Grouping and Initial Evaluation of Case Studies for Integrated Safety Assessment in the European BESEP Project

Attila Bareith[1], Tamas Siklossy[1], Pavol Hlavac[2], Zoltan Kovacs[2]

[1]NUBIKI Nuclear Safety Research Institute Ltd., Budapest, Hungary
[2]RELKO Ltd. Engineering and Consulting Services, Bratislava, Slovakia

ABSTRACT

A Benchmark Exercise on Safety Engineering Practices is conducted with participants from several countries of the European Union to underpin and accelerate the implementation of improved and better integrated safety engineering methods. These methods support both the assessment and evaluation of safety margins of nuclear power plants for design basis as well as design basis-exceeding external hazards, and the verification of fulfilling stringent safety requirements for the defenses against external hazards. The aim of the benchmark exercise is to provide guidance on how to enhance the flow of information between different safety analysis methods and how to adapt a graded approach for the deployment of sophisticated safety analysis methods in different disciplines including deterministic safety analysis, probabilistic safety assessment and human factors engineering. The first technical tasks in this joint effort were concerned with the definition of a benchmark baseline on safety requirements important to licensing nuclear power plant upgrades and new builds. Also, the key features of an efficient safety engineering process were outlined and recommendations were developed for the assessment of safety margins. More recent tasks in the project focused on the development and evaluation of case studies on the safety engineering process from the participating organizations for the purposes of comparative assessments and benchmarking to help refine the definition of a good safety engineering process and demonstrate this process by specific examples. The paper summarizes the objectives, the main tasks and the expected results of the project followed by a brief description of case study development and evaluation.

Keywords: safety requirements, safety margins, safety analysis, human factors engineering, safety engineering process

1. INTRODUCTION

In the post-Fukushima era, there is a Benchmark Exercise on Safety Engineering Practices (BESEP) in place with participants from six countries of the European Union (EU) to underpin and accelerate the implementation of improved and better integrated safety engineering methods. VTT Technical Research Centre of Finland Ltd. is the project coordinator. The other project partners are Électricité de France (EDF), France; Fortum Corporation, Finland; NUBIKI Nuclear Safety Research Institute Ltd., Hungary; RELKO spol. s r.o., Slovakia; Risk Pilot AB, Sweden; and ÚJV Řež a.s., Czech Republic. The project is funded by the Horizon 2020 research and innovation funding programme of the EU.

First of all, the project is expected to support the assessment and evaluation of safety margins of nuclear power plants for design basis as well as design basis-exceeding external hazards, and the verification of fulfilling the increasingly stringent safety requirements for the defenses of nuclear power plants (NPPs) against external hazards. Further, it is envisioned that the cooperative efforts made in the project will lead

to recommendations on safety engineering practices that better integrate different disciplines in safety analysis, including deterministic safety analysis (DSA) probabilistic safety assessment (PSA) and human factors engineering (HFE), when fulfilling the relevant safety requirements and assessing plant safety. Case studies are collected in the project based mostly on existing safety analyses for NPPs operating in the EU. Each case study includes:

- a description of safety requirements addressed in the study from among a set of requirements specified as a requirement baseline in the project;
- the safety analyses, i.e., DSA, PSA and HFE evaluations, performed to support the fulfilment of the relevant safety requirements;
- a top-level characterization of the associated safety engineering process (SEP) from the perspectives of the project.

The case studies are subject to successive comparative evaluations and refinements in pursuit of reaching consensus in what the project partners consider an improved integrated safety engineering process that can be recommended for use to better serve the purposes of nuclear safety authorities and the industry as well. This process of learning and improvement by means of structured and systematic evaluations of basically existing case studies is understood as benchmarking in the project, as opposed to performing a benchmark in its classical sense using pre-set, uniform initial and boundary conditions when solving a common problem by different analysis methods and/or tools. Comparisons of the case studies with the advisable safety engineering process are another dimension of benchmarking in the project After providing a short summary of the project in terms of its objectives, tasks and expected results, this paper focuses on the efforts made to develop case studies and perform their initial evaluation. The conclusions that could be drawn from these efforts are also listed with implications to further technical tasks of the project.

2. OVERVIEW OF THE BESEP PROJECT

2.1. Objectives

The overall objective of BESEP is to support the assessment and evaluation of safety margins of NPPs by recommending good practices for safety requirements verification against external hazards. To fulfill this objective, the benchmark exercise is to provide guidance on how to enhance the flow of information between different safety analysis methods and how to adapt a graded approach for the deployment of sophisticated safety analysis disciplines including DSA, PSA and HFE.

2.2. Tasks and Schedule

The BESEP project includes six work packages (WPs):

- WP1: Project management and coordination;
- WP2: Benchmark baseline;
- WP3: Case studies;
- WP4: Result evaluation;
- WP5: Dissemination and communication;
- WP6: Training and education.

The project time span is 42 months starting 1st September 2020. From among the technical tasks, work in WP2 and WP3 has been completed up to now, while work is ongoing in the rest of the work packages (WP4 through WP6). The project is expected to conclude by the end of February 2024 according to the current schedule. The technical tasks in WP2 were concerned with the definition of a benchmark baseline on safety requirements important to licensing nuclear power plant upgrades and new builds [1], [2]. The

benchmark baseline is made up of 82 specific safety requirements, called BESEP requirements. These requirements are broken down into 24 areas, designated as requirement topics, in relation to DSA, PSA, HFE and safety engineering (SE) practices. Also, the key features of an efficient safety engineering process were outlined and recommendations were developed for the assessment of safety margins in WP2 [3]. More recent tasks in WP3 focused on the development and evaluation of case studies on the safety engineering process from the participating organizations for the purposes of comparative assessments and benchmarking to help refine the definition of a good safety engineering process and demonstrate this process by specific examples. Definition and grouping as well as an initial evaluation of the case studies are described below in Sections 3 and 4, respectively. Reference to achievements in further tasks within WP3 is made in Section 5, i.e., in the conclusions of this paper. Use has been made of an extensive list of references during the conduct of the various project tasks. It is not practicable to include all these references in this paper. Therefore, only the most important and relevant project reports are cited.

2.3. Expected Results

The key results expected from the project include the following:

- a safety engineering methodology for the management of requirements and risks to ensure sufficient safety margins in NPPs against external hazards;
- guidance on integration of methods and tools for functional analysis, analysis of compliance with codes and standards, and probabilistic safety assessment;
- a graded approach to balance the plant's safety design against different external hazards;
- a procedure for establishing recommendations for improving emergency response;
- integration of PSA and human reliability analysis (HRA) with HFE.

These results will be manifested in project deliverables including technical reports, tutorials, workshop proceedings, a project website and publications. Most of the project deliverables will be made publicly available. Almost all the technical reports developed so far within WP2 and WP3 are already accessible at the project website.

3. CASE STUDY DEVELOPMENT

3.1. Definition of Case Studies

Case study requirements were defined in the first step of this task. The output from WP2 formed the technical basis of specifying these requirements including, in particular, the BESEP requirements [1], [2] and the envisioned features of a good safety engineering process [3]. A template was prepared to give guidance on the required contents and format of initial, concise case study descriptions. Two sample case study descriptions were elaborated to demonstrate how the case study requirements were meant to be fulfilled. To help develop an extended pool of case studies, 30 concise case descriptions were provided by the partners in total, in accordance with the requirements of the template. Each individual concise case study description was evaluated to support the selection of cases for detailed elaboration. By considering the findings of this evaluation and taking the needs of putting the case studies into characteristic and distinctive groups (see Section 4), a short list of case studies was composed for the purposes of detailed elaboration and self-evaluation by the project partners.

A template was also prepared to foster a coherent description of the different case studies. The detailed case study descriptions had to include all the information considered necessary for comparative evaluation to enable efficient benchmarking in WP3 and WP4. 12 detailed case study descriptions were provided in total by fulfilling the requirements of the template [4]. Since these case study descriptions are extensive, only the main features of a selected case study are given in Table I followed by a condensed description. A listing of the 12 case studies is provided in Section 4 together with their grouping.

Table I. Summary of a case study

Title	Protection of the reactor hall from the effects of extreme snow
Relevant external hazard(s)	Natural non-seismic hazard / extreme weather conditions / extreme snow
Plant systems, structures and components (SSCs) involved	Complete building structure of the reactor hall Equipment and tools for snow removal
Key safety requirement topics	Physical separation and structural integrity (DSA) Support to developing abnormal and emergency operating procedures and severe accident management guidelines (PSA) Confidence in provision for defenses against the occurrence of cliff edge effects (PSA) Guidance selection, decision making, intelligent use of guidance (HFE) Safety design and requirement management for external hazards (SE)
Safety analysis involved and support to SEP	Structural strength and structural reliability analyses (DSA) Fragility analysis for SSCs (PSA) Snow PSA (PSA) Analysis of the snow removal strategy and corresponding emergency operating procedures (HFE) Availability and adequacy of equipment, tools, and administrative arrangements and controls for snow removal (SEP)
Administrative and/or technical measures implemented	Strengthening some structural components Improvements to the strategy for snow removal

Based on the results of an upgraded hazard assessment for meteorological hazards, it was found in a recent Periodic Safety Review (PSR) of the plant as well as in its lifetime extension efforts that plant safety might be challenged for design basis loads, and the safety margins beyond design basis loads may not be sufficient. Thus, improved defenses had to be ensured against the effects of meteorological hazards through establishing and maintaining sufficient safety margins for design basis loads and beyond and, also, to reassuringly exclude potential cliff-edge effects due to such loads. The case study covers the description and evaluation of the applied safety engineering process aimed at justifying the protection of the reactor hall, as a building structure of a nuclear power plant, against the effects of extreme snow.

Use was made of structural strength analysis to assess whether the reactor hall can withstand the design basis snow load at high confidence level or not. Some plant modifications were found necessary to provide appropriate protection against the design basis loads. The proposed modifications included strengthening selected structural components. Subsequently, structural reinforcement was made in accordance with the proposal. After implementing the proposed plant modifications, fragility analysis was performed to enable a quantitative assessment of safety margins by means of the plant PSA for extreme snow. The fragility analysis made use of structural strength as well as structural reliability analyses. PSA was applied to justify the fulfilment of probabilistic safety criteria and qualify the adequacy of reactor hall protection against snow loads at a higher, facility level.

The occurrence of snow-induced plant transients can be prevented if snow is removed from some designated plant areas, important to plant safety, in a timely manner. 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 for timely snow removal. The review led to improvements in the snow removal strategy.

3.2. Grouping of Case Studies

Key attributes were defined to enable a meaningful grouping of the case studies developed by the project partners. It was considered in the specification of the grouping attributes that the case study groups should reflect the main engineering aspects that are in the focus of the whole BESEP project. In order to achieve this goal, the safety requirement topics and the safety requirements of project focus defined in WP2 were taken into account. In addition, the needs of (i) cross-case comparison within case study groups as well as (ii) developing generalized case studies in further project tasks were also considered during grouping. Finally, the following types of case study groups were developed [5]:

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

Table II lists the definition and grouping of the 12 case studies elaborated in the project.

Table II. Case studies and case study groups

ID	Partner	Title
STIN – Structural Integrity (requirement-based case study group)		
STIN_1	RELKO	Collapse of venting stack due to high wind
STIN_2	UJV	Probabilistic analysis of aircraft crash risk for an NPP
STIN_3	VTT	Loss of heat removal of spent fuel pool due to external impact
LUHS – Loss of Ultimate Heat Sink (safety function-based case study group)		
LUHS_1	FORTUM	Loss of ultimate heat sink (frazil ice or oil spill)
LUHS_2	RELKO	Loss of service water system due to extremely low temperature
LUHS_3	RISK PILOT	Blockage of water intake building
LUHS_4	NUBIKI	Evaluation of plant vulnerabilities to riverine events
PVES – Plant Vulnerability to Extreme Snow (hazard-based case study group)		
PVES_1	RISK PILOT	Extreme snow and wind affecting diesel generators
PVES_2	NUBIKI	Protection of the reactor hall from the effects of extreme snow
PVES_3	UJV	Analysis of extreme snow risk for an NPP
EIIC – External Impact on Safety Classified I&C Systems (SSC-based case study group)		
EIIC_1	EDF	Loss of instrumentation and control due to high ambient temperature
EIIC_2	VTT	Loss of on-site power supply and control due to lightning

4. SELF-EVALUATION OF CASE STUDIES

4.1. Self-Evaluation Process

As a first step of benchmarking on the basis of the case studies, each project partner performed a self-evaluation of their case studies by the use of pre-defined evaluation requirements and an associated template designed to harmonize the self-evaluations of the different partners [6]. The self-evaluation requirements were determined by taking the overall project objectives and, in particular, the needs of further evaluations and comparisons in subsequent project tasks into consideration.

The evaluation requirements covered the following key technical aspects:

- fulfilling the relevant BESEP requirements;
- definition, assessment and evaluation of safety margins against the effects of the relevant external hazards;
- characterizing the interactions between DSA, PSA and HFE;
- characterizing the overall safety engineering process;
- identifying lessons to be learned for a meaningful benchmark.

4.2. Example of Self-Evaluation

An extract from the self-evaluation of the case study on the "Protection of the reactor hall from the effects of extreme snow" for a VVER-type NPP is presented below to illustrate the results of self-evaluation.

4.2.1. Fulfilment of safety requirements

From among the complete list of 82 BESEP requirements, the verification of 13 requirements is included in the case study in relation to the protection of the reactor hall from the effects of snow load. These requirements belong to higher level requirement topics as follows:

- Physical separation and structural integrity (DSA);
- Justification of the engineering assumptions used in analysis (DSA);
- Confidence in provision for defenses against the occurrence of cliff edge effects (PSA);
- *Support to developing abnormal and emergency operating procedures and severe accident management guidelines (PSA);*
- Guidance selection, decision making and intelligent use of guidance (HFE);
- Safety design and requirement management for external hazards (SE).

The evaluation of fulfilling a BESEP requirement belonging the requirement topic given in italic typeface above is described briefly in the rest of this section to exemplify the approach used. This BESEP requirement includes the following: "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

The key analysis steps to underpin the fulfilment of the given requirement as well as the development of proposals for safety enhancement included:

- identification of the major performance shaping factors relevant to the success of snow removal;
- review of the snow removal strategy at the plant;
- 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.

Adequacy of verification

The operating procedure that controls snow removal had been elaborated before the snow PSA was completed. Consequently, PSA could only be applied to review and to further improve the relevant operating procedure, since the strategy had originally been developed without giving explicit considerations to risk aspects. However, the risk-informed review was as a sufficiently detailed evaluation that included the elaboration of new approaches.

Proposals for improvement

Not all the proposals for safety enhancement resulted from the risk-informed review have been considered during the revision of the plant procedure that controls snow removal. The operating procedure, training as well as the available equipment for snow removal should be further improved on the basis of the analysis findings. From a broader perspective, it is seen advantageous to utilize PSA and PSA insights as an integral part of developing operating procedures 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. This finding is well supported by the fact that external hazards are found important contributors to plant risk.

4.2.2. Assessment of safety margins

Safety margins were assessed on the basis of three main disciplines considered in the project, i.e.:

- deterministic safety analysis;
- probabilistic safety analysis;
- human factors engineering.

The assessment of safety margins from the point of view of PSA is evaluated in the following description to characterize the evaluation process.

Definition

The fragility curves of the reactor hall can help develop a good understanding of the safety margin beyond the design basis snow load and enable a quantitative evaluation of this margin. The margin can be defined as (i) the conditional failure (or more precisely, the conditional success) probability for the design basis snow load, or (ii) the difference between the median capacity and the design basis snow load. Also, the risk due to snow-induced reactor hall failure characterizes the adequacy of the safety margin.

Assessment

In the analysis of plant response to extreme snow, the snow-induced loads on SSCs were characterized in a form that was appropriate for use in PSA. The probability of loss of essential safety functions and spurious actuations for different levels of snow load was described by means of fragility curves. A methodology was developed with the involvement of civil engineering experts to establish fragility curves based on the theory of structural reliability analysis. Figure 1 shows the snow fragility curves for the reactor hall derived from the use of this dedicated analysis method. These are empirical distributions, i.e., the failure probability is determined at numerous discrete points with the corresponding confidence intervals without fitting a specific distribution to these discrete points.

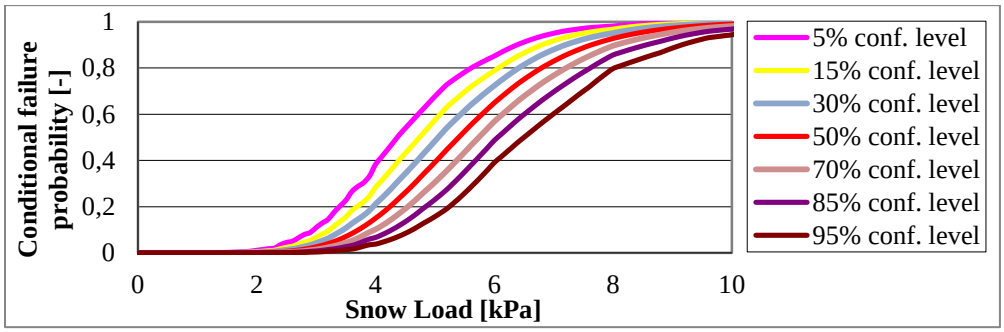

Figure 1. Snow-related fragility curves for the reactor hall

A PSA model was developed for extreme snow. The dominant core damage minimal cut sets of failures induced by extreme snow were determined followed by the calculation of core damage risk as well as quantitative uncertainty and sensitivity analyses using a dedicated computer code.

Evaluation

Based on the fragility curves of the reactor hall superstructure, the safety margin beyond the design basis snow load was determined and was found sufficient. The margin was 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: 3 kPa. The point estimate of the annual core damage probability attributable to extreme snow is $6.5 \cdot 10^{-7}$. The risk from extreme snow is moderate in comparison to the risk originated from other types of initiating events analyzed in the plant PSA. Moreover, the risk due to snow is not significant in comparison to the quantitative safety criterion, i.e., $1 \cdot 10^{-4}$/y for the total core damage frequency from all internal and external events. The failure of the reactor hall induced by snow does not play a significant role in the plant risk from snow (5% only). This finding further supports the conclusion that there are sufficient safety margins beyond the design basis snow load for the reactor hall.

Proposals for improvement

It is re-emphasized that the fragility curves can be used in support of determining the safety margins as presented in this case study. These margins can be defined as 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 may be further utilized for describing safety margins by depicting the conditional core damage probability as a function of hazard-induced loads, and deriving similar characteristics as those mentioned above for the fragility curves.

4.2.3. Interactions between DSA, PSA and HFE

The design basis load that was in the focus of the structural strength analysis (DSA) was defined by considering the results of hazard assessment. Use was made of the results of these structural strength calculations when elaborating the operating procedure (HFE) controlling snow removal to (i) determine criteria to begin snow removal from the roofs, and (2) to include a high quality snow load map in the procedure. Subsequently, plant response and fragility analysis was performed to help quantify safety margins by means of the plant PSA for extreme snow. Plant response and fragility analysis made use of structural strength and structural reliability analyses. Also, it considered the available snow removal strategy too. The plant procedure for 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 the success rate for snow removal. This review led to improvements in the snow removal strategy. Thus, HRA and HFE activities mutually supported each other.

Adequacy

DSA (i.e., structural strength analysis) needed no input from PSA or HFE; however, PSA and HFE utilized the results of DSA as input. Consequently, performing structural strength analysis first, independently of all other disciplines, seems appropriate in this case. The results of DSA were used in HFE and PSA, as far as it was seen practicable and feasible. The operating procedure for snow removal had been elaborated before performing the snow PSA. The output from HFE was considered in PSA. In addition, use was made of PSA to review and to further improve HFE (the relevant operating procedure), as the snow removal strategy had originally been developed without explicit considerations to risk.

Proposals for improvement

It is seen advantageous and advisable to utilize PSA as an integral part of developing operating procedures 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 for the operational and mitigation strategy, including the identification of the most important cornerstones, instead of making late adjustments to the available strategy elaborated previously by using deterministic considerations only. In summary, PSA and HFE should be performed simultaneously, interacting actively, so that PSA insights can be used efficiently to underpin HFE.

4.2.4. Characterization of the overall safety engineering process

Figure 2 depicts the stages and the main elements of the safety engineering process followed in the exemplary case study as well as the interconnections between the process stages and process elements. As an example of the information flows, arrow '2a' indicates that the need for the structural re-analysis of the reactor hall for snow loads was identified in the PSR for the plant. In the detailed evaluation, all these elements and the flow of information are described at length to point out the strengths of the process and identify areas that are in need of improvement to enhance the usefulness and effectiveness of the approach. Some lessons learned from this exercise are discussed in Section 4.2.5.

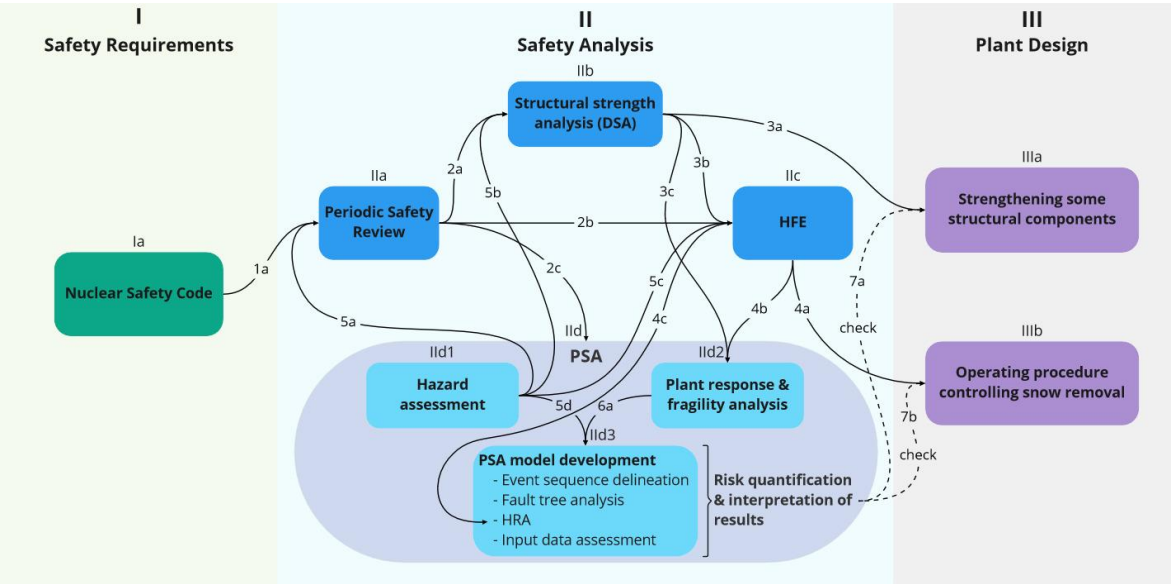

Figure 2. Scheme of the safety engineering process

4.2.5. Further lessons learned

Unlike new NPP designs, external hazards may not have been considered exhaustively in the design of operating NPPs of older designs. The interconnections and interfacing of DSA, PSA and HFE can be ensured more readily for new NPP builds in the design phase, as these disciplines are better built into the design process when justifying the fulfilment of the safety requirements related to the protection against the effects of external hazards. Indeed, this should be a core activity in safety design. In contrast, the utilities of the operating fleet with earlier designs may need to focus more on operational and maintenance issues, so the fulfilment of newly emerging requirements can become challenging to overcome. Consequently, some level of distinction may be necessary when applying the safety engineering process to the operating plants of earlier designs and to the new units, respectively.

In the country where the case study comes from, the design basis for loads from natural external hazards shall be set at $1 \cdot 10^{-4}$/y hazard frequency for operating NPPs and at $1 \cdot 10^{-5}$/y hazard frequency for new NPP builds. Also, the residual risk from natural external hazards beyond the design basis shall be assessed. The high level nuclear safety requirements yield a clear definition of design basis external hazards; however, it is seen challenging how to interpret and assess beyond design basis external hazards deterministically. It is necessary to discuss these aspects in later phases of the project.

5. CONCLUSIONS

Engineering and research organizations from six countries cooperate in the EU-funded BESEP project to underpin and accelerate the implementation of improved and better integrated safety engineering methods. These methods support the assessment and evaluation of the safety margins of NPPs for design basis as well as design basis-exceeding external hazards, and verifying the fulfilment of increasingly stringent safety requirements for the defenses against external hazards. The initial tasks in this joint effort were concerned with the definition of a benchmark baseline on safety requirements important to licensing nuclear power plant upgrades and new builds. Also, the key features of an efficient safety engineering process were outlined with recommendations for the assessment of safety margins. More recent tasks in the project focused on the development and evaluation of case studies on the safety engineering process from the participating organizations for the purposes of successive comparative assessments and benchmarking to help achieve the project goals. Altogether, 12 case studies were prepared and put into 4 distinctive case study groups. The case studies were subject to a self-evaluation by the project partners to identify strengths and weaknesses in the associated safety engineering processes and pave the road for further benchmarking and targeted evaluations in the project. Use has already been made of the self-evaluation findings to make cross-case comparisons within the case study groups and prepare a so-called generalized case study for each case study group. In the forthcoming project phases, the generalized case studies will serve as a tool to help the project partners describe what they consider a useful and efficient safety engineering process that systematically integrates different safety analysis disciplines.

ACKNOWLEDGMENTS

The work described in this paper is funded by the European Union's Horizon 2020 research and innovation programme under grant agreement No. 945138.

REFERENCES

1. "BESEP Deliverable 2.1: Results on the assignment of safety requirement topics", RELKO spol. s r.o., Slovakia., http://www.besep.eu/documents/ (2021).
2. "BESEP Deliverable 2.2: Requirement Baseline for BESEP", Fortum Power and Heat Oy, Finland, http://www.besep.eu/documents/ (2021).
3. "BESEP Deliverable 2.3: Specification on the key features of efficient and integrated safety engineering process", VTT Technical Research Centre of Finland Ltd., Finland, http://www.besep.eu/documents/ (2021).
4. "BESEP Deliverable 3.1: Definition of a Pool of Case Studies", NUBIKI Nuclear Safety Research Institute Ltd., Hungary, http://www.besep.eu/documents/ (2022).
5. "BESEP Deliverable 3.2: Description of Case Study Groups", NUBIKI Nuclear Safety Research Institute Ltd., Hungary, http://www.besep.eu/documents/ (2022).
6. "BESEP Deliverable 3.3: Results of Self-Evaluation of Case Studies against Baseline Requirements, NUBIKI Nuclear Safety Research Institute Ltd., Hungary, http://www.besep.eu/documents/ (2022).