Proceedings of the 32nd European Safety and Reliability Conference (ESREL 2022)
Edited by Maria Chiara Leva, Edoardo Patelli, Luca Podofillini, and Simon Wilson
 Published by Research Publishing, Singapore.
doi: 10.3850/978-981-18-5183-4_R18-16-434-cd

Benchmark Exercise on Nuclear Safety Engineering Practices

Essi Immonen

VTT Technical Research Centre of Finland Ltd, Finland. Email: essi.immonen@vtt.fi

Joonas Linnosmaa

VTT Technical Research Centre of Finland Ltd, Finland. Email: joonas.linnosmaa@vtt.fi

Atte Helminen

VTT Technical Research Centre of Finland Ltd, Finland. Email: atte.helminen@vtt.fi

Jarmo Alanen

VTT Technical Research Centre of Finland Ltd, Finland. Email: jarmo.alanen@vtt.fi

This paper introduces the EU research project Benchmark Exercise on Safety Engineering Practices by presenting the safety engineering concept and methodology applied in the benchmark exercise. The safety engineering concept leans heavily to the principles of model-based systems engineering, aimed to balance the interaction between management of safety requirements, plant design and system safety analyses. Initial results from the first half of the project are demonstrated using the safety engineering process of one of the project case studies as an example. The case study example is presented to concretise the kind of cases to be applied in the benchmarking for the actualization and comparison of safety engineering processes. An important part of safety engineering process is the management, allocation and elaboration of the safety requirements. The topics for the safety engineering process related requirements are explained and the benchmark specific requirements for one topic are stated. Finally, the fulfillment of requirements is evaluated for the example case study and observation on the potential strength and weaknesses of the applied safety engineering process are collected. In the second half of the project, the applied safety engineering processes of project partners will be further studied and compared to create best practices for the verification of evolving and stringent safety requirements against external hazards using efficient and integrated set of safety engineering practices and probabilistic safety assessment.

Keywords: Safety Engineering, Requirement Management, Nuclear Safety Analysis, Benchmarking

1. Introduction

Development and utilization of large and complex systems, such as nuclear power plants (NPP), require a rigorous and a well-organized approach to continue managing the plant in a safe and economically feasible manner through its long, now in many cases approaching 60 years, life span. This process is supervised by the national and international safety authorities by reviewing and assessing the fulfilment of plants' safety criteria. In the licensing process of nuclear power plant, the safety authority will review and assess the design basis of the plant. In the very core of this review is the assessment of following: The requirement specifications, the analyses substantiating the fulfilment of safety criteria, the implementation of defence-in-depth concept in the design as well as the implementation of redundancy, physical separation, functional isolation and diversity principles in the design and implementation of safety functions.

The management of the plant's safety is a continuous process of balancing the interaction between the plant's design, requirements and assessment of their fulfilment. Over time, as more knowledge of the technical and physiological limitations of the systems, materials, humans, or environment used in the plant become available, the safety criteria and the related requirements are updated to correspond with it. On the other hand, updated safety requirements can also force modifications to the plant, thus becoming another driving factor for the constant change in plant systems. The nuclear industry has extensive safety analysis methods to take care of the safety requirements, to analyze, evaluate and justify the plant safety.

However, managing this interaction between main elements of safety design (safety requirements, safety analyses and plant design) is a complicated process, which needs to be integrated across many disciplines, methods, and processes. This integration is typically

handled in the safety engineering practices. Thus, efficiency can be pursued from better safety engineering practices, which process the effect of changes in any of the main elements of safety design.

2. Benchmark exercise on nuclear safety engineering practices

Benchmark Exercise on Safety Engineering Practices (BESEP) is conducted between several European Union (EU) countries. The EU-project supports finding the most efficient safety engineering practices to support the safety margins determination and safety requirement verification helping the licensing process of nuclear power plant new builds and upgrades. The overall structure of BESEP project is illustrated in Figure 1. The work is carried out as a benchmark exercise between the project members participating in the project.

The exercise is based on relevant case studies previously performed by the participants, which are further refined during the project to support the benchmarking. The main focus of the exercise is on the comparison of failure analyses performed in the case studies, on the balancing of workload between different hazards, and on the interconnections and interactions of different analysis methods involved in the safety assessment of different external hazards. The integration of safety analysis methods is typically managed in a safety engineering process. The general safety engineering process approach is explained in Section 3 of this paper.

The benchmark exercise is conducted in two comparisons. In the first comparison, a cross-case comparison is performed for case studies belonging to the same group. The cross-case comparison focuses on the safety margins determination and safety requirements verification (shown with the vertical arrow in Figure 1).

In the second comparison, a representative generalized case study is defined for each group and a cross-group comparison is performed. The cross-group comparison focuses on the identification of benefits for increasing the level of detail in the applied safety analysis methods, e.g. the benefits of applying more detailed models or additional simulations. This helps in balancing the plant safety against different external hazards (shown with horizontal arrow in Figure 1). For the balancing, risk estimates from probabilistic safety assessment (PSA) are applied.

Together, the results of both comparisons can be used to estimate the resilience of safety margins in case of design-basis exceeding external hazards. One case study example is presented in Section 5 of this paper.

The expected key results from the benchmark exercise are:

- Best practices for the verification of evolving and stringent safety requirements against external hazards.
- Guidance on the closer connection of deterministic and probabilistic safety analysis and human factors engineering for determination and realistic quantification of safety margins.
- Guidance on creation of graded approach for deployment of more sophisticated safety analysis methods, such as upgrades of simulation tools, while maintaining the plant level risk balance originating from different external hazards.

The outcomes help streamline the licensing process of nuclear power plant new builds and upgrades. Use of best practices will give maximum output for the amount of analysis work invested to the safety margins determination and safety requirements verification. At the same time, the amount of analysis work is optimised for a specific plant design and the plant level risk is balanced against different external hazards.

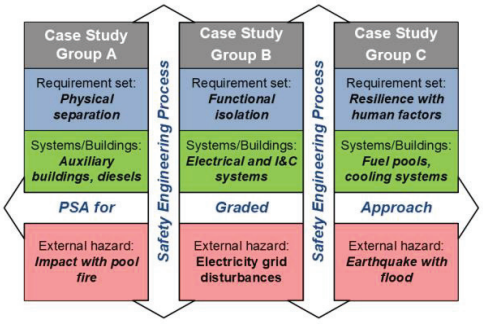

Figure 1. The overall BESEP concept.

3. Safety engineering process and plant safety analyses

In the licensing process of nuclear power plant, the safety authority will review and assess the design basis of the plant. The licensing process is endorsed by a safety engineering process that connects the main elements of safety design: safety requirements, safety analyses and plant design. In case there is a change in one of the main elements the change should be reflected in the two other elements. This is usually for the safety engineering process to take care of. The main elements of safety design are shown in Figure 2. In a steady-state situation, the three main elements are in balance, and there is consensus that based on the safety analyses the current plant design fulfils the given safety requirements.

Thus, safety engineering is an overarching continuous process starting with the very idea of building a plant and ending to the decommissioning of

the plant and the disposal of the used nuclear fuel. The focus is mainly on the safety engineering activities of the design phase with the inclusion of possible retrofit of new safety requirements to old nuclear power plants in their operation phase.

During the lifecycle of a plant, there can be various changes to the elements, for example:

- *New design* concepts and feasibility studies may give new ideas to refresh the plant design;
- International and national safety agencies may introduce *new safety goals* leading to changes in the safety requirements; or
- *Operational experience* from internal and external hazards may challenge the existing safety analyses giving initiative for more stringent safety margins.

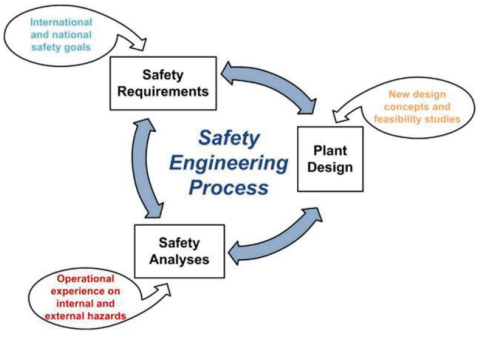

Figure 2. The main elements of safety design.

The need for change can be subtle, giving time for the safety engineering process to adjust the changes to the other main elements. Or the need for change can be abrupt, putting extra stress on the performance of the safety engineering process. There are two typical stress situations. The first is the case of sudden, unexpected operational experience, for example on an internal or external hazard. The second is the case of licensing of new nuclear power plant when the timetables create constraints to the safety engineering process. Both situations are challenging and the best way to answer to the challenge is to create robust practices to support the safety engineering process.

Traditional nuclear safety analyses can be categorized to deterministic safety analysis (DSA), probabilistic safety analysis (PSA) and human factors engineering (HFE). Each analysis provides feedback to the other analyses and to the overall safety design. How well this feedback is exploited is dependent on the information management between the different safety analyses and the main elements of safety design, see similar approach e.g. by Sun et al. (2021). The safety engineering process is, therefore, not only limited to the main elements of safety design, but it has an important role also in ensuring the information flow and utilization inside each element.

Increasingly stringent safety and licensing requirements and new design solutions necessary to match the expectations present challenges regarding how to demonstrate the compliance of sufficient safety margins. The challenge can be answered by closer connection of different safety analyses (i.e., DSA, PSA and HFE) and the failure analyses. For external events including complex failure combinations, it is vital to have an integrated safety engineering process to ensure the fluent interactions among various analyses.

For this purpose, it is important to identify the different methods involved in the different safety analysis areas and their interactions. The presumption in the benchmark exercise is that the established system and safety engineering standards and guides can provide support for deploying efficient and integrated safety engineering processes.

Safety engineering can be thought as a slice of the overall systems engineering and defined to be a systematic safety related engineering of a system through its whole life cycle, see Linnosmaa et al. (2021). From the process point-of-view, it is suggested to apply the systems engineering base standard ISO/IEC/IEEE 15288 (ISO/IEC/IEEE, 2015), which defines the systems engineering processes as suggested e.g. by IAEA (2021).

Yet another aspect of systems engineering is the system life cycle model. Life cycle model is a framework of processes and activities concerned within the life cycle that may be organized into stages, which also acts as a common reference for communication and understanding (ISO/IEC/IEEE, 2015). The life cycle model depends on the system type and system context, and the systems engineering strategy of the producing organisation. Hence ISO/IEC/IEEE 15288 does not explicitly define a life cycle model, but provides an example set of life cycle stages: concept, development, production, utilization, support, and retirement.

4. BESEP requirements

The participating countries of BESEP project have different nuclear safety requirements which has led to different safety engineering practices. Although, there are differences in the practices, the goal is the same: Showing the fulfilment of the safety requirement in the nuclear power plant design and operation.

A requirement baseline for the benchmark exercise has been created as first steps of the project. The requirement baseline is used to help the cross-case and cross-group comparisons of the case studies.

The following safety analyses and safety engineering practices are needed to ensure compliance with safety requirements for the plant:

(i). **Deterministic safety analyses (DSA)** – analyses of initiating events induced by external hazards, evaluating of plant response, plant performance or success criteria
(ii). **Probabilistic safety analyses (PSA)** – modelling of accident sequences, quantification of their risk significance
(iii). **Human factors engineering (HFE)** – scope of testing and maintenance, operator and emergency response actions on the basis of pre- and post-hazard procedures, emergency operation procedures and severe accident management guidelines.
(iv). **Safety engineering practices (SEP)** – implementation of safety requirements to existing plant design for fulfilling the defence-in-depth principle

Based on the case studies and general experience of the partners the safety requirement topics have been defined for the above-mentioned safety analyses and safety engineering practices to be applied. As an example, the topics and short descriptions on their focus in the category of safety engineering practices are listed below. The presented list is not trying to be a comprehensive representation of safety engineering practice topics. The purpose is to identify safety engineering practice topics of interest supporting the benchmark and the objectives of BESEP project.

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

For all these topics, a set of specific BESEP requirements were defined to support the upcoming benchmarking. The BESEP requirements were elaborated from the high-level requirements of IAEA and national requirements identified and selected by the project partners. As an example, the BESEP requirements on the flow of information between safety analyses topic are shown in Table 1. The collection of BESEP requirements for all topics on safety analyses and safety engineering practices create the requirement baseline for the benchmark exercise. All BESEP requirements are presented by Rein (2021).

Table 1. Requirements related to information flow between analyses.

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

The requirements of Table 1 are allocated to the example case study presented in Chapter 5 and in Chapter 6 the fulfilment of the requirements is evaluated.

5. Case study example

One of the BESEP case studies is presented here as an example to illustrate the type and scope of case studies and their involved safety analyses. The working process for defining and evaluating the case studies is following:

(i). An accident scenario initiated by an external hazard with the expected plant response is defined.
(ii). The different safety analyses (i.e. DSA, PSA and HFE) involved in the investigation of the accident scenario are identified and described to create the case study.
(iii). The BESEP requirement topics and requirements are assigned to the case study.
(iv). The results of the identified safety analyses are used to evaluate the fulfilment of the assigned BESEP requirements.

(v). The underlying safety engineering process and the activities concerning the handling of requirements and analyses in the case study are described and studied.
(vi). The evaluation results on the fulfilment of the requirements and applied safety engineering process are collected and reported for later use in the project.

The case study example describes an event where heat removal of a spent fuel pool is lost due to an external impact (e.g. airplane crash, missile, explosion or a seismic event).

A generic spent fuel pool with the residual heat removal (RHR) systems is illustrated in Figure 3. The normal RHR system has two redundant pipelines, pumps and heat exchangers. Backup cooling is available from an emergency water tank. Also an external source of water, such as a fire engine, can be connected to the backup line. The RHR system is essential for the cooling of spent fuel storage pools. If the cooling function cannot be maintained, the water boils off and the spent fuel rods become uncovered. Potential further accident escalation may be caused by collapsing structures and leakages in the pool structure, which are not in the scope of this study.

Process in Figure 4 summarises the accident progression and related safety analyses. The deterministic analyses of the case start with impact analysis and assessment of the structural integrity of the spent fuel pool and the RHR system components, by characterization of the impact load and induced vibrations. In the load characterization analysis, generally the following steps are included:

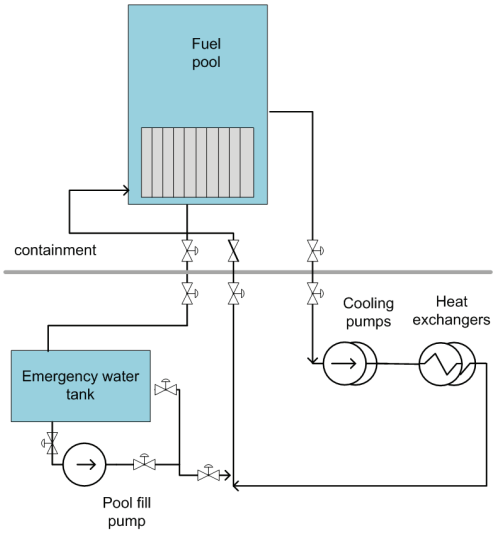

Figure 3: Illustration of the spent fuel pool and the RHR system.

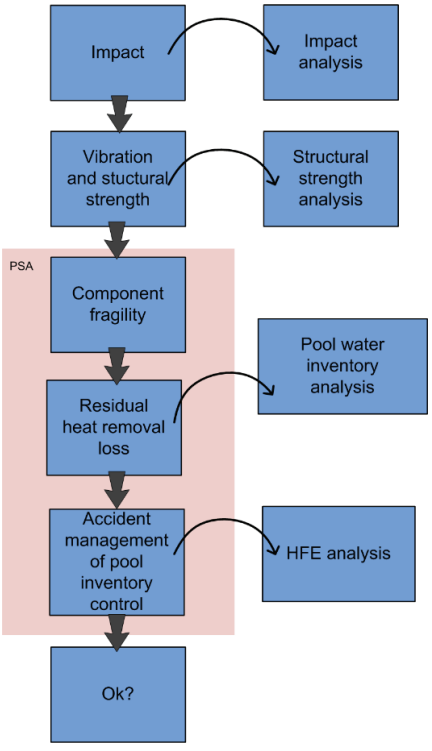

Figure 4. Case study process and safety analyses.

(i). Selection of representative impact locations,
(ii). Structural response analysis,
(iii). Assessment of performance: penetration resistance, induced vibrations,
(iv). Capacity check for the technological systems installed in the structures to demonstrate their sufficient design functionality under the induced loads.

The accident frequency for the loss of cooling accident of spent fuel pool due to external impact can be defined in a specific probabilistic safety analysis procedure called seismic PSA, which is illustrated in Figure 5. Generally, the methodology has been developed for the risk assessment of seismic events, but the same methodology is applicable for different kinds of external impacts. A probabilistic seismic hazard analysis is conducted in the first phase of seismic PSA to quantify the probabilistic site-specific ground motion parameters. In the second phase, the information of the vibrations provided by the deterministic analyses is propagated to fragility curves developed for the critical components and structures. In the final phase, the information is combined in the seismic PSA model (NEA, 2022).

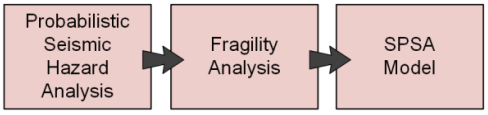

Figure 5. Seismic PSA process based on NEA (2022).

If the residual heat removal is lost due to the impact, MELCOR code analysis is needed to calculate the evolution of the pool water inventory and estimate the times when radiation protection is lost and fuel is damaged. MELCOR analyses of this kind have been performed for example by Könönen (2013). The time windows are used as input for analysis of operator actions.

The assessment is further developed by evaluation of operator responses to the accident progression and mitigation. Control room operators' ability to detect, control, and limit the accident, and to ensure that the performance of safe shutdown functions is not prevented, and the risk of radioactive release to the environment is minimized, can be analysed. Feedback from the analysis can be used to update the risk models and to support the human reliability analysis.

6. Evaluation of SEP requirements

The safety engineering practices requirements (presented in the Table 1) concerning the flow of information between analyses are evaluated for the example case presented in the Chapter 5. The evaluation is divided into three steps: i) summary of the verification process, ii) adequacy of the verification, and iii) proposals for improvement.

i) Summary of the verification process

The flow of information between safety analyses is straight-forward in this case, as the sequence of events from the impact to pool cooling management and the associated safety analyses is linear. Each analysis provides information to the other 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. The flow of information between central topics in the accident scenario has been roughly specified in the safety engineering process. Information flow for the topics important for risk analysis has been explicitly specified in the seismic PSA process. Information flow between different safety analyses has been only specified where applicable.

ii) Adequacy of the verification

Defining the safety engineering process revealed that the case study is not necessarily comprehensive in means of safety analysis areas, however the existing analyses are quite clearly linked and there is flow of information between the safety analyses. The specific inputs and outputs of central topics in the accident scenario have not been fully specified between safety analyses.

iii) Proposals for improvement

The detailed specification of the safety engineering process could be performed as the first step of the analysis to ensure that every safety analysis needed for the comprehensive understanding of the issue is performed. It would also be beneficial to keep a database of the input and output information of the analyses. Also, the different information flow models, see for example Figure 4 and Figure 5, should be integrated more closely.

Accommodating the pool leakage to the case study would make the accident scenario more comprehensive, but at the same time increase the scenario complexity. The increased complexity would emphasize the need for analyses interaction, and therefore, would increase the value of management of information flow.

7. Discussion on safety engineering process strengths and weaknesses

In addition to evaluating the fulfilment of requirements, the safety engineering process has been compared to the V-model approach widely applied in the verification and validation of systems. In the comparison, potential strengths and weaknesses are identified and proposals for improvements are stated for the safety engineering process applied in the case study. Figure 4 outlines the safety analysis activities and safety engineering process of the case study. The activities and BESEP requirement topics are mapped to the V-model in Figure 6.

The following strengths have been identified for the safety engineering process of the case study:

- Safety analyses focus on the essential part of plant design and important safety system relevant to the accident scenario. The potential different initiating events have been identified and the different accident sequences have been specified.
- Safety analyses and their outcomes are identified in the safety engineering process, which helps to produce the needed evidence for the requirement verification.
- The technical disciplines relevant for the case study can be identified from the overall safety engineering process presented in the V-model.

The following weaknesses have been identified:

- As the case stays only at functional and architecture level, the further elaboration of

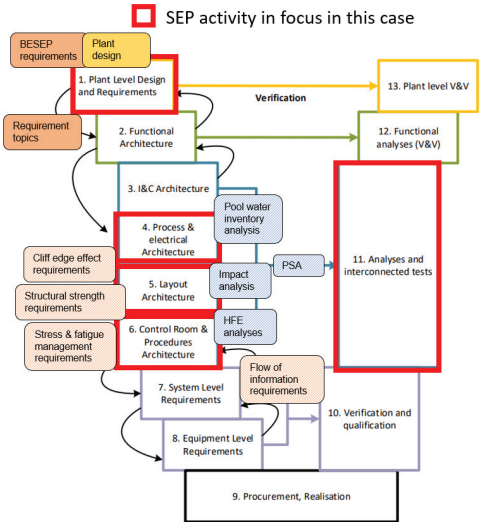

Figure 6. Focus of the overall safety engineering process in the case study adapted to V-model by Nuutinen, Sipola and Rantakaulio (2017).

requirements down to system and component specific level has not been performed.

- Interactions and interfaces to other, possibly dependent, plant systems have not been properly considered.
- Comprehensive PSA model was not available for the case study but was created specifically for the case.
- As the requirements had not been specified while conducting the safety analyses, the formal verification of requirements could only be performed after the analyses had been completed. There was no possibility to do detailed analyses on areas of specific interest.

As an improvement proposal, it would be beneficial to create a more comprehensive PSA model for the case study. With the more comprehensive model versatile failure combinations could be recognized and it would be possible to study in detail, why the residual heat removal system is lost. Also, detailed system and component level analyses would improve the assessment and make it more accurate. One of the most valuable improvements would be to outline the safety engineering process to three levels, the highest being the balance between the plant design, safety requirements and safety analyses as described in Figure 2. The middle level would be the interaction between the safety analyses types and the lowest the process of each safety analysis as shown in Figure 7.

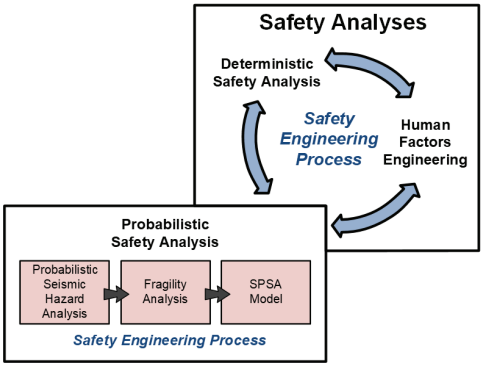

Figure 7. Middle and lower levels of safety engineering process illustrating the interaction of the safety analyses in the middle level and the safety engineering process of a seismic probabilistic safety analysis on the lower level.

8. Conclusions

The paper presents initial results from EU BESEP project. The findings will be further refined and developed in the cross-case and cross-group comparisons performed in the second half of the project. An example case study was presented to illustrate the evaluation of requirement fulfilment and the applied safety engineering process.

The analysis of the example case study reveals, that more detailed formulation of the safety engineering process would be beneficial for the future cross-case and cross-group comparisons. Outlining the safety engineering process in three levels: (i) the balance of the safety requirements, the safety analyses and the plant design, (ii) the interaction of the DSA, PSA and HFE, and (iii) the safety engineering process behind each of the specific safety analyses. Balance should be reached between the elements, wherever they are connected, ensuring the information flow and utilization inside and between each element. In an ideal situation, there is a consensus that, based on the safety analyses, the current plant design fulfils the given safety requirements.

A detailed description of the three levels of safety engineering practices for each of the BESEP case studies will significantly ease the safety margin assessment and requirement verification, as well as the overall objective of the benchmarking to find an efficient and integrated set of safety engineering practices and probabilistic safety assessment.

Furthermore, an effective and integrated set of safety engineering practices should provide support for the safety margin assessment and the verification of the safety requirements under focus. Traditional nuclear safety analyses can be categorized to deterministic safety analysis, probabilistic safety analysis and human factors engineering. Optimally,

each analysis provides feedback to the other analyses and to the overall safety design. How well this feedback is exploited is dependent on the information management and information flow between the different safety analyses. The information flow has been evaluated for the example case study. Based on the evaluation results there is still room for improvements. The improvements can be achieved for example by developing the safety engineering process to better support the information flow. One improvement could be the creation of more comprehensive PSA model to better integrate the information from different safety analysis together.

To summarize an efficient and integrated safety engineering process based on the findings from the first half of the project, it should include at least the following actions: (i) Connect together the main elements of safety engineering process: safety requirements, safety analyses and plant design. (ii) Safety analyses (probabilistic, deterministic and human factor engineering) should provide feedback and information to the other analyses and to the overall safety design. (iii) The process behind each specific safety analysis should be clearly formulated to support the higher-level safety engineering process.

In the second half of the BESEP project, the efficiency and integration of the safety engineering processes utilized in the partner countries will be studied with cross-case and cross-group comparisons.

Acknowledgement

The BESEP project has been co-funded by the European Commission and performed as part of the EURATOM Horizon 2020 Programmes respectively, under contract 945138 (BESEP).

References

Honour, E. C. (2013). Systems engineering return on investment. University of South Australia.

IAEA (2021) Introduction to systems engineering for the instrumentation and control of nuclear facilities. International Atomic Energy Agency. Vienna.

ISO/IEC/IEEE (2015). IEC 15288: Systems and software engineering — System life cycle processes. Geneva.

ISO/IEC TS (2011). IEC 15504-10: Information technology - Process assessment — Part 10: Safety extension. Geneva.

Könönen, N. E. (2013). "Spent Fuel Pool Accidents in a Nordic BWR." In International Conference on Nuclear Engineering, vol. 55805, p. V003T06A020. American Society of Mechanical Engineers.

Linnosmaa, J., Alanen, J., Helminen, A., Immonen, E., Holy, H. (2021). EU BESEP Deliverable 2.3 Specification on the key features of efficient and integrated safety engineering process. Finland.

NEA (2022). "Seismic Probabilistic Safety Assessment for Nuclear Facilities", *CSNI Technical Opinion Papers*, No. 18, OECD Publishing, Paris

Nuutinen, P., Sipola, S. and Rantakaulio, A. (2017). "Advanced licensing and safety engineering method – ADLAS", 10th International Topical Meeting on Nuclear Plant Instrumentation, Control, and Human-Machine Interface Technologies, NPIC and HMIT 2017, pp. 2020–2030.

Rein, S. (2021). EU BESEP Deliverable 2.2 Requirement baseline for BESEP. Finland.

Sun. D., Li. L., Tian Z., Chen. S., Wang. H., Chen. G., Zhang. Y., Zhang. L. (2021). "An advanced probability safety margin analysis approach combined deterministic and probabilistic safety assessment" *Nuclear Engineering and Design.* Vol 385.