be defined considering the results of the hazard assessment as the return value corresponding to this predefined exceedance frequency. In two case studies, the design basis values were defined in line with this approach. In the third case, plant specific hazard assessment was performed in the framework of PSA; however, no detailed analysis was performed to ensure that the design basis values derived earlier from the use of some general principles are plant specific.

Adequacy of Verification

All the self-evaluations suggest that the verification of requirement fulfilment can be regarded as adequate. In two case studies, it is described that plant design basis was defined on the basis of a site-specific analysis, considering the applicable hazard curve and the prescribed screening value set in the national nuclear safety regulations. The analyses were based on state-of-practice probabilistic methods. Furthermore, in one of the case studies it is also highlighted that the SEP for design considers all relevant requirements for the SSCs involved in the design process including requirements on protection against relevant external events.

Proposals for Improvement

In one of the case studies, no improvement was identified. In another one, it is noted that more site-specific information could be used when setting the design basis values; however, according to the responsible organization, it is not seen useful or necessary for extreme snow. According to the third case study, even if hazard assessment can be regarded as state-of-practice, regional data and further methods should also be used to verify the design basis value as well as the assessed hazard curves.

It can be concluded that the plant design basis should be defined by means of a site-specific analysis, considering the applicable hazard curves and the prescribed screening value set in the national nuclear safety regulations. The analyses have to apply state-of-practice probabilistic methods, e.g. by using the extreme value theorem. The case studies seem adequate in this respect. However, it is also seen useful to collect and process (1) data measured for longer time periods in other meteorological stations, and (2) historical data. The use of some further analysis methods may be advantageous too. A comparative analysis of the hazard curves established for European NPP sites would also be beneficial to verify the design basis values as well as the assessed hazard curves.

Requirement No. 8. – BESEP_SEP_SDRM_007: The decision whether a given hazard of low probability is relevant for the nuclear safety of the power plant, shall be based on engineering judgement, for example using fragility curves.

Summary of the Verification Process

In one of the case studies, the fulfilment of this requirement was verified on the basis of defining the design basis load considering the return value corresponding to $10^{-5}$/a exceedance frequency of snow load, rather than establishing fragility curves. The value assessed in this manner is in good agreement with the international practise as well as with the requirements of the national regulations. Beyond design basis loads were not
assessed directly; however, PSA was performed considering the same design basis value in the plant response analysis.

In the other two case studies, the probability of loss of essential safety functions for different levels of snow load was described by means of fragility curves. The effects of snow load on structures and outdoor facilities were analysed in detail for the purposes of plant response analysis. To satisfy the corresponding safety regulations, the risk from snow beyond the design basis was assessed at least to $10^{-7}$/a occurrence frequency. The PSA results show that the risk from extreme snow is moderate or high in comparison to the risk originated from other types of initiating events analysed in the PSA for the different NPPs. The results of structural strength analysis confirmed the importance of the effects of extreme snow on plant safety.

**Adequacy of Verification**

In one of the case studies, the verification of the requirement fulfilment is seen adequate by defining the design basis load appropriately. The use of this load value resulted in the re-construction of the roof of the emergency diesel generator building to enhance the safety of the plant. In the other two case studies, the verification is considered adequate, as the risk due to beyond design basis loads was quantified utilizing hazard as well as fragility curves considering loads with sufficiently low exceedance frequencies.

**Proposals for Improvement**

Only one proposal was specified for improvement, namely to establish and use fragility curves in order to enhance the realism in the assessment. It can be concluded that the fulfilment of this requirement can be verified regarding plant vulnerabilities due to snow, if risk due to beyond design basis loads was quantified utilizing hazard and fragility curves. The conditional core damage probability or large early release probability for different snow load intensities or intensity ranges may be a good metric for use in a comprehensive verification process.

**Requirement No. 9. – BESEP_SEP_SDRM_010:** The applicability of the standards selected for the design process shall be justified.

**Summary of the Verification Process**

In the different case studies, the structural strength analyses (design processes) were based on:

- guidance issued by the national regulator that adapts the content of widely used international standards (e.g. Eurocode);
- specific national normative document for specification of critical load for the rooftops of plant buildings;
- Eurocode standard system or an earlier national standard series.

In the first two cases, the national legislative documents have been applied, that have the first priority in the design process; hence the applicability of the standards used were considered justified. In the third case an attempt was made to apply the Eurocode standard system during the structural re-analysis of the safety related buildings both for steel and for reinforced concrete structures. However, it was not found feasible to fully meet all the requirements of this standard in the analysis. Consequently, if the capacity of a structure could not be justified within the prescriptive Eurocode standard framework, then the superseded national standard series was applied. Furthermore, the analysis was done primarily on the basis of the Eurocode; however, complementary analysis was performed using some designated parts of the national standard. Based on a comparison of the different standards from theoretical point of view, it was concluded that the fulfilment of the Eurocode requirements ensures a higher safety level for reinforced concrete structures than the fulfilment of the prescriptions laid down in the national standard. However, for steel structures, the use of the national standard ensures a safety level that is in agreement with the application of the Eurocode standard.

**Adequacy of Verification**

The standards applied in the case studies are considered adequate as they are specific national normative documents, international standards approved or adjusted by national regulators, or superseded national standards.
standards the applicability of which in the structural re-analysis for a certain area was assessed and justified properly.

Proposals for Improvement

No improvement seems necessary to justify the applicability of the standards selected for the design process. In one case the extension of the analysis scope to buildings that are not regarded traditionally as safety buildings but are still related to safety in some way (e.g. important from risk point of view). In summary, the applicability of standards is either self-evident as they are specified in the national legislative documents, or a targeted assessment and justification is necessary to substantiate the applicability of some designated parts of the standard.

A short summary of the assessment made to compare how the fulfilment of the BESEP requirements are verified in the three case studies of case study group PVES is presented in Table E.1.
### Table E.1. Fulfilment of BESEP Safety Requirements in Case Study Group PVES

<table>
<thead>
<tr>
<th>BESEP requirement topic: Physical separation and structural integrity (DSA)</th>
<th>PVES_1</th>
<th>PVES_2</th>
<th>PVES_3</th>
<th>Conclusions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>BESEP requirement ID:</strong> BESEP_DSA_PSEP_002</td>
<td>structural calculations based on EuroCode; reconstruction of the roof; calculations updated after the reconstruction; analysis of blockage of air intake system due to snow.</td>
<td>structural strength analysis applying Eurocode; structural reinforcement of two chord members; fragility analysis for beyond design basis loads.</td>
<td>definition of scope of the buildings to be analysed; vulnerability of structures; assessment of the consequences of roof collapse on the SSCs located inside the buildings; fragility analysis.</td>
<td>structural strength analysis of buildings, traditional DSA in structural engineering; widely accepted standards or well-elaborated methods; structural reinforcements; fragility analyses.</td>
</tr>
<tr>
<td><strong>Key features of the verification process</strong></td>
<td>finite element model and use of Eurocode is state-of-practice; structural reinforcement based on widely accepted methods; fragility curves based on structural reliability analysis (state-of-the-art).</td>
<td>all main risks coming from extreme snow cover were analysed; the verification is considered adequate.</td>
<td>widely accepted standards or well-elaborated methods in structural strength analysis, fragility analysis.</td>
<td></td>
</tr>
<tr>
<td><strong>Adequacy of Verification</strong></td>
<td>structural verification adequate thanks to the use of EuroCode standard and following the SSM; analysis of blockage of air intake is qualitative.</td>
<td>finite element model and use of Eurocode is state-of-practice; structural reinforcement based on widely accepted methods; fragility curves based on structural reliability analysis (state-of-the-art).</td>
<td>all main risks coming from extreme snow cover were analysed; the verification is considered adequate.</td>
<td>widely accepted standards or well-elaborated methods in structural strength analysis, fragility analysis.</td>
</tr>
<tr>
<td><strong>Proposals for Improvement</strong></td>
<td>use fragility curves; use structural reliability analysis.</td>
<td>structural strength analysis and fragility analysis to be performed in combination and by the same expert group.</td>
<td>new supporting deterministic analyses should be performed to reduce the conservatism in the assessment (including the PSA results).</td>
<td>structural strength analysis and fragility analysis is to be performed in combination by the same group; refined calculations to reduce conservatism.</td>
</tr>
</tbody>
</table>

### BESEP requirement topic: Justification of the engineering assumptions used in analysis (DSA)

<table>
<thead>
<tr>
<th><strong>BESEP requirement ID:</strong> BESEP_DSA_JEA_001</th>
<th>assumptions used in the analysis are described and justified.</th>
<th>the use of appropriate standards implicitly ensures the justification.</th>
<th>1) detailed fragility analysis for rooftop vulnerability; 2) system / component fragility based on general vulnerability and location.</th>
<th>justification aspects not provided in detail; use of appropriate standards and methods ensures justification implicitly.</th>
</tr>
</thead>
</table>
### PVES_1
- **Adequacy of Verification:** Adequate, since all engineering assumptions are addressed and discussed.
- **Proposals for Improvement:** None.

### PVES_2
- **Adequacy of Verification:** Adequate, as the relevant standards apply justified assumptions.
- **Proposals for Improvement:** Make the justification more explicit and thorough.

### PVES_3
- **Adequacy of Verification:** Adequate, need to identify and assess vulnerability of some indoor systems and components.
- **Proposals for Improvement:** Assess vulnerability of components and systems to roof collapse.

### Conclusions
- Use accepted standards; describe all engineering assumptions; describe all aspects considered during engineering judgement.
- Proposals for Improvement: Make the justification more explicit and thorough.
- PSAs were applied to review and further improve the relevant operating procedures; risk-informed review can be considered a sufficiently detailed evaluation (including new approaches).

### BESEP Requirement Topic
- Support to developing abnormal and emergency operating procedures and severe accident management guidelines (PSA)

### BESEP Requirement ID: BESEP_PSA_EOP_001
- **Key Features of the Verification Process**
  - PSA not applied, only to identify hazards that should be considered in operating procedures.
  - Risk-informed review of the operating procedure that controls snow removal: identification and evaluation of the key influences on snow removal activities; development of proposal to ensure more reliable snow removal.
  - Important local actions related to extreme snow scenarios identified; several factors that impact the work of plant crew (incl. existence and ergonomics of procedures) addressed during quantification; recommendations regarding procedures and guidelines related to extreme snow.

- **Adequacy of Verification**
  - PSA could only be applied to review and further improve the relevant operating procedures; the risk-informed review can be considered a sufficiently detailed evaluation (including new approaches).
  - All accident sequences and human actions were considered when making recommendations on improving procedures and guidelines.

- **Proposals for Improvement**
  - Identification and evaluation of key performance shaping factors related to snow removal; evaluation of plant procedures considering the influencing factors; proposal to ensure more reliable snow removal, if necessary.
  - PSA was applied to review and further improve the relevant operating procedures; risk-informed review can be considered sufficiently detailed.
## PVES_1

- **Proposals for Improvement**: Integrate PSA when developing abnormal and emergency operating procedures and severe accident guidelines, if needed.

## PVES_2

- **Operating procedures, training as well as available equipment for snow removal should be further improved**: Utilize PSA and PSA insights as an integral part of developing operating procedures for coping with external events.

## PVES_3

- **Refine input to EOPS and SAMGs by considering the lessons learned from dedicated analyses in the HRA and PSA**.

## Conclusions

- **Utilize PSA and PSA insights as an integral part of developing operating procedures for coping with external events**: Integrate lessons learned from dedicated analysis or from similar assessments performed for similar plant types.

### BESEP requirement topic: Guidance selection, decision making and intelligent use of guidance (HFE)

### BESEP requirement ID: BESEP_HFE_GS_001

#### Key features of the verification process

- Procedure controlling snow removal; actions dependent on warnings by the meteorological institute.

- Procedure controlling snow removal; sufficient time to start snow removal activities.

- Procedure controlling snow removal; symptom-oriented emergency operating procedures used by the control room crew; plant staff should be prepared to use these procedures in due time.

#### Adequacy of Verification

- Part of the procedures used during the life-time of the plant verifying the relevance and applicability.

- Identification and selection of the relevant procedures and guides during heavy snowfall are ensured.

- Verification is considered adequate, as all aspects of the requirement were addressed.

#### Proposals for Improvement

- Theoretically, detailed evaluation of the organisations' capabilities to follow the procedures – seems unfeasible.

- None.

- None.

#### BESEP requirement ID: BESEP_HFE_GS_002

- No detailed justifications seem necessary, as the use of the relevant procedures seems self-evident (that is supported by earlier usage).
### Key features of the verification process

<table>
<thead>
<tr>
<th>PVES_1</th>
<th>PVES_2</th>
<th>PVES_3</th>
<th>Conclusions</th>
</tr>
</thead>
<tbody>
<tr>
<td>actions dependent on warnings by the meteorological institute; prioritization of snow removal activities.</td>
<td>main decision points during the whole snow removal process and the support given by procedures thereto are identified and evaluated.</td>
<td>symptom-oriented EOPs: - structure to support decision making; - training; - efforts to optimize timing of actions; - application of simulator to evaluate EOP changes and maintain EOPs.</td>
<td>evaluation of decision points, e.g.: - preparation for timely snow removal; - prioritization of snow removal activities.</td>
</tr>
<tr>
<td>feasibility of actions in line with the procedures has not been verified with respect to capabilities and availability of personnel.</td>
<td>preparatory measures for timely snow removal activities should be defined in an action plan or in the relevant operating procedures; the buildings in need of snow removal should be ranked by safety significance.</td>
<td>cover all the aspects from this BESEP requirement in the process of making changes to emergency procedures; regular review of the emergency procedures ergonomics.</td>
<td>support given by the relevant procedures to main decision points during snow removal should be evaluated and its adequacy justified.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>BESEP requirement ID: BESEP_HFE_GS_003</th>
</tr>
</thead>
</table>

<p>| Key features of the verification process | Risk-informed review of the operating procedure that controls snow removal: identify and evaluate the key influences on snow removal activities; increase in the number of persons to remove snow seem necessary; incorporate training on the use of EOPs used in the MCR | No significant difference in workload of MCR crew in case of a heavy snow; EOPs used in the MCR take into account the capabilities and limitations of the crew. | identification and evaluation of key performance shaping factors related to snow removal; evaluation of the number of the plant personnel considering the influencing factors; proposal to ensure more reliable snow removal, if necessary. |</p>
<table>
<thead>
<tr>
<th>PVES_1</th>
<th>PVES_2</th>
<th>PVES_3</th>
<th>Conclusions</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>of the relevant organizational plan.</td>
</tr>
</tbody>
</table>

**Adequacy of Verification**

- feasibility of actions in line with the procedures has not been verified with respect to capabilities and availability of personnel.
- human capabilities and limitations were evaluated and HRA was performed to identify and evaluate the key influences on snow removal activities; expert judgement played an important role in HRA.
- all related aspects taken into account – considered adequate.
- human capabilities and limitations need to be evaluated and HRA needs to be performed to identify and evaluate the key influences on snow removal activities.

**Proposals for Improvement**

- theoretically, detailed evaluation of the organisations’ capabilities to follow the procedures – seems unfeasible.
- compare the amount of snow that may be removed by an individual / team with the snow that needs to be removed from the roofs.
- to develop the procedures for local actions, human capabilities and limitations during extreme snowfall should be addressed, considering multi-unit aspects.
- consider multi-unit aspects; hardly feasible to perform detailed evaluations; compare the amount of snow that may be removed by an individual / team with the snow that needs to be removed from the roofs.

**BESEP requirement topic:** Safety design and requirement management for external hazards (SE)

**BESEP requirement ID:** BESEP_SEP_SDRM_003

**Key features of the verification process**

- use of methods for specification of event data for DSA and PSA based on site-specific data, if available; method includes appropriate screening criterion.
- hazard assessment based on:
  - maximum thickness of snow;
  - collected at a nearby meteorological station in the past few decades;
  - Gumbel distribution;
  - design basis: 10^{-4}/a freq.
- design basis load is based on common practice, state-of-the-art:
  - establishing hazard curves;
  - typical screening criteria for external hazards;
  - no detailed analysis to ensure plant specificity of the design basis values.
- few decades of site-specific data; extreme value theorem; application of hazard curves; application of screening criteria relevant to design basis load.

**Adequacy of Verification**

- identification of external events considering generic and site-specific events; extreme value theory considering site specific data;
- design basis definition solely on site-specific analysis, considering applicable hazard curves and prescribed screening values;
- adequately verified based on the current status of engineering support of plant operation.
- state-of-the-art methods and plant specific data are widely used; the verification is regarded as adequate.
## PVES_1

<table>
<thead>
<tr>
<th>SEP for design considers protection of SSCs for extreme hazards.</th>
</tr>
</thead>
</table>

## PVES_2

<table>
<thead>
<tr>
<th>some further research and development is seen advisable in order to verify the applicability of the assessed hazard curve and the design basis.</th>
</tr>
</thead>
</table>

## PVES_3

<table>
<thead>
<tr>
<th>more site-specific information could be used when setting the design basis; however, it is not seen necessary.</th>
</tr>
</thead>
</table>

## Conclusions

<table>
<thead>
<tr>
<th>for verification purposes: - data for longer periods or historical data from other stations; - use of further methods; - comparison of hazard curves for different NPP site.</th>
</tr>
</thead>
</table>

### Proposals for Improvement

| none. |
| regional data and further methods should also be used. |
| more site-specific information could be used when setting the design basis; however, it is not seen necessary. |

### BESEP requirement ID: BESEP_SEP_SDRM_007

#### Key features of the verification process

<table>
<thead>
<tr>
<th>no fragility curves; in line with the international practice and national regulations, snow load corresponding to $10^{-5}$/a frequency was considered in the design basis.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>snow fragility curves established; application of advanced analysis methods; risk from snow beyond the design basis (range: $10^{-7}$-$10^{-4}$/a freq.).</th>
</tr>
</thead>
</table>

| snow fragility curves established; PSA results and deterministic vulnerability analysis of roofs pointed out that snow is important from safety point of view. |

#### Adequacy of Verification

<table>
<thead>
<tr>
<th>considering the return value of $10^{-5}$/a exceedance frequency seems adequate; re-construction of the roof of the EDG-building.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>adequate, as the risk due to beyond design basis loads was quantified utilizing hazard and fragility curves.</th>
</tr>
</thead>
</table>

| is seen adequate. |

#### Proposals for Improvement

<table>
<thead>
<tr>
<th>establish fragility curves for a more realistic analysis.</th>
</tr>
</thead>
</table>

| none. |

| none. |

| risk due to beyond design basis loads needs to be quantified utilizing hazard and fragility curves; risk due to different snow loads. |

### BESEP requirement ID: BESEP_SEP_SDRM_010
## Key features of the verification process

<table>
<thead>
<tr>
<th>PVES_1</th>
<th>PVES_2</th>
<th>PVES_3</th>
<th>Conclusions</th>
</tr>
</thead>
<tbody>
<tr>
<td>use of guidance issued by the Swedish Authority (SSM) that is based on widely used international standards (e.g. Eurocode).</td>
<td>use of Eurocode or a superseded national standard series; comparison of the different standards from theoretical point of view to substantiate the use of either standard.</td>
<td>use of a specific Czech normative document ČSN EN 1991-1-3 to specify the critical load for rooftops of plant buildings.</td>
<td>use of national legislative documents, or widely applied and accepted international or national standards.</td>
</tr>
<tr>
<td>Adequacy of Verification</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>use of international standards adjusted by the Swedish Authority ensures adequacy.</td>
<td>the applicability of the standards in the structural re-analysis was assessed and justified properly – ensures adequacy.</td>
<td>use of national normative document ensures adequacy.</td>
<td>self-evident in most of the cases or needs to be justified if an irregular standard needs to be used.</td>
</tr>
<tr>
<td>Proposals for Improvement</td>
<td>none.</td>
<td>none.</td>
<td>extend the scope of safety buildings by considering new aspects (e.g. risk-important buildings).</td>
</tr>
</tbody>
</table>
E.3 Safety Margins Assessment

Safety margins addressed in the case studies belonging to the PVES case study group were compared from the point of view of the three main types of safety analysis, i.e.:

- deterministic safety analysis;
- probabilistic safety analysis;
- human factors engineering.

A short summary of the comparison of these analyses is presented in Table E.2. The different analyses are discussed one by one following the table.
### Table E.2. Assessment of Safety Margins in Case Study Group PVES

<table>
<thead>
<tr>
<th>Deterministic Safety Margins</th>
<th>PVES_1</th>
<th>PVES_2</th>
<th>PVES_3</th>
<th>Conclusions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Definition</td>
<td>design basis load / design value of capacity; DEC systems designed against higher load than plant design basis.</td>
<td>design basis load / design value of capacity; applied safety factors according to the standard.</td>
<td>design value of capacity – design basis load.</td>
<td>comparison of design basis load and design value of capacity.</td>
</tr>
<tr>
<td>Assessment &amp; Evaluation</td>
<td>EDG building: load/capacity ratio well below 1 for most structural elements; ICCS is capable of withstanding higher snow load than the EDG building.</td>
<td>strengthening some elements based on the initial results; safety margin ensured by fulfilling the Eurocode; actions/capacity ~1; SSCs located in the reactor hall conservatively assumed as failed.</td>
<td>capacity value transformed to equivalent water column; comparison shows sufficient safety margin.</td>
<td>comparison of the design value of the actions and the design value of the capacity; a sufficiently high level of reliability is ensured by the use of partial factors applying relevant standards.</td>
</tr>
<tr>
<td>Comparison with D2.3</td>
<td>physical phenomena and plant parameters in Ch. 4.2 of D2.3 not applicable; SM: difference between “value computed by conservative calculation” and the “safety limit”; further margin between DBA and BDBA requirements; in agreement with Ch. 4.1 of D2.3.</td>
<td>physical phenomena and plant parameters in Ch. 4.2 of D2.3 not applicable; “safety limit” = “regulatory acceptance criterion” = “value computed by conservative calculation” (no margin); margin: difference between the “value computed by conservative calculation” and the upper bound of the uncertainty interval of the best estimate calculation in agreement with Ch. 4.1 of D2.3.</td>
<td>no information.</td>
<td>physical phenomena and plant parameters in Ch. 4.2 of D2.3 not applicable; “safety limit” = “regulatory acceptance criterion” = design basis; “value computed by conservative calculation” = design value of capacity; difference between the “value computed by conservative calculation” and the upper bound of the uncertainty interval of the best estimate calculation; in agreement with Ch. 4.1 of D2.3; further margin between DBA and BDBA requirements.</td>
</tr>
<tr>
<td>Proposals for Improvement</td>
<td>PVES_1</td>
<td>PVES_2</td>
<td>PVES_3</td>
<td>Conclusions</td>
</tr>
<tr>
<td>---------------------------</td>
<td>------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>clear description is needed on how the different factors of the Eurocode contributes to the safety margin.</td>
<td>partial factors of the Eurocode ensure a sufficiently high level of reliability; use of structural reliability analysis.</td>
<td>none.</td>
<td>more explicit quantification of the safety margins ensured by the different partial factors of the standard; use of structural reliability analysis.</td>
<td></td>
</tr>
</tbody>
</table>

**Probabilistic Safety Margins**

<table>
<thead>
<tr>
<th>Definition</th>
<th>compare calculated CDF and PSA target (defined by the Licensee, not the regulator).</th>
<th>compare calculated risk to criteria; conditional success probability at the design basis snow load level; difference between the median capacity and the design basis snow load.</th>
<th>risk contribution of snow to the overall risk; compare calculated risk to criteria.</th>
<th>compare calculated risk (due to all hazard; snow; given snow-induced failure) to criteria or target; information derived from the fragility curves.</th>
</tr>
</thead>
</table>

| Assessment & Evaluation | snow PSA; contribution of snow risk to the overall risk: 1%. | snow PSA; contribution of snow risk to the overall risk: 1%; risk contribution of the failure of the reactor hall due to snow to snow risk: 5%; conditional success probability at the design basis snow load level: more than 99.9%; difference between the median capacity and the design basis snow load: 3 kPa. | snow PSA; ratio of risk to safety criterion: 0.1; contribution of snow risk to the overall risk from external hazards: 26%. | snow PSA; interpretation of results and comparison of risk attributable to snow or different snow induced failures to the overall risk and safety criterion or target; further margins based on the fragility curves. |

| Comparison with D2.3 | in full agreement. | in agreement, with the exception of: - mean value vs. upper bound of uncertainty range; - no LERF, only CDF; - use of fragility curves (not discussed in D2.3). | in agreement. | in agreement, e.g.: - compare calculated risk to criterion; - MCSs and important measures; differences: - mean value vs. upper bound of uncertainty range; - LERF not used; - use of fragility curves (not discussed in D2.3); - not each aspect seemed applicable. |
### Proposals for Improvement

- **PVES_1**: none.
- **PVES_2**: For SSCs based on fragility curves and for risk based on CCDP by hazard load:
  - conditional success probability at the design basis snow load level;
  - difference between the median capacity and the design basis snow load.
- **PVES_3**: none.

### Conclusions

- For SSCs based on fragility curves and for risk based on CCDP by hazard load:
  - conditional success probability at the design basis snow load level;
  - difference between the median capacity and the design basis snow load.

### Safety Margins for Human Actions

#### Definition

- **PVES_1**: not addressed.
- **PVES_2**: conditional success probability of snow removal at the design basis snow load level;
  - difference between the snow load that may be removed with 50% probability and the design basis snow load.
- **PVES_3**: use of fractional contribution and risk increase factor for human actions.

#### Assessment & Evaluation

- **PVES_1**: not addressed.
- **PVES_2**: the likelihood of timely snow removal from the roofs of safety related buildings was assessed;
  - conditional success probability of snow removal at the design basis snow load level: 95%;
  - the difference between the snow load that may be removed with 50% probability and the design basis snow load: 2 kPa.
- **PVES_3**: identification and evaluation of human actions with high importance measures.

#### Comparison with D2.3

- **PVES_1**: not addressed.
- **PVES_2**: analysis steps addressed in the report are also performed;
  - additional efforts, see the definition cell.
- **PVES_3**: similar, supporting the use of FC and RIF.

- **PVES_2**: conditional success probability of snow removal at the design basis snow load level;
  - difference between the snow load that may be removed with 50% probability and the design basis snow load.
<table>
<thead>
<tr>
<th>Proposals for Improvement</th>
<th>PVES_1</th>
<th>PVES_2</th>
<th>PVES_3</th>
<th>Conclusions</th>
</tr>
</thead>
<tbody>
<tr>
<td>not addressed.</td>
<td>use PSA to address safety margins for human actions.</td>
<td>none beyond the one described in the case study.</td>
<td>no further proposal beyond the one described in the case study.</td>
<td></td>
</tr>
</tbody>
</table>
E.3.1 Deterministic Safety Margins

E.3.1.1 Definition

The deterministic safety margin related to structural analysis, that is in the focus of the deterministic analyses in this case study group, is defined similarly and in mutual agreement in the different case studies. Although, the deterministic structural analyses were performed in a very similar manner, there are some slight differences in the interpretation of the deterministic safety margins derived from the structural analyses. This may be due to small differences in national practices. An overview is given hereby on the possible definitions of the deterministic safety margins based on the case studies belonging to the PVES group.

According to the approach generally used in civil engineering, a structure is regarded as sufficiently protected, if the vector sum of the impacting actions, modified with the relevant safety factors as well as with the combination (simultaneity) factors, is lower than the modified structure capacity considering the relevant partial or safety factor. Otherwise, the building does not meet the applicable requirements; hence, strengthening the relevant structural element(s) is needed. The applied partial or safety factors as well as the ratio (if it is below 1) of the design value of the actions and the design value of the capacity ensure the existence of a deterministic safety margin. Also, the approach is applicable to characterizing the degree of the safety margin.

In particular, if the design basis snow load is considered in the analysis, the safety margin may be interpreted as the ratio of the load combination (including the design basis snow load) and the capacity of the building, additionally to the applied safety factors. Another approach can be to assess the maximum snow load when the load combination is equal to the capacity (considering the safety factors too) of the building; hence, the safety margin is the difference or ratio of the maximum allowed snow load and the design basis snow load, additionally to the applied safety factors. Similarly, if some systems are originally designed against loads higher than the general plant design basis to mitigate core damage in certain beyond design basis scenarios, the intendedly higher load capacity ensures further safety margins. This issue is described in more details for the independent core cooling system (ICCS) of the Ringhals NPP, where the rationale for assigning different design values to the system in question was the corresponding defence-in-depth level and the relevant national regulatory requirement.

E.3.1.2 Assessment and Evaluation

A widely accepted standard system (e.g. Eurocode) was applied during the structural re-analysis of the different safety buildings and systems in the case studies. In buildings and systems designed by applying such standards, a sufficiently high level of reliability is ensured by the use of partial factors. In this framework, it shall be justified that the design values of actions (loads) and the effects thereof, the material properties and the geometrical data are in the established limit states in any of the possible design situations. Based on the Eurocode standard, for example, the fundamental assumption in the limit state method is that all the actions and structural resistances have a statistically interpreted distribution (density function), i.e. in a certain design situation, different frequency values are applicable to certain values. It shall be justified in the assessment that the design value for the effect of actions does not exceed the design value of structural resistance (capacity). This may be interpreted as the ratio of the design value of the actions and the design value of the capacity. If this ratio is below 1, then the building meets the requirements; if it exceeds 1, then it does not. It is noted that the assessment and evaluation of deterministic safety margins can be considered very similar and applicable to quantifying deterministic safety margins in the different case studies. The different assessments and evaluations are briefly discussed below.

The steel superstructure of the reactor hall is in the focus of one of the case studies. The results of the detailed structural re-analysis demonstrated that each structural element meets the requirements of the Eurocode, except for two top chord members. The ratios of the design value of the actions and the design value of the capacity are 1.070 and 1.096 for these members. Consequently, these two top chord members were strengthened to ensure appropriate protection against the design basis loads. As a result of structural strength analysis, it could be concluded that the reactor hall steel superstructure can withstand the design basis loads, and safety margin beyond the design basis loads exist, as ensured by fulfilling the Eurocode requirements. The deterministic safety margin can be regarded as high on the basis of the partial factors as well as the
simultaneity factors defined by the Eurocode standard. Although this generalized approach helps develop a coarse understanding of the degree of the deterministic safety margins, the margins ensured by the safety factors of the standard cannot be quantified and interpreted in a precise and traceable manner. Further deterministic safety margins cannot be witnessed, since the ratio of the design value of the actions and the design value of the capacity is nearly 1. However, it should be noted that all the SSCs located in the reactor hall are conservatively assumed as failed, if the ultimate state of the steel structure is on the “damage side” of the limit surface. This conservative assumption may also ensure some further significant margin that was not quantified.

According to the structural re-analysis of the emergency diesel generator building in another case study, a safety margin beyond the design basis snow load is also ensured, as the ratio between the design basis load and the design value of capacity is well below 1 for most of the structural elements of the roof. These results were obtained considering the strengthening of the roof based on the Eurocode standard. In the same case study, it was also verified that the ICCS is capable of withstanding higher snow load than the EDG building ensuring a further safety margin against core damage due to BDBA external events.

In the third case study, the capacity (so called fragility) resulted from the structural analysis of each safety related building was transformed to equivalent water column to enable comparison with recorded values of extreme snow cover. The transformed capacity values of the buildings are 198.8, 199.8, 203.9, 217.1, 234.5 and 301.7 mm (equivalent water column). Since the highest value of extreme snow cover recorded during the last 50 years (i.e. within the time period snow cover values have been recorded) is below 100 mm of equivalent water column, the safety margin can be considered sufficient.

### E.3.1.3 Comparison of the Safety Margin Interpretation with Chapter 4 of Deliverable 2.3

The deterministic analyses in the case studies focus on the protection of safety related buildings and systems from structural integrity point of view, as this aspect is generally the most relevant concern when the protection against snow load is to be verified. Chapter 4.2 of Deliverable 2.3 deals mostly with physical phenomena and plant parameters to be assessed primarily by thermal-hydraulic and reactor physics calculations (see the listing at the end of the Chapter). These phenomena and parameters are not in the forefront of the case studies.

However, the general scheme in Chapter 4.2 (i.e. Figure 16) can be interpreted in relation to the case studies belonging to the PVES case study group as follows. The “safety limit” equals the “regulatory acceptance criterion” in the case studies as the design basis snow load corresponding to a selected hazard frequency (prescribed by the regulator) was considered in the deterministic structural evaluation. The “value computed by conservative calculation” corresponds to the design value of the capacity. In one of the case studies, this is also the same as the regulatory acceptance criterion, since the ratio of the design value of the actions and the design value of the capacity is nearly 1 in that case. For the other two case studies, a safety margin can be observed between the regulatory acceptance criterion and the value computed by conservative calculations. An additional safety margin exists in all the case studies as the difference between the “value computed by conservative calculation” and the upper bound of the uncertainty interval of the best estimate calculation; however, this margin cannot be quantified directly.
The interpretation of the relevant safety margins as well as their assessments in the case studies is, however, in good agreement with the description in Chapter 4.1 of Deliverable 2.3. The load and strength density functions as well as their relative position are the basis of the applicable structural analysis standards.

E.3.1.4 Proposals for Improvement

In the state-of-practice, the design as well as the strength analysis of a structure is based on the use of widely accepted standards (primarily Eurocode). In buildings designed on the basis of such standards, a sufficiently high level of reliability is ensured by the use of partial factors, which yields adequate safety margin too. In the state-of-practice, safety margins are not quantified more precisely than assessing the ratio of the design value of the actions and the design value of the capacity. A more explicit quantification of the safety margins ensured by the different partial factors of the standard could be beneficial. Alternatively, the safety margin in the structural design can be adequately interpreted and quantified by the use of structural reliability analysis, i.e. by quantifying the failure frequency of a certain structure due to snow load (see also Chapter E.3.2 for more details).

E.3.2 Probabilistic Safety Margins

E.3.2.1 Definition

All three case studies in the PVES case study group define probabilistic safety margins primarily according to the traditional interpretation, i.e. the calculated mean risk values are compared to pre-defined probabilistic safety criteria or targets. The core or fuel damage frequency was in the focus of each case study. By comparing the quantitative risk target for core damage with the risk attributable to all hazards, only to snow, or directly to the snow-induced failure of the safety related building addressed in the case study can characterize the adequacy of the safety margin. According to one of the case studies, the fragility curves of a given safety related building can help develop a good understanding of the safety margins beyond the design basis snow load, as it enables a quantitative evaluation of the safety margin. This margin can be defined as the conditional failure or, more precisely, the conditional success probability at the design basis snow load level or as the difference between the median capacity and the design basis snow load. This approach was elaborated during
the targeted safety assessment (so-called stress-test), when the regulatory body required sound assessment techniques to quantify safety margins.

E.3.2.2 Assessment and Evaluation

In compliance with the relevant national regulatory requirements, external events PSA of a given NPP was performed in each case study. The snow PSAs followed the commonly known steps: probabilistic hazard assessment, plant response analysis, PSA model development, and risk quantification and interpretation of results. It is demonstrated, amongst others, in each case study that the probabilistic risk criteria are met considering all screened-in external hazards and further initiating events. Consequently, the assessment and evaluation of probabilistic safety margins can be considered very similar and applicable to quantifying probabilistic safety margins in the different case studies. The different assessments and evaluations are briefly discussed below.

According to the results presented in one of the case studies, the probabilistic safety margin relevant to the whole spectrum of external hazards equals approximately one order of magnitude corresponding to fuel damage frequency, and the contribution of extreme snow to the overall risk from external hazards is significant (26%). Another case study concluded that the CDF attributable to extreme snow contributes to the overall CDF for power operation by less than 1%. It is also highlighted in this case study that the absolute value of CDF attributable to snow is not among the most valuable lessons learned from the study, but the change in the relative contribution of snow risk to the overall plant risk due to the reinforcement of the roof of the EDG building and the implementation of the ICCS system. The plant modification resulted in a change from 17% to 1%. The results of the third case study show that the risk from extreme snow is moderate in comparison to the risk originated from other types of initiating events analysed in the PSA (~1%). Moreover, it can also be concluded that the risk due to snow is not significant in comparison to the quantitative safety criteria for core damage frequency. The failure of the reactor hall induced by snow does not play a significant role in the plant risk from snow, the risk contribution thereof is around 5% only.

Furthermore, in one of the case studies the fragility curves of the reactor hall played also a role in assessing and evaluating the probabilistic safety margin. Fragility curves were established using a unique methodology developed on the basis of structural reliability analysis. Based on the fragility curves of the reactor hall superstructure, the safety margins beyond the design basis snow load were determined and found sufficient. These margins were calculated on one hand as the conditional success probability at the design basis snow load level: more than 99.9%, and as the difference between the median capacity and the design basis snow load on the other hand: 3 kPa.

E.3.2.3 Comparison of the Safety Margin Interpretation with Chapter 4 of Deliverable 2.3

The interpretation of probabilistic safety margins given in the case study descriptions is in good agreement with the approach discussed in Chapter 4.3 of Deliverable 2.3. In general, the regulatory probabilistic safety criteria were compared to the calculated mean risk values, which is similar to the approach described in Deliverable 2.3. The only difference is that in Deliverable 2.3, the upper bound of the uncertainty range is applied instead of the mean value. The difference between the mean value and the upper bound of the uncertainty range is often significant. Therefore, this deviation in the definition of relevant measures can be regarded as substantial. It is noted that in the majority of national requirements and international recommendations, probabilistic risk criteria or targets are typically defined considering the mean values with additional requirements to assess the effects of uncertainties in the fulfilment of the safety goals. Therefore, a revision of the approach described in Deliverable 2.3 can be useful from this aspect. The development and publication of a refined definition of probabilistic safety margin is seen necessary in the next project phases.

Besides, the basis of the evaluation was the CDF or FDF value in the case studies. However, Deliverable 2.3 addresses the evaluation of risk metrics for LERF too. Similarly to the approach described in Deliverable 2.3, the relevant minimal cut sets as well as the importance measures related to the snow-induced failures were assessed and evaluated. On one hand, it is to be noted that several aspects addressed in Deliverable 2.3 do not seem directly applicable to this case study group. On the other hand, use was made of the fragility curves...
in determining safety margins in one of the case studies, although such an approach is not addressed in Deliverable 2.3.

E.3.2.4 Proposals for Improvement

In general, the regulatory probabilistic safety criteria or targets are compared to the calculated mean risk values. The latter ones can be interpreted as the risk attributable to all hazards, only to snow, or directly to the snow-induced failure of the safety related building addressed in the case study. The relevant minimal cut sets as well as the importance measures related to the snow-induced failures are assessed and evaluated. It is also emphasized that the fragility curves may be utilized in support of determining the probabilistic safety margins. These margins can be defined as the conditional failure or, more precisely, the conditional success probability at the design basis load level or as the difference between the median capacity and the design basis load. Moreover, the PSA results can be further utilized for describing safety margins by depicting the conditional core damage probability as a function of hazard load and deriving similar characteristics as mentioned above for fragility curves (i.e. conditional success probability at the design basis load level or the difference between the median capacity and the design basis load).

E.3.3 Safety Margins for Human Actions

E.3.3.1 Definition

There are no explicitly defined quantitative safety margins in place for human actions in the national practices of the countries the case studies are relevant to. Hence, the partners made an attempt to define safety margins for human actions in their case studies themselves, which led to quite different approaches.

No safety margins are addressed in the HFE area in one of the case studies and the authors do not consider it possible addressing them either. This case study used the concept of HFE when trying to define safety margins, HRA was considered as a part of the PSA safety margin. Therefore, this case study was not included in the comparative analysis from this aspect. As described in another case study, importance measures, including fractional contributions and risk increase factors of human actions, can be used for the safety margin related discussions and analyses. The implications of these measures for safety margins are addressed in the case study; however, a precise definition and an applicable, well-founded analysis method have not been developed yet, at least not in such level of detail as it is described in Chapters 0 and 0 for deterministic and probabilistic safety margins.

The third case study focuses on the snow removal activities. In this case study, the mean failure probability curve to remove snow as a function of snow load was used to visualise the safety margins beyond the design basis snow load. Also, this characterisation enables a quantitative evaluation of the safety margin too. This margin can be defined as the conditional failure probability or, more precisely, the conditional success probability of snow removal at the design basis snow load level or as the difference between the snow load that may be removed with 50% probability and the design basis snow load.

E.3.3.2 Assessment and Evaluation

According to one of the case studies, the general basis for analysing the impact of human factors on the safety margin is the evaluation of important measures related to human actions in the PSA results. The actions with high importance measures are possible candidates that may significantly challenge the plant safety margin corresponding to human failures. In such cases, the relevant conditions are carefully reviewed. A sufficient balance of error impact potential for the actions performed from the control room and in addressing their results in the risk engineering processes at the plants under concern was achieved as a result of many years of development of PSA studies for internal events and external hazards. The failure probabilities of preventive local actions are typically much higher, since they represent unfamiliar conditions not completely covered by training (it is not seen realistically feasible to cover all aspects of external event scenarios in the training of the plant crew).
The occurrence of snow-induced transients can be prevented, if snow is removed from some affected plant areas, important to plant safety, in a timely manner. In the other case study, the likelihood of timely snow removal from the roofs of safety related buildings was assessed including:

- identification of the most important performance shaping factors relevant to the success of snow removal;
- review of the snow removal strategy at the NPP;
- evaluation of the plant procedure and associated arrangements in place for snow removal with considerations to the influencing factors identified in the first step;
- quantification of failure to remove snow from the roofs based on an evaluation of the applicable plant procedure and other relevant influences on performance.

Based on the mean failure probability curve for snow removal as a function of snow load, the safety margins beyond the design basis snow load were determined and found sufficient. These margins were calculated on one hand as the conditional success probability of timely snow removal at the design basis snow load level: 95%, and as the difference between the snow load that may be removed with 50% probability and the design basis snow load on the other hand: 2 kPa.

Different HFE/HRA aspects were considered in the two case studies analysed. It can be concluded that the two different approaches may supplement rather than contradict each other.

E.3.3.3 Comparison of the Safety Margin Interpretation with Chapter 4 of Deliverable 2.3

Although there is no specific approach presented in Deliverable 2.3 to interpret safety margins for human actions, the analysis steps addressed in the report are also performed within these case studies. Human actions were identified, and then analysed qualitatively and quantitatively, and human failure events and their probabilities were built into the PSA. The qualitative and quantitative assessment was based on the identification of key influencing factors and the evaluation of the human actions (including snow removal) considering thereof. Moreover, one case study strongly supports the proposal also discussed in Deliverable 2.3 that importance measures, including fractional contributions and risk increase factors of human actions, can be used for the safety margin related discussions and analyses; however, a precise definition and an applicable, well-founded analysis method have not been developed yet, at least not in such level of detail as it is described in Chapters 0 and 0 for deterministic and probabilistic safety margins. In addition, efforts were made in one of the case studies to quantify the safety margin for human actions by assessing the conditional success probability of snow removal at the design basis snow load level, and the difference between the snow load that may be removed with 50% probability and the design basis snow load.

Concerning safety margins for human actions, both in the case studies within the PVES group and in Deliverable 2.3, the focus is on the reliability of human actions rather than HFE in its entirety. This is in agreement with the following statement from Deliverable 2.3, referring to the possibility to define safety margins in connection to HRA: “In the relation to safety margins in HFE the one identified method is treatment of important human actions, which HRA is a part of.”.

E.3.3.4 Proposals for Improvement

Beyond the attempts made in the case studies to quantify safety margins for human actions as presented above, no proposal for further improvement was identified in this area. One conclusion was that importance measures, including fractional contributions and risk increase factors of human actions, should be used for the safety margin related discussions and analyses. However, a precise definition and an applicable, well-founded analysis method have not been developed yet, at least not in such level of detail as it is described in Chapters 0 and 0 for deterministic and probabilistic safety margins. Moreover, it was found that the mean failure probability curve to remove snow as a function of snow load can be used to visualise the safety margins beyond the design basis snow load. Also, this characterisation enables a quantitative evaluation of the safety margin too. This margin can be defined as the conditional failure probability or, more precisely, the conditional success probability of snow removal at the design basis snow load level or as the difference between the snow load that may be removed with 50% probability and the design basis snow load.
It should also be noted that the human actions (or HRA) are strongly connected to the PSA study and the concept of safety margins within the PSA as described above.

E.4 Interactions between DSA, PSA and HFE

A comparison of the interconnections and flow of information between the safety analyses (DSA, PSA and HFE) in the case studies belonging to the PVES group has been performed. The findings are described in this chapter. Also, a short summary of the comparison is given in Table E.3..

E.4.1 Interactions between DSA, PSA and HFE

In one of the case studies, hazard assessment was regarded as a purely probabilistic assessment; whilst in another one primarily as a deterministic analysis. In the third case study, a probabilistic hazard assessment was performed first that was subsequently complemented by a deterministic hazard assessment. Regardless of whether the analysis was considered deterministic or probabilistic, the results of hazard assessment were taken into account when determining the design basis of the safety related SSCs and the specified design basis was key input to structural analyses, to PSA and to the characterisation of initiating events. According to the case studies, PSA insights were not utilized in the DSA except for one case where the interpretation and evaluation of PSA results included deterministically oriented views and conclusions as well.

Structural strength analysis (DSA) provided input to plant response and fragility analysis preformed in the framework of PSA in all the case studies. The assessment of the overall plant safety was in the focus of one of the case studies, rather than the protection of a particular structure from snow load. Hence, all safety buildings were selected from a deterministic point of view and the result of this selection were utilized in the plant response analysis in PSA. The consequences assessment of a roof collapse (i.e. determining the failure of the SSCs located within the building in question) can be regarded as a deterministic analysis that provides important input to the plant response and fragility analysis in PSA.

In two case studies, use was made of the results of the structural strength calculations when elaborating the operating procedures (HFE) controlling snow removal. One of the case studies witnesses that the DSA helped determine criteria for starting snow removal from the roofs, develop a high quality snow load map and introduce it into the operating procedures. In the third case study, the weaknesses of the EDG building were identified first. The updated structural analysis with considerations to strengthened the EDG building concluded that the reconstructed roof can withstand the loads from extreme snow; hence, manual actions identified earlier are no longer necessary. In the case studies in this group, no HFE results were utilized by DSA. Moreover, it appears that there was no interaction between DSA and HFE at all in the third case study.

The output from HFE was utilized in PSA in each case study. Primarily, the plant response and fragility analysis considered the snow removal strategy elaborated earlier by HFE experts to estimate the failure probability of snow removal. In one of the case studies, it is also described that modelling of control room crew activities as well as the interpretation and evaluation of results considered information processed by HFE activities. Use of PSA insights in HFE was addressed in two of the case studies. In one of them, the operating procedure controlling snow removal was subject to a risk-informed review that included the development of proposals for ensuring reliable snow removal based on an evaluation of the underlying influences on performance and success rate. This review supported the improvement of the snow removal strategy. The other case study also implies that PSA results are relevant to the evaluation of control room crew activities too, and to draw conclusions that can be usefully applied when increasing plant safety. In conclusion, the HRA and HFE activities mutually supported each other in these case studies.

No interaction was described in the case studies concerning analysis of DBA and DEC external hazards, respectively. It is noted however that PSA does not differentiate between DBA and DEC hazard loads, both types of loads are considered in the assessment. The design basis load is in the focus of structural strength analysis; thus it can be interpreted as the analysis of DBA hazard loads, and PSA assesses primarily the residual risk from beyond design basis loads. From this aspect, the interconnection of design basis loads and loads corresponding to design extension conditions is similar to the interaction described for DSA and PSA.
E.4.2 Evaluation of Adequacy

If we consider DSA as structural strength analysis in this case study group, the initial DSA needs no input from PSA or HFE other than the specification of the design basis loads. However, PSA and HFE should utilize the results of DSA as input. Consequently, it is seen appropriate to perform structural strength analysis and other types of DSA (e.g. selection of safety related SSCs, evaluation of the consequences of a roof collapse) in the first place, presumably without a need to use support from the other two disciplines. If some issues significant to risk emerge, then a more detailed deterministic assessment may be necessary. These aspects are depicted in the figure of the SEP process in one of the case studies. The results of DSA were used in HFE and PSA in all the case studies to the extent it seemed practicable and feasible. These interactions can also be regarded as appropriate in the case studies; however, they could have been more intense and frequent. The operating procedures that control snow removal had been elaborated earlier than the snow PSAs were completed. The available information from HFE was considered in the PSAs. In addition, use was made of PSA in two case studies to review and further improve HFE (primarily the relevant operating procedures), as the snow removal strategy had originally been developed without explicitly giving considerations to risk aspects.

E.4.3 Proposals for Improvement

It is seen advantageous and advisable to utilize PSA and PSA insights as an integral part of developing operating procedures for coping with external events, rather than making use of risk insights in a follow-on manner, i.e. mostly for the purposes of reviews. Such uses of risk assessment and risk insights can help establish the basis of the operational and mitigation strategy, including the identification of the most important cornerstones, instead of making only adjustments to the available strategy laid down previously by using deterministic considerations only. In summary, PSA and HFE should be performed simultaneously, interacting actively so that PSA insights can be used effectively to underpin HFE. Moreover, more dynamic and frequent interactions between the different types of safety analyses can be beneficial for improving the efficiency of the SEP. For a discussion on good practices of interconnections and flow of information between DSA, PSA and HFE, see also Chapter E.6.
<table>
<thead>
<tr>
<th>Proposals for Improvement</th>
<th>Evaluation of Adequacy</th>
<th>Interactions between DSA, PSA and HFE</th>
<th>Conclusions</th>
</tr>
</thead>
<tbody>
<tr>
<td>more dynamic, continuous interactions may be beneficial among the safety analyses; development of fragility curves would be beneficial.</td>
<td>PSA based on engineering judgement first, subsequently on structural strength calculations (DSA); HFE based on engineering judgement, giving conservative input to PSA.</td>
<td>structural strength analysis (DSA) input to elaboration of snow removal strategy (HFE); structural strength analysis (DSA) input to plant response and fragility analysis (PSA); procedures for snow removal activities (DSA) input to failure probability of snow removal (PSA).</td>
<td>structural strength analysis (DSA) input to elaboration of snow removal strategy (HFE); structural strength analysis (DSA) input to plant response and fragility analysis (PSA); hazard assessment (PSA) input to structural strength analysis (DSA); procedures for snow removal activities (DSA) input to failure probability of snow removal (PSA).</td>
</tr>
<tr>
<td>more dynamic, frequent interactions is needed between the safety analyses; PSA and HFE should be performed simultaneously and in active interaction.</td>
<td>almost no interaction between DSA and HFE; use of DSA input in PSA and HFE; input from HFE considered in PSA.</td>
<td>no PSA or HFE input to DSA except for design basis loads; use of DSA input in PSA and HFE; risk informed review of operating procedures.</td>
<td></td>
</tr>
</tbody>
</table>

### Table E.3. Interactions between DSA, PSA and HFE in Case Study Group PVES

<table>
<thead>
<tr>
<th>PVES_1</th>
<th>PVES_2</th>
<th>PVES_3</th>
<th>Conclusions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interactions between DSA, PSA and HFE</td>
<td>structural strength analysis (DSA) input to elaboration of snow removal strategy (HFE); structural strength analysis (DSA) input to plant response and fragility analysis (PSA); procedures for snow removal activities (DSA) input to failure probability of snow removal (PSA).</td>
<td>structural strength analysis (DSA) input to elaboration of snow removal strategy (HFE); structural strength analysis (DSA) input to plant response and fragility analysis (PSA); procedures for snow removal activities (DSA) input to assessing failure probability of snow removal; PSA insights used in reviewing and updating operating procedures (HFE).</td>
<td>DSA (safety building selection, evaluation of fragilities, evaluation of consequences of roof collapses) input to PSA (definition and characterization of initiating event, plant response analysis, quantification of the PSA model); PSA results indirectly include deterministically driven assumptions and conclusions; snow removal activities (HFE) input to initiating event definition and characterization (PSA); control room crew and local actions (HFE) input to plant response analysis (PSA); quantification (PSA) may use inputs from HFE related parts; risk results (PSA) input to HFE (comparison of importance of control room crew and local actions).</td>
</tr>
<tr>
<td>Evaluation of Adequacy</td>
<td>PSA based on engineering judgement first, subsequently on structural strength calculations (DSA); HFE based on engineering judgement, giving conservative input to PSA.</td>
<td>no PSA or HFE input to DSA; use of DSA input in PSA and HFE; input from HFE considered in PSA.</td>
<td>almost no interaction between DSA and HFE; use of DSA input in PSA and HFE; strong connection between PSA and DSA.</td>
</tr>
<tr>
<td>Proposals for Improvement</td>
<td>utilize PSA and PSA insights as an integral part of developing operating procedures for coping with external events.</td>
<td>the interactions between PSA and DSA are intensive, no improvement is proposed from this respect; the interactions of DSA and PSA with HFE, in general, should be more intensive and systematic.</td>
<td>more dynamic, frequent interactions is needed between the safety analyses; PSA and HFE should be performed simultaneously and in active interaction.</td>
</tr>
</tbody>
</table>
E.5 Overall Safety Engineering Process

Only one of the case studies provides a V-model representation of the SEP. However, all the case studies, including the one that discusses the V-model, focus the description and evaluation on the interactions between and within the main tasks and steps of the major types of analyses and disciplines (i.e. DSA, PSA and HFE). This belongs to the 2nd and 3rd level of the SEP that is analysed and evaluated in detail in Chapter E.4 of this document. Level 1 of the SEP, i.e. the interactions between requirements, analyses and plant design, is described similarly and on a very high level in each case study.

The following aspects are highlighted in relation to the different steps of the SEP:

- **Safety requirement** sources can be considered similar in each case study, as the requirements of the national nuclear regulations are the primary basis of the driving requirements. In one case study, the Fukushima event and the corresponding stress test, in another one the periodic safety review played also a role in initiating the safety analyses and plant modifications.

- **Safety analyses**: the following analyses were performed in the different disciplines:
  - **DSA**:
    - structural strength analysis was conducted in each of the case studies as it is the primary means of justifying protection against snow loads in a NPP;
    - selection of safety related buildings was included in one of the case studies that was due to the fact that this case study focuses on the assessment of the overall plant safety, rather than the protection of a particular building against snow load;
    - assessment of the effects of roof collapse, i.e. it was assessed in one of the case studies which SSCs should be expected to fail due to roof collapse from among those that are located within the building in question, while in the other cases the expected SSC failure was either self-evident (EDG building), or conservatively assumed that all SSCs within the building will fail;
    - deterministic hazard assessment was mentioned in two case studies; however, the development of hazard curves and definition of the design basis from these curves is usually based on the use of probabilistic methods;
  - **PSA** followed the commonly known steps of external hazard PSA in each case study, i.e.:
    - probabilistic hazard assessment;
    - plant response and fragility analysis;
    - PSA model development (including amongst others the identification and characterization of snow induced transients, development of accident sequence models, fault tree analysis, HRA and input data assessment);
    - risk quantification and interpretation of results;
  - **HFE**:
    - in all the case studies, the main task of HFE was to ensure efficient snow removal from the roofs of safety related buildings, primarily by elaborating the operating procedures controlling snow removal;
    - in one of the case studies, control room actions were addressed too; however, it was stated that these actions do not significantly differ from the operator actions that should be taken in response to internal initiating events, hence these actions are not snow-specific.

- **Plant design** was modified in each of the case studies: in two cases, some structural components were strengthened and all three operating procedures controlling snow removal were elaborated or improved in a similar fashion.

The following aspects are highlighted in relation to the flow of information in the SEP:

- On the 1st level of the SEP (safety requirements, safety analysis and plant design) the flow of information is similar in each case study. On one hand, there is no feedback from the analysis or the plant modifications to the requirements; therefore, this interconnection can be regarded as unidirectional. On the other hand, as safety assessments define the extent and the method of strengthening vulnerable structural elements, or elaborating or refining operating procedures that control snow removal, the modifications were considered in the assessments prior to performing them. Thus, the feedback from the actual plant modifications did not play a significant role in the revised analyses.
Chapter E.4 describes the 2nd level of the SEP (interconnection between DSA, PSA and HFE) in detail. A brief summary is given hereby as follows. It is appropriate to perform structural strength analysis and other types of DSA (e.g., selection of safety related SSCs, evaluation of the consequences of a roof collapse) first. The results of DSA were used in HFE and PSA in all the case studies to the extent it seemed practicable and feasible. The operating procedures that control snow removal had been elaborated earlier than the snow PSAs were completed. Use was made of PSA in two case studies to review and further improve HFE (primarily the relevant operating procedures).

On the 3rd level of the SEP (interconnection within the different disciplines) the flow of information seems reasonably good. The different steps in a discipline are generally performed sequentially, e.g., in PSA (1) hazard assessment, (2) plant response and fragility analysis, (3) PSA model development, and (4) risk quantification and interpretation of results are taken care of one after another. However, there is a strong connection between the experts responsible for the different analysis steps; hence the feedback and refinements made and the revisions initiated by a later analysis step can be performed efficiently. The same approach is applied in DSA and in HFE.

It can be concluded that the safety engineering practice was initiated by some high level safety requirements as well as the conclusions of periodic safety reviews or stress-tests. The relevant requirements were in the forefront of the analyses. The plant design was modified on the basis of the analyses performed. Naturally, on a high level, the interrelationship of safety requirements, supporting analyses and related plant design can be regarded as mature and sound in each case study. The analysis steps in the different case studies seem similar and complete. The interconnection within the different disciplines, i.e., the flow of information between PSA analysis steps (or HFE or DSA analysis steps) seems reasonably good. However, the process of justifying the fulfillment of the relevant, multi-disciplinary requirements was not integrated regarding all the disciplines and analysis aspects. In one case study, it was not foreseen at the beginning that all the disciplines (i.e., DSA, PSA and HFE) should be addressed in the verification of the fulfillment of the relevant requirements. Originally, the scope of the analyses covered structural strength analysis, and some structural components were strengthened based on the analysis results. HFE and PSA were performed only some years later, after implementing the proposed plant modifications. It can also be witnessed in the other two case studies that the interactions among the different safety analyses were not intense enough. To sum up, it is regarded as a weakness in the safety engineering process that the different types of analyses pursued and the plant modifications made to verify the fulfillment of the requirements are not the result of a fully and properly integrated approach/framework and thus there is a lack of systematic considerations to the different aspects in combination and in parallel.
### Table E.4. Characterization of the Overall Safety Engineering Process for Case Study Group PVES

<table>
<thead>
<tr>
<th></th>
<th>PVES_1</th>
<th>PVES_2</th>
<th>PVES_3</th>
<th>Conclusions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overall approach</td>
<td>SEP for plant modifications based on a classical V-model; iteration between: - incoming plant design / requirements (design basis of SSCs for external hazards); - system design (improve the roof of the EDG building); - safety assessment (see Ch. 4).</td>
<td>Nuclear Safety Code -&gt; PSR -&gt; safety analyses (DSA, PSA, HFE) -&gt; plant design (strengthening some structural components, operating procedure controlling snow removal). Safety analyses: 1. Structural strength analysis of reactor hall (DSA); 2. Human Factors Engineering (ensure adequate snow removal); 3. PSA (hazard assessment, plant response and fragility assessment, PSA model development, risk quantification and interpretation of results).</td>
<td>Case study developed in the framework of the living PSA programme for NPP Dukovary: 1. derivation of annual frequency of heavy snow event; 2. determination of structures important as potential targets of damage by snow cover; 3. evaluation of vulnerabilities of the rooftops of the structures; 4. evaluation of consequences of rooftop fall; 5. initiating event definition and more detailed specification; 6. modelling of plant response to the individual variants (impact strengths) of extreme snow cover; 7. quantification of PSA model; 8. analysis and interpretation of results of risk analysis.</td>
<td>on a high level, the interrelationship of safety requirements, supporting analyses and related plant design can be regarded as mature and sound in each case study; the analysis steps seem reasonable and complete.</td>
</tr>
<tr>
<td>and steps of the SEP</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Interrelationship</td>
<td>see Table E.3; see V-model in the self-evaluation sheet.</td>
<td>see Table E.3; strengthening some structural components based on structural strength analysis (PSA only for verification purposes); operating procedures elaborated by HFE (only improvements based on PSA).</td>
<td>see Table E.3.</td>
<td>interconnection within the different disciplines seems reasonably good; interactions among the different safety analyses were not intense enough.</td>
</tr>
<tr>
<td>among the Steps</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Strength of the SEP</td>
<td>interaction among requirements, safety analyses and design (V-model)</td>
<td>on a high level, the interrelationship of safety requirements, supporting analyses and related plant design can be regarded as mature and sound.</td>
<td>on a high level, the interrelationship of safety requirements, supporting analyses and related plant design can be regarded as mature and sound.</td>
<td>interconnections on SEP levels 1 and 3 seem adequate and complete.</td>
</tr>
<tr>
<td>Weaknesses of the SEP</td>
<td>PVES_1</td>
<td>PVES_2</td>
<td>PVES_3</td>
<td>Conclusions</td>
</tr>
<tr>
<td>-----------------------</td>
<td>--------</td>
<td>--------</td>
<td>--------</td>
<td>-------------</td>
</tr>
<tr>
<td>Interactions among the safety analyses; lack of fragility curves.</td>
<td>the different types of analyses pursued and the plant modifications made to verify the fulfilment of the requirements are not the result of a fully and properly integrated approach/framework and thus there is a lack of systematic considerations to the different aspects in combination and in parallel.</td>
<td>some parts of DSA are based on engineering assumptions or insufficient data.</td>
<td>Interconnections on SEP level 2 are not adequate.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Proposals for Improvement</th>
<th>PVES_1</th>
<th>PVES_2</th>
<th>PVES_3</th>
<th>Conclusions</th>
</tr>
</thead>
<tbody>
<tr>
<td>More dynamic and frequent interactions between the safety analyses can be beneficial; development of fragility curves would be beneficial.</td>
<td>An action plan (including a road map) should be developed that integrates the various types of analysis necessary for verification; planning of the interconnections between the different types of analyses and analysis steps including the definition of milestones, application of unified input data, scheduling meetings to be organised to inform each other on intermediate or final results from a certain type of analysis.</td>
<td>Supporting analyses needed for case studies related to the topic of external events should be planned even earlier and more carefully than in the case of risk assessment for internal events.</td>
<td>A more systematic and dynamic integrations between the various types of analyses necessary for verification could improve the SEP.</td>
<td></td>
</tr>
</tbody>
</table>
APPENDIX E

E.6 Key Success Factors for an Efficient and Integrated SEP

E.6.1 Key Success Factors

The assessment and evaluation of plant vulnerabilities to extreme snow is initiated by some high level safety requirements as well as the conclusions of periodic safety reviews or stress-tests. In the safety engineering practice followed to perform these assessments, the relevant requirements are in the forefront of the analyses. It is not seen necessary and generally not feasible either to provide feedback from the analyses or the plant modifications to the requirements. Therefore, a unidirectional interconnection can be regarded as adequate in this respect.

Use should be made of the results and insights obtained from the safety assessments to

- identify plant weaknesses;
- specify how the vulnerable structural elements should be strengthened;
- substantiate how the operating procedures that control snow removal should be developed or refine.

The analyses that support the fulfilment of these goals should consider several plant modification options and quantify their effects in order to help determine the most effective plant design change. After plant modifications are completed, all the assessments need to be revised and finalized considering the as built state of the modified plant design. Regarding plant protection against extreme snow, plant modifications can include structural reinforcements and measures for ensuring efficient snow removal from the roofs of the relevant plant buildings or any other actions needed to successfully cope with an extreme snow situation. The latter may include the development of operating procedures to control snow removal, ensuring proper organizational conditions, and improvements in resources of staff and equipment.

During the justification of fulfilling some complex requirements related to multiple disciplines, a safety analysis master plan (including the methodology, criteria and schedule) should be developed. The master plan should identify and integrate the various types of analysis necessary for verification. Of particular importance is planning of the interconnections between the different types of analyses and analysis steps including the definition of milestones, application of unified input data, scheduling meetings to be organised to inform each other on intermediate or final results of a certain type of analysis. A multidisciplinary expert should be nominated to be responsible for task coordination and follow up. A practically reasonable order of work for DSA, PSA and HFE and their interrelationships should be determined. Plant modifications and requirement justification should build upon the results from all the analysis areas in an integrated manner (i.e. no plant modification should be considered properly justified until all the analyses are completed). Self-evidently, structural reinforcements should be designed considering both structural strength analysis and PSA insights (including fragility analysis and safety enhancement proposals). This approach seems more appropriate and effective than performing modifications based on the DSA and PSA results separately. Similarly, all the insights gained from HFE and PSA should be taken into account when developing operating procedures, elaborating training programmes, defining the appropriate tools and equipment, etc. This ensures an improved risk-informed decision making and better substantiated plant modifications in comparison to considering the findings from different types of assessment separately.

As discussed briefly in this paragraph, several analyses are labelled as deterministic safety analyses in the case studies. However, it is seen more appropriate to primarily consider structural strength analysis as DSA when developing a generalized case study from the PVES case study group. The selection of buildings that need to be subject to structural strength analysis in DSA is defined either in the general design (scope of safety related buildings) or during the elaboration of the safety analysis master plan. Probabilistic hazard assessment should be performed as an initial step of PSA, considering primarily probabilistic and complementary deterministic analyses. It is suggested that the design basis of the safety related SSCs as well as the whole NPP should be derived from this assessment. The evaluation of the consequences of a roof collapse on SSCs should be covered in PSA. The initial DSA, i.e. structural strength analysis in this case study group, needs no input from PSA or HFE other than the specification of the design basis load. Consequently, it is appropriate to perform structural strength analysis first, without a need to use support from the other disciplines, except for the definition of the design basis loads. However, if some issues emerge as risk-significant, then a more detailed deterministic assessment may be necessary, and the results of the PSA should be considered when
the structural reinforcement is specified. The results of DSA should be used in HFE and PSA to the extent it is seen practicable and feasible. The different steps in a discipline should generally be performed sequentially, e.g., in PSA (1) hazard assessment, (2) plant response and fragility analysis, (3) PSA model development, (4) risk quantification and interpretation of results are taken care of one after another. However, there should be intense communication between the experts responsible for the different analysis steps to efficiently perform refinements and revisions of preceding analysis steps based on the feedback from later steps. The process may involve several steps of iteration if seen necessary to ensure a sufficiently high level of safety from the point of view of the three disciplines.

E.6.2 Generalized SEP

In Figure E.1 a scheme of a general safety engineering process for case study group PVES is shown. In general, the national and international requirements (see Ia) prescribe that, amongst others, extreme snow shall be taken into consideration during the justification of the design and safety of a nuclear power plant. Moreover, the risk from natural external hazards beyond the design basis shall be assessed. In the generalized process, it is assumed that either severe weather conditions were not completely considered in the original design with the need for completeness in the design of an operating nuclear power plant or the plant in question is under design. Consequently, it is required that appropriate defences should be ensured against the effects of snow hazards 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. As an initial step (1a), a safety analysis master plan (including the methodology, criteria and schedule) (Ila) is developed that identifies and integrates the various types of analysis necessary for verification. Of particular importance is planning of the interconnections between the different types of analyses and analysis steps including the definition of milestones, application of unified input data, scheduling meetings to be organised to inform each other on intermediate or final results of a certain type of analysis. A generalist expert is nominated to be responsible for task coordination and follow up. A practically reasonable order of work is determined (2a, 2b and 2c) for DSA (IIB), HFE (IIc) and PSA (IId).

Snow hazard assessment (IId1) is performed as the first analysis step considering probabilistic as well as deterministic aspects. The design basis of the safety related SSCs as well as the whole NPP is defined in this assessment too. Subsequently, initial structural strength analysis (IIB) is performed on the basis of relevant standards, considering the design basis snow load (5a). Also, the human factors aspects (IIc) of efficient snow removal from the roof of safety related buildings or any other actions needed to successfully cope with an extreme snow situation are examined and evaluated, considering the results of the hazard assessment (5b) and structural strength analysis (3b).

After completing the initial structural strength analyses and the initial HFE tasks, plant response and fragility analysis (IId2) is conducted to enable a quantitative assessment of safety margins by means of the plant PSA (IId) for extreme snow. The plant response and fragility analysis makes use of structural strength (3c) and structural reliability analyses as well as the snow removal strategy elaborated by HFE experts (4a). PSA is applied to justify the fulfillment of probabilistic safety criteria and qualify the adequacy of protecting of the plant or certain structures against snow loads at a higher, facility level. PSA model development (IId3) builds upon the results of hazard assessment (5c), and plant response and fragility analysis (6a) by exercising the commonly known tasks: event sequence modelling, fault tree analysis, human reliability analysis and input data assessment. The HRA within PSA and HFE in the overall safety analysis are largely interrelated activities (4d).

PSA and HFE studies are performed simultaneously and interfacing largely (4c) to enable the use of the PSA insights (7b) to underpin HFE. HFE experts elaborate (4c) an operating procedure for controlling snow removal (IIIb) and ensure the adequacy (4b) of organizational conditions, resources of staff and equipment (IIlc) with considerations to multi-unit aspects, if relevant. The final operating procedures, the organizational conditions ensured, the resources of staff and equipment are all considered when finalizing the HFE (9a, 10a) and the PSA results (9b, 10b).

A refined deterministic assessment may be necessary based on the PSA results and insights (7a), and the results of the structural strength analysis and PSA are considered (3a) when structural reinforcement (Ila) is specified by structural engineers. After the structural reinforcements are completed, the structural strength analysis (8a) and the PSA (8b) are revised and finalized considering the final state of the plant design.
On a very high level, the classical V-model given in Figure E.2 can also be regarded as applicable to describing the engineering process for making plant modifications.

**Figure E.1. Scheme of the General Safety Engineering Process for Case Study Group PVES**
Figure E.2. Classical V-model as a High-level Representation of the Safety Engineering Process for Plant Modifications in Case Study Group PVES
APPENDIX F: CROSS-CASE COMPARISON IN CASE STUDY GROUP EIIC

F.1 General information

Responsible Organization(s): VTT, EDF

Case Study Group Identifier: EIIC

Date: 23/09/2022

Case Study Titles:
- Loss of I&C due to high ambient temperature (EIIC_1)
- Loss of on-site power supply and control due to lightning (EIIC_3)

F.2 Fulfilment of BESEP Safety Requirements

Following four requirements were comparatively assessed in this cross case comparison, they were the ones shared between both case studies:

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

- Initiating event frequency estimation (PSA):
  - BESEP_PSA_EIF_003: The results from long-term monitoring of the NPP site and the surroundings shall be taken into account in the initiating event frequency estimation for external hazards.

- Applicable HSI (Human System Interface) (HFE):
  - BESEP_HFE_HSI_001: The HSI shall be adapted to human capabilities and limitations and it shall prevent the risk of incorrect action as much as possible.

- Validated modelling and simulation analysis tools (SEP):
  - BESEP_SEP_MST_002: The results gained with modelling and simulation analysis tools shall be collected to enable comparison to previous and following results gained with comparable models and tools.

Requirement No. 1 – BESEP_DSA_DCCF_002: Diversity shall be applied within and between defence-in-depth levels so that a common-cause failure of any individual component type shall not prevent managing the initiating event.

Summary of the Verification Process (summary):

The verification process of the EIIC_1 case-study was decomposed in two separate sub-claims, namely: diversity within DID levels and diversity between DID levels. After that, arguments were identified to support these two sub-claims. Evidence was provided by collecting technical data to support the arguments. The evidence in this case came from:

- Quality of components (datasheet and experiments)
- Technology of components (datasheet)
- Cooling simulations (models and scenarios)
- Experimental validation (measured temperatures)
- Diversity of support for cooling (engineering diagrams including P&ID)
- Real time temperature monitoring and control (P&ID, HMI)

The verification process of the EIIC_3 case-study considers two main topics: the reliability of the protection relay and a diversity analysis of the protection relays.

For the verification of diversity and common-cause failure requirements a previous assessment on the reliability estimation of a computer-based protection relay was applied. The previous assessment focuses mainly on the software reliability of the protection relays, but the quantitative estimates generated in the previous assessment have been used as a basis for the reliability estimates of protection relays and their
configuration in the lightning induced case study of EIIC_1. The reliability estimation methodology of the example is based on Bayesian networks. A prior estimate of example protection relay is created using expert judgements from the relay developers. The prior estimate is later updated to a posterior estimate using operational experience collected for the relay.

To fulfil the common cause failure (CCF) and diversity requirements, the overvoltage protection function has been implemented with a system comprising of two diverse protection relays functioning in 1 out of 2 logic opening of the circuit breakers connecting to the safety bus.

Comparison:
- Both verification processes use the reliability of the I&C component in question, but the means or techniques to obtain the results are not necessarily identical. Nevertheless, Bayesian networks is a well applied technique in reliability studies.
- Both case-studies make use of detailed schemes exposing the functioning and implementation of the (protection) system, in order to analyse the fulfilment of the CCF requirement.

Adequacy of Verification (comparison):

Evidence for all arguments of the EICC_1 case-study to support the justification are compared to their limits, validated norms or other boundary characteristics. The quality of the components is verified by experiments and the numerical findings of room and cabinet temperatures are validated by experiments (on a real plant and / or a mock-up).

Based on the assessment for the EIIC_3 case-study, the impact of CCF within one redundancy is minor. For both redundancies the CCF has not been explicitly included in the assessment, but the assumed to be included in the 10% failure estimate. If CCF would be modelled explicitly for both redundancies the significance of CCF would be increased.

Estimation of software failures for the EIIC_3 case-study is challenging due to lack of available data. The CCF estimation of two diverse computer-based systems is even more challenging as there is basically no good public references available on the topic. In the assessment, the 1% estimate is used for the CCF, however this value is highly speculative and should be considered with caution and compared to literature values.

Comparison: While the EICC_1 concentrates on the margins of the I&C components, the EIIC_3 concentrates on the impact of a (common cause) failure. The latter uses the estimated low frequency values to verify the requirement. Both cases are challenged by the availability of detailed input data.

Proposals for Improvement (identified good practices):

Proposals to improve the fulfilment of the requirements for the EIIC_1 case-study are: Software to apply the CAE method is still under development, and lacks (semi-) automatic verification and connections between cases (and plants).

Proposals to improve the fulfilment of the requirements for the EIIC_3 case-study are: improved methodologies for assessing the software-based CCF are needed to further improve the estimation and to verify the fulfilment of diversity requirement of the protection relays.

More data and better references on the software reliability of I&C system is needed.

The assessment should be complemented by including the manual operations and other defence-in-depth levels to the analysis.

Comparison: the proposed improvements complement each other and at least those listed for EIIC_3 are also valid for EICC_1.

Requirement No. 2 – BESEP_PSA_EIF_003: The results from long-term monitoring of the NPP site and the surroundings shall be taken into account in the initiating event frequency estimation for external hazards.

Summary of the Verification Process (summary):
For EIIC_1 case study, the external hazard of interest is high ambient temperatures that may cause the I&C system to malfunction. The initiating event frequency estimation is based on the use and development of high quality long-term historical temperature data. For rare extreme temperature events, statistic extrapolation methods based on data in limited time, can be applied. Temperature data are measured in various locations and can be available for different time ranges for specific sites. Data from similar sites, notably those in the same climate category (continental, coastal, tempered) can be taken into account to identify trends, or to compare with the local data.

For EIIC_3 case study, the external hazard of interest is lightning induced loss of on-site power supply and control. The site-specific frequency estimates for the lightning strike are based on the data analysis of closest national/international sensor location measurement data. The strike frequency to the site-specific switchyard is based on the conclusions of the data analysis. The switchyard has not been the special focus of the data analysis and therefore some expert judgment has been utilized.

Adequacy of Verification (comparison):

Both case studies rely on data analysis and statistical methods as the main approach for the initiating event frequency estimation. The adequacy of verification is dependent on the quality and sufficiency of the data. To estimate situation of insufficient data, EIIC_1 relies primarily on statistical extrapolation methods also taking climate projections into consideration. EIIC_3 relies primarily on expert judgements taking also into consideration the trend of increased lightning frequency and energy. The application of data from other similar sites is explicitly mentioned in EIIC_1. In EIIC_3, it is mentioned that site initiating event frequencies should be compared to values of other similar sites.

Proposals for Improvement (identified good practices):

The main improvement proposal is the continuous collection of data and improvement of state-of-the-art estimation methods in close connection to measurement disciplines. Further refinement of statistical distribution of weather phenomena and better utilisation of expert judgements to remove uncertainty based on findings on the correlation on climate change and extreme weather conditions.

More interaction and sharing of data and results between PSA, DSA and HFE could give better insights into the sensitivity of variation of weather parameter on the margins of each domain.

Requirement No. 3 – BESEP_HFE_HSI_001: The HSI shall be adapted to human capabilities and limitations and it shall prevent the risk of incorrect action as much as possible.

Summary of the Verification Process (summary):

The verification process for EIIC_1 is based on five performance shaping factors that are selected for the argumentation in support to the top claim. The verification process for EIIC_3 is based on the evaluation of a loss of on-site power supply and control simulator runs in a full-scope plant simulator. Quantitative acceptance criteria for these display-specific requirements are difficult to set, but this limitation can be avoided by a triangulation approach in which multiple qualitative methods and data sources are used to provide cumulative evidence of the acceptability of the requirements. The design of the EDG displays can be considered validated, when all the Human Engineering Discrepancies (i.e., design deficiencies) have been settled, and by implication all the display-specific requirements have been fulfilled.

Comparison: While EIIC_1 takes a more general approach, namely: performance shaping factors, EIIC_3 takes a specific approach tailored for the case-study (EDG display requirement validation and full-scope simulations)

Adequacy of Verification (comparison):

EIIC_1: Performance shaping factors are widely used (IAEA document) to evaluate or assure a good working environment for operators. The control room temperature stays within the defined limits. Evaluation and analysis of experiments validate the human performance on physical interaction with the HMI. Workload is assessed by experiments and by theory. The situation awareness is evaluated to be within the chosen limits and improved by using the same type of interface in accident situations and in normal operation. Time for actions to be taken (relocation to another room, weather forecast analysis), is well within the limits.
EIIC_3: Systems Usability Case (SUC) enables a requirement-based human factors evaluation of the EDG display system. The SUC is based on the Safety Case approach and on the Systems Usability construct. One of the main aims of establishing a Safety Case is to bring to the front the arguments and evidence for safety in such a way that the reasoning supports the work of a regulator or licensing organization. In the end, the SUC enables evaluating the Systems Usability of the display system and making a reasonable solid argument about the acceptance of the system for use. The question is how the conclusions are reached through a reasoning process, in which the arguments are made about the evidence to approve or reject the claim concerning the quality of the system.

Comparison: One case-study is mainly based on the evaluation by HF experts without explicit requirements. It evaluates how well or poorly the potential challenge is managed. This differs from the second case-study, where a requirement-based human factors evaluation is applied enabling the acceptance or rejection of the system.

Proposals for Improvement (identified good practices):

EIIC_1: Continuous improvements are made in the field of human factors, based on new insights. Internationally validated experiments with operators are scarce and the availability of operators to do such experiments is limited.

EIIC_3: The design-specific requirements should be prioritized and graded according to their safety importance.

Comparison: The proposals for improvement are different for both cases: one makes a parallel with the graded approach and the impact on safety. The other tends to improve by continuously following the state of the art in the HFE domain.

Requirement No. 4 – BESEP_SEP_MST_002: The results gained with modelling and simulation analysis tools shall be collected to enable comparison to previous and following results gained with comparable models and tools

Summary of the Verification Process (summary):

The case studies utilise well-known simulation software and modelling methods, such as APROS and Bayesian networks. Before the utilisation, the simulation software and methods have been tested and validated in practice or in research projects of nuclear or similarly critical domains. The human actions modelling includes a specific Systems Usability Case method. Claim-argument-evidence (CAE) approach justify that the set of design and operational measures taken indeed ensure that the risk of unacceptable conditions induced by credible external event, through the I&C, remains acceptable. Example of CAE approach to verification process of the requirement is shown in Figure F.1.

Figure F.1. Example verification process for requirement BESEP_SEP_MST_002.

Adequacy of Verification (comparison):

Both cases have a similar approach to judging the trustworthiness of the tools for the verification process. The creditability of modelling and simulation analysis tools are ensured, for example, with the use of internationally validated software tools, benchmarking of available tools, safe and sure storage and backup of data, interchangeable (open) numerical format for models, and experimental data. The used models include descriptions on what and how they are applied in the overall assessment, no black box models were used. The models use mathematical formulation for calculations. However, some of the models and/or tools were
not previously used in the specific site, so further analysis of their behaviour is required. The results have not been compared to results of other similar, validated tools.

However, neither of the cases truly discuss the collection of the results and comparison of the results to the previously available ones, only mentioned in the improvement part.

*Proposals for Improvement (identified good practices):*

Improvements in a digital platform easily accessible to all disciplines and on different levels of abstraction could simplify the interaction between the different safety analysis. (Semi-)automatic transcription of changes in norms, limits, etc. could be helpful in the above-mentioned digital platform. Other improvements include further collection of results, and further evaluation of models and simulation tools to other similar configurations, sites, and tools.
Table F.1. Fulfilment of BESEP Safety Requirements

<table>
<thead>
<tr>
<th>EIIC_1</th>
<th>EIIC_3</th>
<th>Conclusions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>BESEP requirement ID:</strong> BESEP_DSA_DCCF_002: Diversity shall be applied within and between defence-in-depth levels so that a common-cause failure of any individual component type shall not prevent managing the initiating event.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Key features of the verification process</strong></td>
<td><strong>Methodology for reliability estimation of a computer-based protection relay:</strong></td>
<td><strong>Both verification processes use the reliability of I&amp;C components, but the means or techniques to obtain the results are not necessarily identical.</strong></td>
</tr>
<tr>
<td>Decomposition of the requirement (claim): diversity within DID levels &amp; diversity between DiD levels</td>
<td>• based on Bayesian networks</td>
<td>Both case-studies make use of detailed schemes exposing the functioning and implementation of the (protection) system.</td>
</tr>
<tr>
<td>Each argument is supported by a technical development (evidence):</td>
<td>• The prior estimate by expert judgements (relay developers)</td>
<td></td>
</tr>
<tr>
<td>• quality of components</td>
<td>• Fulfilment of common cause failure (CCF) and diversity requirements:</td>
<td></td>
</tr>
<tr>
<td>• technology of components</td>
<td>• implementation of overvoltage protection function by two diverse protection relays functioning in 1 out of 2</td>
<td></td>
</tr>
<tr>
<td>• cooling simulations</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• diversity of support for cooling</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Adequacy of Verification</strong></td>
<td><strong>Assessment show that the impact of CCF within one redundancy is minor. With explicit modelling of both redundancies, the significance of CCF would be increased.</strong></td>
<td><strong>EICC_.1 concentrates on the margins of the I&amp;C components. EIIC_.3 concentrates on the impact of a common cause failure. The requirement verification is based on the estimated low frequency values for CCF.</strong></td>
</tr>
<tr>
<td>Evidence for all arguments to support the justification are compared to their limits, validated norms or other boundary characteristics.</td>
<td>Estimation of software failures is challenging due to lack of available data. No good public references are available on the topic. The CCF estimate used in the assessment should be considered with caution.</td>
<td>Both case-studies consider the verification approach adequate, but notify that the verification is challenged by the availability of detailed input data.</td>
</tr>
</tbody>
</table>
### Proposals for Improvement

<table>
<thead>
<tr>
<th>Proposals for Improvement</th>
<th>Improvement Methodologies for Assessing the Software-based CCF are needed. These would improve the verification of the fulfilment of the diversity requirement of the protection relays.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software to apply the CAE method is still under development, and lacks (semi-) automatic verification and connections between cases</td>
<td>More data and better references on the software reliability of I&amp;C system is needed. The assessment should be complemented by including the manual operations and other defence-in-depth levels to the analysis.</td>
</tr>
</tbody>
</table>

#### BESEP requirement ID: BESEP_PSA{EIF}_003: The results from long-term monitoring of the NPP site and the surroundings shall be taken into account in the initiating event frequency estimation for external hazards.

<table>
<thead>
<tr>
<th>Key features of the verification process</th>
<th>Site specific lightning frequency estimates are based on the data analysis of closest national/international sensor location measurement data. More specific frequency estimates are generated from the data using expert judgements.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use and development of high quality long-term historical temperature data</td>
<td>Both case studies rely on data analysis and statistical methods as the main approach for the initiating event frequency estimation. Therefore, the performance of the data analysis creates the basis of the verification process.</td>
</tr>
<tr>
<td>For rare extreme temperature events, statistic extrapolation methods based on data limited in time</td>
<td></td>
</tr>
<tr>
<td>Data collection from various sites with same climate category</td>
<td></td>
</tr>
</tbody>
</table>

The proposed improvements complement each other and those listed for EIIC_3 are also valid for EIIC_1.
| Adequacy of Verification | Internationally validated state-of-the-art statistical tools are used.  
For rare events, statistical extrapolations and internationally validated specific distributions are applied.  
Climate projections are taken into account but have high uncertainty.  
Temperatures at/or near the site are measured with a low and known uncertainty for several decades.  
Data from similar sites, notably those in the same climate category (continental, coastal, tempered) can be taken into account to identify trends, or to compare with the local data. | The verification is based on best available lightning strike frequency data from the closest national measurement/sensor locations.  
The data estimate has been supported by expert judgement.  
The trend of lightning frequency and energy seems to have increased causing uncertainty to the applicability of frequency estimates in the future.  
Site initiating event frequencies should be still compared to values of other similar sites. | The adequacy of verification is dependent on the quality and sufficiency of the data.  
For the estimation of events with insufficient data base, statistical extrapolations and expert judgements have been applied as the main approaches. |
| Proposals for Improvement | Continuous improvements to obtain a reasonably representative distribution of the frequency of rare events are desirable.  
The survey and improvement of state-of-the-art estimation methods and close connection to measurement disciplines.  
Reduce the uncertainty of climate change on extreme temperatures and heatwaves  
More interaction and sharing of data or results between PSA, DSA and HFE could give better insights into the variations on the margins of each domain. | The continuous collection of lightning data to enable the long term monitoring of lightning induced initiating events at site.  
Better lightning data coverage from more site specific measurement / sensor locations will improve the analysis.  
Further refinement of expert judgment in the initiating event frequency estimation based on finding correlations between future evolution of convective weather conditions and the lightning strike frequency and energy. | Continuous collection of data and improvement of state-of-the-art estimation methods in close connection to measurement disciplines.  
Better interaction and sharing of data and results between PSA, DSA and HFE to give better insights into the sensitivity of variation of weather parameter on the margins of each domain. |

**BESEP requirement ID:** BESEP_HFE_HSI_001: The HSI shall be adapted to human capabilities and limitations and it shall prevent the risk of incorrect action as much as possible.
### Key features of the verification process

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
<th>Requirements</th>
<th>EIIC_1 takes the performance shaping factors approach.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Five performance shaping factors are selected to support the argumentation for the top claim.</td>
<td>Requirements are evaluated for loss of on-site power supply using a full-scope plant simulator runs.</td>
<td>Quantitative acceptance criteria for display-specific requirements by a triangulation approach: multiple qualitative methods &amp; data sources to provide cumulative evidence of the acceptability of the requirements. Validation of the design of the EDG displays: no Human Engineering Discrepancies (i.e., design deficiencies) &amp; fulfilment of all display-specific requirements.</td>
<td>EIIC_3 takes a specific approach tailored for the case-study (EDG display requirement validation and full-scope simulations).</td>
</tr>
</tbody>
</table>

### Adequacy of Verification

<table>
<thead>
<tr>
<th>Description</th>
<th>Systems Usability Case (SUC) enables a requirement-based human factors evaluation of the EDG display system.</th>
<th>The SUC is based on the Safety Case approach and on the Systems Usability construct. It exposes the arguments and evidence for safety.</th>
<th>One case-study is mainly based on the evaluation by HF experts to avoid explicit requirements, it evaluates how well or poorly the potential challenge is managed. This differs from the second case-study where a requirement-based human factors evaluation is applied enabling the acceptance or rejection of the system.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Performance shaping factors are widely used (IAEA document) to evaluate or assure a good working environment for operators.</td>
<td>Systems Usability Case (SUC) enables a requirement-based human factors evaluation of the EDG display system.</td>
<td>SUC enables evaluating the Systems Usability of the display system and making a reasonable solid argument about the acceptance of the system for use.</td>
<td></td>
</tr>
<tr>
<td>The control room temperature stays within the defined limits</td>
<td>Systems Usability Case (SUC) enables a requirement-based human factors evaluation of the EDG display system.</td>
<td>The question is how the conclusions are reached through a reasoning process, in which the arguments are made about the evidence to approve or reject the claim concerning the quality of the system.</td>
<td></td>
</tr>
<tr>
<td>Evaluation and analysis of experiments validate the human performance on physical interaction with the HMI</td>
<td>Systems Usability Case (SUC) enables a requirement-based human factors evaluation of the EDG display system.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Workload is assessed by experiments and by theory</td>
<td>Systems Usability Case (SUC) enables a requirement-based human factors evaluation of the EDG display system.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The situation awareness is evaluated to be within the chosen limits and improved by using the same type of interface in accident situations and in normal operation</td>
<td>Systems Usability Case (SUC) enables a requirement-based human factors evaluation of the EDG display system.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Time for actions to be taken (relocation to another room, weather forecast analysis), is well within the limits.</td>
<td>Systems Usability Case (SUC) enables a requirement-based human factors evaluation of the EDG display system.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Proposals for Improvement
Continuous improvements are made in the field of human factors, based on new insights. Internationally validated experiments with operators are scarce and the availability of operators to do such experiments is limited.

The design-specific requirements should be prioritized and graded according to their safety importance.

Proposals for improvement are different for each case. One makes a parallel with the graded approach and the impact on safety. The other tends to improve by continuously following the state of the art in the HFE domain.

### BESEP requirement ID: BESEP_SEP_MST_002
The results gained with modelling and simulation analysis tools shall be collected to enable comparison to previous and following results gained with comparable models and tools.

### Key features of the verification process
- The use of internationally validated software tools.
- Benchmarking of available tools. Safe and sure storage and backup of data. Interchangeable (open) numerical format for models, experimental data, hypothesis, etc…
- CAE method for constructing the verification of the requirement.

### Description of the different modelling and simulation analysis tools used in the verification process of safety requirements.

### Evaluating the trustworthiness of the tools and models; well-known simulation software and modelling methods; that have been in use in nuclear or similarly critical domains; CAE approach

### Adequacy of Verification
- Use of only validated or recognised (software) tools in each discipline (DSA, PSA, HFE).
- The CAE method can be seen as a systematic and logic way in the SEP process.

### Descriptions on what and how tools and models; no black box models; use of mathematical formulation for calculations.
- Further analysis of their behaviour on the specific site is required.
- Need comparing to results of other similar, validated tools.

### Both cases approach the verification of the results by judging the trustworthiness of the tools, not specifically comparing the results.

### Proposals for Improvement
- Improvements in a digital platform easily accessible to all disciplines and on different levels of abstraction could simplify the interaction between the different safety analysis.
- (Semi-)automatic transcription of changes in norms, limits, etc., could be helpful in the above mentioned digital platform.

### Further collection of results, and evaluation of models and simulation tools to other similar configurations, sites, and tools.

### Both cases mention further collections of results and comparing them to other similar results and norms.
F.3 Safety Margins Assessment

**Deterministic Safety Margins**

*Definition (comparison):*

The definition as stated in deliverable D2.3 of the deterministic safety margin was adopted for case-study EIIC_1. The main deterministic safety margin of interest was the allowable temperature for the (safety related) I&C components.

For EIIC_3, the deterministic safety margins under consideration were:

- Lightning strike frequency and progression at the plant;
- The component (software and hardware) reliability estimates;
- Common-cause frequency estimates;
- Relay configuration and voting logic selection.

Comparison: While EIIC_1 has studied the margins related to the physical variable temperature, EIIC_3 has focused on the lightning strike frequency, its effects and component reliability estimates and uncertainties.

*Assessment and Evaluation (comparison):*

EIIC_1: The assessment and the evaluation are based on deterministic simulations (with validated software tools) of the temperature (room, components, etc.), possibly by CFD. Additionally, a mock-up is constructed for validation.

The “distance” to the limits according to the DSA safety definition before component failure (including margins and uncertainties) are then determined.

EIIC_3: Lightning strike frequency was estimated based on meteorological measurement data. The over-voltage effect of lightning to the on-site electrical networks of the plant was modelled and simulated using simulation tools. The component software reliability estimates were generated based on expert judgement and operational experience data.

Hardware and common cause failure estimates were generated from the software reliability estimates.

Relay configuration and voting logic selection was not explicitly assessed, but the selection was done with fail-safe emphasis.

Comparison: In one case-study, the focus was on the simulation of physical temperature of system components / rooms and their validation (including uncertainties of the measurements). In the other case-study the focus was on the lightning frequency estimates and over-voltage simulations, which provided background information for the component reliability and CCF estimates.

*Comparison with D2.3*

The main deterministic safety margins in the case studies were the results of component temperature and lightning induced over-voltage simulations. The deterministic safety margins are in line with D2.3. Of course, it could be argued if component reliability estimates should be considered in deterministic or probabilistic safety margins.

*Proposals for Improvement (identify good practices):*

EIIC_1: More interaction (in both directions) with PSA and HFE could improve the weaknesses (and strength) of the system as well as a common ground for improvement.

The reduction of the uncertainties that are naturally present like turbulence can always be improved by specific experiments and measurement devices.
The use of components consuming less power could increase dramatically the safety margin of the components. This implicates the potential improvement to eliminate sophisticated simulations.

EIIC_3: More data and better utilisation of over-voltage simulation results in the reliability estimates, and on the other hand, a comprehensive PSA model to guide where the reliability estimations have the most impact, would be beneficial.

Comparison: Both case-studies propose to tighten the interactions with other disciplines (DSA, PSA, HFE) for improvement.

**Probabilistic Safety Margins**

*Definition (comparison)*:

EIIC_1: The scope was limited to the frequency and amplitude of high ambient temperatures. In order to compare the impact of high ambient temperatures on CDF and LERF scenarios are to be simulated with deterministic models, and apparently after that, the results would be implemented to a PSA model.

EIIC_3: The closest correspondence to probabilistic safety margins is the initiating event frequency estimate for the loss of on-site power in one or two redundancy. For the case study, comprehensive PSA model was not available. Therefore, it was not possible to calculate typical probabilistic safety margins, such as CDF and LERF, listed in D2.3.

Based on the self-evaluation results the probabilistic safety margins listed in D2.3 have been acknowledged, but not applied in the case studies. This is mainly due to the unavailability of PSA models and the scope and focus of the case studies. Both cases concentrate on the evaluation of the initiating frequency, or its progression to certain plant state, which has been different from CDF or LERF.

*Assessment and Evaluation (comparison)*:

Since both cases concentrate on the estimation of initiating event frequency, or its progression to certain plant state, without an actual PSA model, the chosen assessment methods are similar and rely strongly on the results of data analysis.

*Proposals for Improvement (identify good practices)*:

Data analysis and statistical methods are the default approaches for the initiating event frequency estimation. For situation with sparse data, the analysis can be supported by expert judgements.

In EIIC_1, the analysis can be improved by reducing the uncertainty around the frequency estimation of high ambient temperatures and around the non-detection of heatwaves by meteorological forecasts. One improvement can be also the use of low power or passive systems. The low power or passive systems reduce the impact of high temperatures on I&C systems leading to inherent safe systems, where risk of power loss due to high ambient temperatures becomes insignificant.

In EIIC_3, the system architecture and protection configuration has been described in more detail. If more penetrating analysis on the strengths and weaknesses of different system architectures or protection configurations would be desired, this could be achieved for example by comparing the minimum cut sets of PSA models for different architectures or configurations. Of course, these analyses can be quite involving and laborious requiring detailed PSA models.

**Safety Margin for Human Actions**

*Definition (comparison)*:

EIIC_1: In this case-study, the safety margin assessment follows the performance shaping factors methodology. Two different parts intervene: human reliability and resilience or the ability to generate correcting or mitigating actions that were not foreseen in advance. It is possible to apply the CAE method even when no hard limits are available or when unforeseen situations happen.
EIIC_3: Measures for human performance evaluation of the EDG displays system are categorized into the following six classes:

- plant performance
- personnel task performance
- situation awareness,
- stress, workload and fatigue
- teamwork
- anthropometric physiological indicators

Comparison: Both case-studies use measures to evaluate the human performance, most of them coincide.

Assessment and Evaluation (comparison):

EIIC_3: Systems Usability Case (SUC) enables the evaluation of the Systems Usability of the EDG system and making a reasonable solid argument about the acceptance of the system for use. It describes how the conclusions are reached through a reasoning process, in which the arguments are made about the evidence to approve or reject the claim concerning the quality of the system.

Comparison: The elements coming from human performance analysis are at the basis of the reasoning to accept the system or not from the HRE point of view.

Comparison with D2.3:

EIIC_3: Verification and validation of the EDG system in terms of Systems usability demonstrates that the system fulfils the general systems usability and specific system-specific requirements and thus supports the safe operation of the power process.

Comparison: as stated in D2.3, the safety margins cannot be defined by numerical values as can be done by PSA (CDF, LERF) or DSA (fuel temperature, etc), but both use a method and reasoning to assess how well the system copes in certain situations (like in the two case-studies).

Proposals for Improvement (identify good practices):

EIIC_3: Quantitative acceptance criteria for the systems usability and system-specific requirements are difficult to set, but this limitation can be avoided by a triangulation approach in which multiple qualitative methods and data sources are used to provide cumulative evidence of the acceptability of the requirements.

Comparison: Continue the human performance studies with their measurements and uncertainty (specifically in similar situation). This concerns the availability of data in foreseen, but also in unforeseen situations. In some cases, qualitative criteria could be defined.
Table F.2. Assessment of Safety Margins:

<table>
<thead>
<tr>
<th>EIIC_1</th>
<th>EIIC_3</th>
<th>Conclusions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Deterministic Safety Margins</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| **Definition** | Deterministic safety margins under consideration were:  
  - Lightning strike frequency and progression at the plant;  
  - The component (software and hardware) reliability estimates;  
  - Common-cause frequency estimates;  
  - Relay configuration and voting logic selection. |
| | While EIIC_1 has studied the margins related to the physical variable temperature, EIIC_3 has focused on the lightning strike frequency, its effects and component reliability estimates and uncertainties. |
| **Assessment & Evaluation** | Lightning strike frequency was estimated based on meteorological measurement data.  
  The lightning induced over-voltage effects based on simulation tools.  
  The component software reliability estimates were generated based on expert judgement and operational experience data.  
  Hardware and common cause failure estimates were generated from the software reliability estimates.  
  Relay configuration and voting logic selection was not explicitly assessed, but the selection was done with fail-safe emphasis. |
| | EIIC_1 focused on the simulation of physical temperature of system components / rooms and their validation (including uncertainties of the measurements).  
  EIIC_3 focused on the lightning frequency estimates and over-voltage simulations, which provided background information for the component reliability and CCF estimates.  
  As one validation method, both cases applied simulation of physical variables having an impact to the functioning of safety system. The simulations based assessment results were complemented with using expert judgement and operational experience assessments. |
## Comparison with D2.3

| Comparison with D2.3 | Same definition | Deterministic safety margins in the case study focused on the lightning frequency estimates and over-voltage simulations, which provided background information for the component reliability and CCF estimates. | The main deterministic safety margins in the case studies were the results of component temperature and lightning induced over-voltage simulations. In general, both case-studies are compatible with the deterministic safety margin definition of D2.3. Of course, it could be argued if component reliability estimates should be considered in deterministic or probabilistic safety margins. |

## Proposals for Improvement

| Proposals for Improvement | More interaction with PSA and HFE. Reduction of the uncertainties that are naturally present like turbulence Use of components consuming less power | More and better data. Better utilisation of over-voltage simulation results in the reliability estimates, and on the other hand, a comprehensive PSA model to guide where the reliability estimations have the most impact. | Both case-studies propose to tighten the interactions with other disciplines (DSA, PSA, HFE) for improvement, especially emphasising interaction with PSA. |

## Probabilistic Safety Margins

<table>
<thead>
<tr>
<th>EIIC_1</th>
<th>EIIC_3</th>
<th>Conclusions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Definition</strong></td>
<td>Frequency and amplitude of high ambient temperatures.</td>
<td>Lightning strike initiating event frequency. Initiating event frequency estimate for the loss of on-site power in one or two redundancy.</td>
</tr>
</tbody>
</table>
### Assessment & Evaluation

| Use of distributions that are specifically adapted to rare events at the edges of the distribution. Uncertainties of the whole chain of measurements are taken into account (including sensors, data compression, bit length, database, etc.) |
| Data analysis and expert judgement were used to generate the initiating event frequency for the lightning strike external hazard and for the loss of on-site power in one or two redundancy. |
| In both cases the chosen assessment methods are similar and rely strongly on the results of data analysis. |

### Comparison with D2.3

| D2.3 definition are acknowledged, but not applied in the case study. |
| No CDF was estimated due to unavailability of comprehensive PSA model. With PSA model, the CDF could be estimated using the estimated initiating event values. |
| Safety margins listed in D2.3 could be applied but haven’t been applied due to the unavailability of PSA models and the scope and focus on the case studies. |

### Proposals for Improvement

| Reduction of the uncertainty around the frequency estimation of high ambient temperatures Use of low power or passive systems |
| More penetrating analysis on the strengths and weaknesses of different system architectures or protection configurations could be achieved by comparing the minimum cut sets of PSA models for different architectures or configurations. |
| For the purposes of the case studies, data analysis and statistical methods have been seen sufficient approaches. With comprehensive PSA model the CDF values could be attained and compared to regulatory acceptance criteria. Minimum cut sets from PSA model could be also used to evaluate the strengths and weaknesses of different system architecture designs or protection configurations. |

### Safety Margins for Human Actions

<table>
<thead>
<tr>
<th>EIIC_1</th>
<th>EIIC_3</th>
<th>Conclusions</th>
</tr>
</thead>
</table>
| Definition | Safety margins evaluated from performance shaping factors.  
Two sides:  
- human reliability  
- resilience and generation of unforeseen actions. | Measures for human performance evaluation of the EDG displays system are categorized into the following six classes:  
- plant performance  
- personnel task performance  
- situation awareness,  
- stress, workload and fatigue  
- teamwork  
- anthropometric physiological indicators | Both case-studies use measures to evaluate the human performance, for example using performance shaping factors. |
| Assessment & Evaluation | Five topics from the performance shaping factors.  
Deterministic simulations of room temperatures and distance / time needed for relocation.  
Expert judgement for workload assessment | Systems Usability Case (SUC) enables the evaluation of the Systems Usability of the EDG system | The elements coming from human performance analysis are at the basis of the reasoning to accept the system or not from the HRE point of view. |
| Comparison with D2.3 | Same as D2.3.  
Safety-margins from HRE:  
- Resilience  
- “deterministic” HRA | Verification and validation by systems usability demonstrates that the system fulfils the requirements. | No numerical value can be defined for the safety margin (No CDF, LERF or fuel temperature, etc), but both case-studies apply a similar method and reasoning to for the assessment. |
| Proposals for Improvement | Good performance measures and their uncertainty of human capabilities to recreate safety margins in stressful and unforeseen situations.  
Extended data and experiences to evaluate the credit of human actions in unforeseen situations. | Definition of quantitative acceptance criteria where possible.  
Extended development on the triangulation approach: more qualitative methods and more data sources to provide cumulative evidence of the acceptability of the requirements. | Studies on human performance (in situ).  
Availability of data (in foreseen and in unforeseen situations). |
F.4 Interactions between DSA, PSA and HFE

Interactions between DSA, PSA and HFE (describe and compare):

EIIC_1: DSA, PSA and HFE interact with each other by exchanging information and results of their studies respectively. One of the results coming from PSA is the frequency of high external ambient temperatures. Thus, the probability that a design extension event of high amplitude occurs.

PSA also estimates (but not only):
- rank the importance of the components in case of high ambient temperatures (fault trees).
- estimate the probabilities of human errors due to an uncomfortable temperature.

This gives information on which scenario to simulate (in DSA and HFE), to demonstrate the ability of the safety systems and the performance of the plant operators. DSA estimates the strength of the components, the thermal distribution of the heat in and around the I&C components, cabinets and rooms that can be used in PSA. In addition, probabilistic inputs from PSA, concerning the scenarios to simulate in accordance with the importance of potential failures (of components, HVAC, ventilation, ...) are used in the simulations.

On one hand, HFE can provide insights and evidence into ways to estimate and keep human errors to a minimum with attention to procedures or manipulations / actions that are important for the safety of the plant (training, international experience, ).

On the other hand, in case of heatwaves that are unexpected or unforeseen in amplitude and/or duration by the design, the safety concept is adapted to the operators and information is exposed according to their capabilities to deal with the uncomfortable situation and take the right decisions. The estimation of human performance is fed back to PSA.

EIIC_3: DSA, PSA and HFE analyses have all been utilized in the case study. The DSA, PSA and HFE analyses are described and connected through the accident progression, described in the SEP, and results provided by one analysis, are in many cases essential inputs to perform the other analyses. The main interaction point between DSA and PSA disciplines are the protection relay configuration and the related reliability analyses, in which the safe configuration of the systems is first decided by DSA and then verified by PSA. In the case, the requirements of the HFE focuses mainly on the HSI of the startup of EDG and its connection to safety busbar, which happens later in the safety engineering process than the system configuration and reliability analyses, this leads to HFE analyses to be rather separated from the rest of the analyses.

Interactions are also found within disciplines, for example, within PSA. First, an initiating event and hazard analysis is performed to create a frequency estimate for the lightning events. Next, the selectivity protection planning is analysed to support the reliability estimation of systems’ protection. Finally, the internal events PSA model is used to generate plant level risk estimates for lightning induced events.

The interconnections between analyses have been identified in the safety engineering process, which tries to manage them. In general, it is seen more that DSA feeds information to PSA, and not the other way around.

Comparison: The case-studies have some similarities:
- Accident progression or the definition of the scenarios to simulate by DSA are derived from PSA analysis
- Mainly the results from DSA are fed to the PSA analysis
- HFE communicates results to DSA and PSA, but is less connected to them and is more at the end of the total analysis

Compare how the HFE is connected to safety analyses methods DSA/PSA. Is the basis of the connection only HRA-activities or are there any other relevant areas of connection:

EIIC_1: HRA is one part of the interaction with the two other disciplines (especially PSA), but this point was not underlined in the case-study. The case study also mentions the capabilities of creation and resilience in unexpected situations. In that case the connection with DSA can be linked to the possibilities of bringing in
for example mobile equipment or on the flexibility of reconfigurations (open doors to cooler parts of the
installation, etc...).

EIIC_3: In the case study, HFE is considered for the assessment of required manual actions of the
operators. Manual actions are needed when the plant faces an SBO and the EDGs are needed. Human
actions in the overvoltage situation outside the starting of EDGs have not been assessed. This creates gaps
between HFE and DSA/PSA analyses. The focus of DSA/PSA analyses has been in the reliability
assessment of I&C configuration and, for example, no specific HRA has been considered for the case.

Comparison: Both case-studies treat the usability of the system from a human factor point of view (workload,
situation awareness, physiological capabilities, etc.). Thus, HRA was not described as the most relevant
activity for the cases. When regarding the connection between the disciplines, DSA and PSA provide inputs
for HFE, but less information goes the other way around. HFE seems to be capable of dealing with the data
coming from DSA/PSA.

Compare how the interactions have been made for analyses of DBA and for the analyses of DEC respectively.
Describe commonalities and differences on how the interconnections and flow of information have been
ensured for DBA and DEC external events:

EIIC_1: No distinction has been made in the case-study between the interactions in DBA analyses and in DEC
analyses. Although the analyses may need different experts and another level of detail. Diversification and
independence of DiD level may need different studies and persons. No difference in the type of interactions
came on the surface.

EIIC_3: No interaction was described in the case studies concerning analysis of DBA and DEC external
hazards, respectively

Comparison: Both case-studies do not make a distinction between DBA and DEC for the information
exchange between HFE/DSA/PSA.

Identify strengths of different ways of interconnecting the safety analyses and also identify possible alternative
interconnections and information exchange that could be beneficial to apply:

EIIC_1: Many interactions today are based on hypotheses and boundary conditions. This simplifies the
information exchange between disciplines and allows specialists from each domain to concentrate on his/her
core discipline. These interactions are chosen to be conservative, which enhances safety.

EIIC_3: The main idea has been to describe the accident scenario as a cascading process, which also defines
the interconnections between safety analyses. This illustrates, for example, the flow information between
safety analyses clearly and the significance of different analyses in the assessment and preventing the
accident progression. However, as a hindsight, if the accident progression is uncertain and there are several
possible ways it can progress, the presumption of cascading process is not necessarily applicable.

Comparison: For both cases it is important to identify the role and significance of each safety analysis. This
helps to recognise their interconnections and how they support each other. The safety analyses show that
the requirements are met for each discipline and that their methods / tools are well defined, as well as their
role and responsibilities. Nevertheless, while continuous improvements are made to the internal methods
and tools, studies on the optimization of efficient information exchange should be looked at (which is fully in
the scope of BESEP).

Identify good practice of interconnections and flow of information between DSA, PSA and HFE which can be
used in the generalised case study to be developed in T3.5:

For the cases studies, interconnections between safety analyses are relatively simple and limited. This is
mainly due to the boundary conditions and hypotheses done for the accident scenarios and the related
analyses. Interconnections and flow of information are beneficial as long as they support the main goal of
verifying the safety requirements without bringing in unnecessary complexity. Graded approach can be used
to limit this complexity. It is therefore beneficial to identify the role and significance of each safety analysis
within the case under study.
Specific points of difficulties that need particular interest from other disciplines are nowadays treated in more multi-disciplinary way. It seems efficient to keep the interactions simple (also for in-depth analyses) and concentrate only on specific multi-disciplinary topics if necessary.
Table F.3. Interactions between DSA, PSA and HFE.

<table>
<thead>
<tr>
<th>Interactions between DSA, PSA and HFE</th>
<th>EIIC_1</th>
<th>EIIC_3</th>
<th>Conclusions</th>
</tr>
</thead>
<tbody>
<tr>
<td>PSA delivers probabilities and scenarios to be simulated by deterministic tools, which in return calculate or simulate temperatures of components and rooms. These results are put in regard to their limits and used to assess the importance of the robustness of components. The rank of importance of components resulting from PSA studies can prioritise DSA studies. Estimation of the probability of human errors due to an uncomfortable environment are fed into PSA studies. HRE studies provide insights to human errors and resilience, and gives inputs to DSA in order to continuously improve the systems design.</td>
<td>PSA delivers probabilities and scenarios to be simulated by deterministic tools, which in return calculate or simulate temperatures of components and rooms. These results are put in regard to their limits and used to assess the importance of the robustness of components. The rank of importance of components resulting from PSA studies can prioritise DSA studies. Estimation of the probability of human errors due to an uncomfortable environment are fed into PSA studies. HRE studies provide insights to human errors and resilience, and gives inputs to DSA in order to continuously improve the systems design. DSA, PSA and HFE analyses have all been utilized in the case study and described through the accident scenario, which links them together. The main interaction point is the protection relay configuration and reliability analyses, where the configuration is decided by DSA and verified by PSA. HFE focuses mainly on the startup of EDG and its connection to safety busbar.</td>
<td>DSA, PSA and HFE analyses have all been utilized in the case study and described through the accident scenario, which links them together. The main interaction point is the protection relay configuration and reliability analyses, where the configuration is decided by DSA and verified by PSA. HFE focuses mainly on the startup of EDG and its connection to safety busbar.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Similarities:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Accident progression / scenarios to simulate are inputs for DSA, but are derived from PSA analysis.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>DSA results feed PSA.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>HFE communicates results to DSA and PSA, but is more situated at the end</td>
</tr>
<tr>
<td>Evaluation of Adequacy</td>
<td>Each discipline has its own proven tools. No measurement was available to determine if the interaction between PSA, DSA and HFE is enough</td>
<td>Role and significance of analyses is described for the scenario; however the general adequacy of interconnections has not be evaluated. HFE is separated from the DSA/PSA analyses as the focus on the case is different.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Interconnections between safety analyses are relatively simple and limited, but seen sufficient for cases under study.</td>
</tr>
<tr>
<td>Proposals for Improvement</td>
<td>Tacit knowledge coming from HRE could be made more explicit and shared with the other disciplines. Dynamic interaction could be improved by a central information database or digital platform, containing input data, models of different abstraction levels and results from all disciplines that are involved in the safety analysis (in a readable / importable format to all). Without the need to have a profound knowledge of the other disciplines.</td>
<td>Overvoltage analyses on the performance and behaviour of the protection relays. Evaluation of other potential selectivity protection measures. Extending HFE analyses to cover further human actions relevant to the scenario, would improve it’s interconnections to other disciplines.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>For both cases it is important to identify the role and significance of each safety analysis. This helps to recognise their interconnections and how they support each other.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Define a way to measure the interaction between the disciplines.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Define a method to assess the level of interaction.</td>
</tr>
</tbody>
</table>

Evaluation of Adequacy:

Each discipline has its own proven tools. No measurement was available to determine if the interaction between PSA, DSA and HFE is enough. Role and significance of analyses is described for the scenario; however the general adequacy of interconnections has not been evaluated. HFE is separated from the DSA/PSA analyses as the focus on the case is different. Interconnections between safety analyses are relatively simple and limited, but seen sufficient for cases under study.

Proposals for Improvement:

Tacit knowledge coming from HRE could be made more explicit and shared with the other disciplines. Dynamic interaction could be improved by a central information database or digital platform, containing input data, models of different abstraction levels and results from all disciplines that are involved in the safety analysis (in a readable / importable format to all). Without the need to have a profound knowledge of the other disciplines. Overvoltage analyses on the performance and behaviour of the protection relays. Evaluation of other potential selectivity protection measures. Extending HFE analyses to cover further human actions relevant to the scenario, would improve it’s interconnections to other disciplines. For both cases it is important to identify the role and significance of each safety analysis. This helps to recognise their interconnections and how they support each other. Define a way to measure the interaction between the disciplines. Define a method to assess the level of interaction.
<table>
<thead>
<tr>
<th>EIIC_1</th>
<th>EIIC_3</th>
<th>Conclusions</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Optimize the interaction level of PSA/DSA/HFE.</td>
</tr>
</tbody>
</table>
F.5 Overall safety engineering process

Compare the overall SEP approaches and its steps between the case studies. How different are the approaches and which steps are common and which steps are unique? Explain the underlying causes of the differences, if feasible.

First, it should be noted that either of the cases in this group do not specifically describe or evaluate an existing plant, case study or SEP, but are rather prospective and exemplary. Thus, the cases have quite a different approaches for describing the safety engineering processes, which is mainly based on the interest of the respective companies. As so, comparing of the SEPs was difficult.

The SEP of the other case focuses more on fulfilling the topical requirements with a higher-level claim-argument-evidence (CAE) approach and showing how the topical requirements are in each case broken down in to claim and sub claims, and how the possible evidence could be produced with exemplary analyses. The focus is placed on proof of concept and not on a complete in-depth implementation with all the details or materials, etc. The intended CAE structure is meant to be supported by advanced deterministic and probabilistic modelling and simulations, to justify that the set of design and operational measures taken ensure that the risk of unacceptable conditions induced by external event, through the I&C, remains acceptable. So, the overall SEP was, uniquely within the cases, structured around the CAE method, where:

- Safety requirements are represented by claims.
- Supporting safety analysis (generally numerical results, but other results can be included such as expert judgement) are the evidence.
- The glue between the safety requirements and evidence corresponds to the arguments that support the safety analysis.

The method has been mostly applied to the two upper levels, but it is said to be sufficiently generic that it can be used at all levels (like matryoshka dolls). However, it doesn’t introduce or specifically explain any specific steps or workflow or V-model for the use of method in any SEP level.

Quite contrary, in the other case, the focus on SEP is more about describing the process on all three levels, giving high-level steps, flow of information and specific analyses needed for the assessment of the related safety margins and the requirements topics. The levels of SEP, quite specific to this case study, are described from bottom-up, starting from level 3.

- Level 3 covers the risk estimation from lightning to the electrical systems with the help of internal events PSA model.
- The level 2 safety engineering process focuses on the case-specific safety analyses.
- Level 1 attempts to demonstrate how the safety engineering activities of this case study are connected to the overall safety engineering process.

This is also unique approach within the cases of the group. However, this case doesn’t bring up the way the requirements will be argued to be fulfilled. It only roughly described the potential analyses to bring up the needed evidence.

Compare the flow of information in the SEPs of the case studies. Which flow patterns (interrelationships) are common and which are unique? Explain the underlying causes of the differences, if feasible.

On Level 1, neither of the case studies explicitly describe the flow of information between the main components of SEP (requirements, design and analyses), they are both staying on quite high and vague level on this topic. In fact, a similar trend is followed also in the other two levels, this might be because both cases are more of a methodological approach rather than describing a realistic safety margin assessment case.

However, even if not explicitly, they both try link the three main components on Level 1 on some level. The flow of information on the Level 1 SEP, in one of the cases, is described in the Figure F.2. It shows the relation of high-level concepts between the main components of SEP and illustrates the flow of information between them. On the other hand, the similar Level 1 information for the other case is shown in Figure F.3.
As can be seen from the figures, the cases have approached the Level 1 descriptions differently and don’t really share any flow patterns as such. The methods would seem to complement each other quite nicely. Other one explains the main SEP cycle and relations, while the other focuses on linking the requirements and analyses on relevant architecture within the V-model. However, neither really tie in the CAE approach to the information flow diagrams of Level 1 (or Level 2 as shown below), the flow of information and steps within the CAE approach has been described (evidence supports the arguments which in its turn supports the (top) claim).
Both cases also explain their interpretation of the Level 2 SEP (the interconnection between safety analyses), as shown in Figure F.4 and Figure F.5. Even though they are pictured differently (and thus harder to compare), they share similar flows. For example, deterministic analyses mostly feeding simulation and experimental results towards probabilistic ones.

**Figure F.4. Level 2 SEP.**

![Diagram of Level 2 SEP showing the interconnection between safety analyses and the cyclic flow of information.]

**Figure F.5. Level 2 SEP.**

On the other case, the DSA, PSA and HFE analyses are connected through the accident progression, and results provided by one analysis, are in many cases essential inputs to perform the other analyses, while on the other case, the cyclic flow of information is pictured. Again, these two approaches are complementing each other, as the accident progression needs to be iterated whenever there is change in any of main components of SEP (requirements, design and analysis).

Reveal and evaluate strengths and weaknesses, and challenges and successes of the different SEP approaches. Provide justifications for the use of the chosen approach. Incorporate findings and conclusions based on the “Further Lessons Learned” section in the self-evaluation sheets.
The strength of CAE approach to SEP is that complex chains of reasoning are made explicit, it is inspired by mathematical demonstrations, where a theorem (claim) is progressively broken down into lemmas (sub claims). And where each reasoning step is explicit so that it can be understood, verified and if necessary, challenged. The CAE method is applicable throughout the engineering process, from the beginning to the end of the engineering cycle, the expression and explanation of solution strategies and principles are needed, even in an early stage when details of the solution are not finalized. One weakness is that the language and tool support the CAE is still in progress. Also the use of resources should be made more explicit and to visualise the importance of each element in order to have a better view of the graded approach.

The other SEP approach helps to show that safety analyses focus on the essential part of plant design and important safety system relevant to the accident scenario. The initiating event has been identified and the accident sequence has been clearly specified. The technical disciplines relevant for the case study and the hazard has been identified from the overall safety engineering process presented in the V-model. Safety analyses and their outcomes were identified in the safety engineering process, which helps to produce the needed evidence for the requirement verification. As a weakness, as the case stays only at architecture, or some cases in system level, the further elaboration of requirements down to system and component specific level has not been made. Interactions and interfaces to other, possibly dependent, plant systems have not been properly considered. For the case study, comprehensive PSA model has not been created. The risk assessment is purely case specific, focusing only on a single failure combination, i.e., the failure relay configuration. As the requirements had not been specified while conducting the safety analyses, the formal verification of requirements could only be performed after the analyses have been made. There was no possibility to do detailed analyses on areas of specific interest.

In both cases, a more detailed information on system and component level analyses would improve SEP description and make it more accurate.
Table F.4. Characterization of the Overall Safety Engineering Process:

<table>
<thead>
<tr>
<th>Overall approach and steps of the SEP</th>
<th>EIIC_1</th>
<th>EIIC_3</th>
<th>Conclusions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application of the Claim-Argument-</td>
<td></td>
<td></td>
<td>Different approach to describing SEP:</td>
</tr>
<tr>
<td>Evidence method.</td>
<td></td>
<td></td>
<td>CAE approach and more scenario-based</td>
</tr>
<tr>
<td>Mostly applied to the two upper</td>
<td></td>
<td></td>
<td>Can be complementary to each other</td>
</tr>
<tr>
<td>levels, but the method is</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>sufficiently generic that it can</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>be used at all levels (like</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>matryoshka dolls).</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEP is described and characterized</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>in three levels. Analysis steps and</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>interactions are given on a case</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>specific level.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Different approach to describing</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEP: CAE approach and more scenario-</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>based</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Can be complementary to each other</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| Interrelationship among the Steps    | Evidence supports the arguments which in        | Step structure has been described, accident  |
|                                      | its turn supports the (top) claim, CAE can      | progression in the hazard scenario and the   |
|                                      | be applied to all Levels of SEP                 | related analyses                             |
|                                      |                                                  | Steps are different, or not really            |
|                                      |                                                  | explicitly specified;                         |
|                                      |                                                  | Interrelations exists in both, but have       |
|                                      |                                                  | been described in different manner            |

<p>| Strength of the SEP                  | The CAE method makes it possible to             | Safety analyses focus on the essential part  |
|                                      | explicit complex chains of reasoning (like      | of plant design and important safety system. |
|                                      | in mathematical proofs).                        | The initiating event has been identified and  |
|                                      | Human judgement can be included into            | the accident sequence has been specified.    |
|                                      | this method.                                    | Safety analyses and their outcomes are       |
|                                      | The CAE method is sufficiently universal that   | identified in the safety engineering process.|
|                                      | it can be used by different disciplines.        | The technical disciplines relevant for the    |
|                                      | Method can be used at different levels of       | case study are identified from the overall    |
|                                      | abstraction.                                    | safety engineering process presented in the    |
|                                      |                                                  | V-model.                                     |
|                                      |                                                  | Strengths lie in different areas             |
|                                      |                                                  | In one case CAE method strength is in         |
|                                      |                                                  | supporting the reasoning behind               |
|                                      |                                                  | fulfilment of requirements, as well as        |
|                                      |                                                  | good generalization to different levels of    |
|                                      |                                                  | abstraction                                  |
|                                      |                                                  | Other cases strength is describing the        |
|                                      |                                                  | specific analyses, their steps and            |
|                                      |                                                  | interconnections, and finally linking         |
|                                      |                                                  | these to the plant design process, which is   |
|                                      |                                                  | based on V-model approach                    |</p>
<table>
<thead>
<tr>
<th><strong>Weaknesses of the SEP</strong></th>
<th><strong>EIIC_1</strong></th>
<th><strong>EIIC_3</strong></th>
<th><strong>Conclusions</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>The supporting language is still in progress.</td>
<td>The supporting language is still in progress.</td>
<td>Further elaboration of requirements down to system and component specific level has not been made.</td>
<td>CAE approach is lacking further language support</td>
</tr>
<tr>
<td>It doesn't perform the safety analyses automatically, which needs to be done by humans.</td>
<td>It doesn't perform the safety analyses automatically, which needs to be done by humans.</td>
<td>Interactions and interfaces to other, possibly dependent, plant systems not been properly considered.</td>
<td>SEP not specified down to system and component level yet</td>
</tr>
<tr>
<td>Further elaboration of requirements down to system and component specific level has not been made.</td>
<td>Further elaboration of requirements down to system and component specific level has not been made.</td>
<td>Interactions and interfaces to other, possibly dependent, plant systems not been properly considered.</td>
<td>Neither really specify the process descriptions and/or inputs and outputs required at each step</td>
</tr>
<tr>
<td>Interactions and interfaces to other, possibly dependent, plant systems not been properly considered.</td>
<td>Interactions and interfaces to other, possibly dependent, plant systems not been properly considered.</td>
<td>Interactions and interfaces to other, possibly dependent, plant systems not been properly considered.</td>
<td>Resources are not specified either</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Proposals for Improvement</strong></th>
<th><strong>EIIC_1</strong></th>
<th><strong>EIIC_3</strong></th>
<th><strong>Conclusions</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Improvement of the supporting language for the CAE method</td>
<td>Improvement of the supporting language for the CAE method</td>
<td>With the help of a more comprehensive PSA model versatile failure combination could be recognized.</td>
<td>Process descriptions according to D2.3</td>
</tr>
<tr>
<td>Improvement to visualise the importance of each element of the evidence to fulfil the arguments</td>
<td>Improvement to visualise the importance of each element of the evidence to fulfil the arguments</td>
<td>Detailed system and component level analyses would improve the assessment and make it more accurate.</td>
<td>Further visualizing the importance of CAE elements</td>
</tr>
<tr>
<td>With the help of a more comprehensive PSA model versatile failure combination could be recognized.</td>
<td>With the help of a more comprehensive PSA model versatile failure combination could be recognized.</td>
<td>Detailed system and component level analyses would improve the assessment and make it more accurate.</td>
<td>Further detailing the comprehensive PSA model as part of the SEP</td>
</tr>
<tr>
<td>Detailed system and component level analyses would improve the assessment and make it more accurate.</td>
<td>Detailed system and component level analyses would improve the assessment and make it more accurate.</td>
<td>Detailed system and component level analyses would improve the assessment and make it more accurate.</td>
<td>Inclusion of detailed component and system level analysis in the assessment</td>
</tr>
</tbody>
</table>
F.6 Key success factors for an efficient and integrated SEP

Key Success Factors

D2.3 identifies Key aspects for an efficient and integrated safety engineering process (SEP). Below, the case studies are reflected to some of these identified key aspects.

Key aspect 1) “Connecting together the main elements of SEP: safety requirements, safety analyses and plant design of an efficient and integrated safety engineering process”; and Key aspect 2) “Safety analyses (probabilistic, deterministic and human factor engineering) providing feedback and information to the other analyses and to the overall safety design”.

As stated in the previous chapter, the case studies have quite a different approaches for describing the SEP. The first case study concentrates more on fulfilling the topical requirements with a higher-level claim-argument-evidence (CAE) approach, and how the possible evidence could be produced with exemplary analyses. The second case study divides the SEP to three levels describing the specific analyses, their steps and interconnections, and finally linking these to the plant design process, which is based on V model approach. The first SEP is strong in connecting together the main elements of SEP, and explicitly elaborating the requirements and defining arguments for the requirements. The second SEP is strong in providing feedback, or i.e. evidence, and describing the flow of information between the different analyses.

Key aspect 4) “Comprehensive and documented set of safety engineering processes to ensure that the design meets all the safety requirements throughout the lifetime of the plant”.

The CAE approach ensures the formal documentation and justification of safety requirements, which can be efficiently updated when the requirements are revised. The three level integrated SEP makes it easier to implement SEP for a specific case under study and with the three level approach it is easier to identify the right improvement areas for SEP if there is a need to modify the SEP during the lifetime of the plant.

Key aspect 7) “Support the integration of safety analysis methods to obtain more accurate estimates and to save resources”; Key aspect 8) “Help to reach common understanding on the importance of different factors influencing safety and to apply graded approach, i.e. perform more detailed analysis for more important factors”; and Key aspect 9) “Use failure analyses systematically and comprehensively”.

With the CAE approach the main focus is on the fulfilment and elaboration of the requirements. How to provide the arguments and evidence is not defined in detail. With the three level integrated approach, the roles of different safety analyses are described in more detail. Together these two approaches can enhance the SEP so that the safety analysis support each other as well as possible and that they are clearly targeted to the justification of the requirements.

With closer interconnection of requirements, arguments and evidence, it is easier to identify possible shortcomings. The three level representation gives good insight to the failure analysis and their objective in the overall picture. The identified shortcomings can be removed by performing additional or more detailed failure analysis. The combination of SEP approaches of the two case studies can help reach common understanding for the safety justifications and the application of grade approach for failure analysis more efficiently.

Generalized SEP

A suggestion for the generalised SEP of EIIC group is presented in Figure F.6. The generalised SEP is a merger of two SEP methods applied in the case studies. The main structure of the generalised SEP is built on the three level approach that can be found in the project proposal and is applied by the second case study. It is reinforced with the CAE approach from the first case study. The initial impression is that the approaches complement each other and they can be used jointly without significant overlap. The practical implementation of generalised SEP depends on the actual generalised case study, which is to be decided later.
Figure F.6. Suggestion for generalized SEP.
This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 945138.