EURATOM Project BESEP - Deliverable 4.3 Evaluation of balance in verification efforts of safety margins between different external hazards

Carl Sunde[a], Elias Brådenmark[a], Stefan Authén [a*]
[a]Risk Pilot AB, Stockholm, Sweden

Abstract: This paper presents Deliverable 4.3, Evaluation of balance in verification of safety margins between different external hazards, of the EU research project BESEP, Benchmark Exercise on Safety Engineering Practices. BESEP was conducted between several European Union (EU) countries during 2020 to 2024 with the aim of giving guidance for efficient Safety Engineering practices in order to support the safety margins determination and safety requirement verification in the licensing process of nuclear power plant new builds and upgrades.

Keywords: PSA Applications, Risk Significance, External Hazards, Safety Engineering Process.

1. INTRODUCTION

The Benchmark Exercise on Safety Engineering Practices (BESEP) has been conducted between several European Union (EU) countries. BESEP aims to develop best practices for the verification of stringent safety requirements against external hazards. The aim is achieved using efficient and integrated set of safety engineering practices and probabilistic safety assessment. The efficient and integrated set of safety engineering practices support the safety margins determination and safety requirement verification helping the licensing process of nuclear power plant new builds and upgrades.

The management of nuclear power plant's safety is a continuous process of balancing the interaction between the main elements of plant's safety design: requirements, safety analyses and plant design itself. Managing this interaction between these main elements is a complicated process that is addressed in the BESEP project's context as the safety engineering process (SEP). During the lifecycle of a plant, there can be various changes to the plant's safety design, with focus on safety related SSCs, for example:

- New design concepts and feasibility studies may give new ideas to upgrade 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.

In case there is a change in one of these three main elements of plant's safety design, the change should be reflected in the two other elements. This is usually taken care of by the safety engineering process. The integration of these main elements through the safety engineering process is illustrated in Figure 1.

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 and sufficient safety margins are present. The changes to the main elements 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.

In practice, the safety engineering processes vary between organizations. Therefore, the purpose in BESEP project has not been to develop an all-inclusive safety engineering process suitable for all subjects, but to identify important features of an efficient and integrated safety engineering process suitable for the practitioners in nuclear safety.

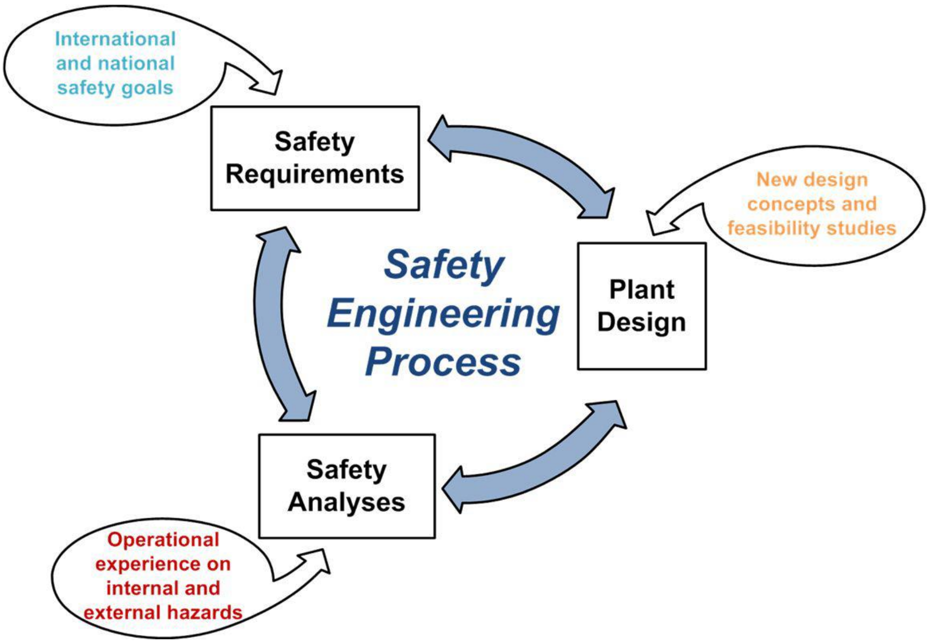

Figure 1. The main elements of plant´s safety design and safety engineering process.

Based on identified key features, success factors and evaluation results from the benchmark exercise, best practices are given on how to achieve an efficient and integrated safety engineering process to better support the safety design of a nuclear power plant. Guidance addressing the utilization of improved safety analysis methods in an integrated manner is given. The previous is allocated under following topic areas:

- 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.

This paper addresses Task 4.3 of the BESEP project, Evaluation of balance in verification efforts, [1].

2. OBJECTIVES OF BESEP TASK 4.3

The main objective of Task 4.3 was to compare the benefits and the amount of extra work with the risk significance of the involved external hazard and SSC to the plant. The comparison helps to create a graded approach for the deployment of more sophisticated safety analysis methods while maintaining a balance between different external hazards. This is achieved by performing an evaluation of the balance in verification efforts (i.e., the level of efforts spent on each type of analysis (PSA, DSA and HFE)) of the different Generalized Case Studies (GCSs) developed in BESEP Task 3.5, [2]. The GCSs were developed based on the case studies and grouping of case studies in Tasks 3.1-3.2, [3]-[4]. In Task 3.5 each of the four case study groups developed a generalised case study, hence four GCSs were available for evaluation within Task 4.3. The basis for the evaluation of the balance in verification efforts were the comparison criteria developed in Task 4.1, [5]. The cross-case comparison between case study groups performed in Task 4.2 [6] also served as input to Task 4.3.

The horizontal flow in Figure 2 illustrates the cross-group comparison of the GCSs in Task 4.3. The different case study groups are compared based on the amount of work and effort used in the safety margins verification compared with the risk significance of the involved external hazard and SSCs of the plant. The results of the probabilistic safety assessments are used for describing the risk significance. The evaluation aims to identify benefits from increasing the level of detail in the applied safety analysis methods, e.g., the benefits of applying more detailed models or additional simulations. The aim of the comparison is also to help create a graded approach for the deployment of more sophisticated safety analysis methods while maintaining a balance between different external hazards.

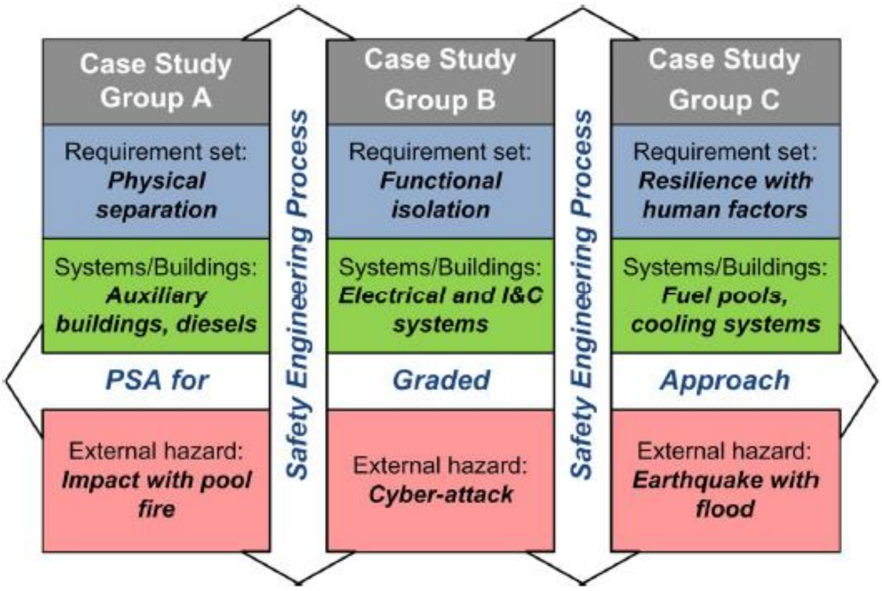

Figure 2: The overall structure of the benchmark exercise.

3. METHOD FOR CROSS-CASE COMPARISON

Within Task 4.3 the focus was on comparing the benefits and the amount of work and effort used in the SEP with the risk significance of the GCSs. The aim of the comparison is to help create a graded approach for a balanced deployment of analysis efforts between different external hazards. On a holistic level, and with a reactor safety perspective, "balance" is normally interpreted as using a safety graded approach in the SEP, which for Task 4.3 is interpreted as spending the amount of efforts motivated by safety importance, i.e., the risk significance of the GCS. The following key aspects are evaluated in Task 4.3, where the first three will be addressed in this paper:

- Level of efforts in the SEP
- Risk significance
- Risk significance vs efforts
- Benefits of applied efforts

3.1. Level of Efforts

The level of efforts spent on each type of analysis (PSA, DSA and HFE) needs to be estimated for each GCS. One option to perform this is to use only qualitative measures of spent efforts instead of actual working hours. The main advantage of qualitative measures is that they are easier to apply in situations where the actual measures are unknown or at least difficult to calculate. The main disadvantage is of course that they are subjective and that it is vital that different estimates are based on the same perception of the used qualitative scale in order to be comparable. Hence, the option chosen in Task 4.3 was to use a scale with absolute values representing actual spent working hours, depending on the scope of labour, see Table 1. The scale is based on estimates from the expertise of the BESEP project team and their experience from previously performed analyses. As such, it should be seen as realistic estimates, and not scientifically validated data.

Table 1. Scale of working hours.

Scope of labour	Scale of working hours
Editorial changes to models, data and methods.	100
Existing models, data and methods slightly modified.	500
Moderate modifications on models, data and methods. New parts developed.	1000
Extensive modifications of existing models, data and methods.	2500
Completely new models, data and methods.	5000

By using the scale in Table 1 as reference, the absolute numbers for each individual analysis discipline (DSA, PSA and HFE) involved in each GCS could be estimated by using Table 2.

Table 2. Table for evaluation of amount of labour in working hours.

Type of labour	**Analysis/ discipline**			
	PSA	**DSA**	**HFE**	**Total**
Models				
Data				
Methods/procedures				
Total				

3.2. Risk Significance

For Task 4.3 the results of PSA should be used to gain information about the risk significance, but since risk significance can be described by different measures on different levels, depending on the application, e.g.:

- Absolute Core Damage Frequency (CDF) value that describes an early position in the SEP, prior to any installed Safety Measures (SMs), where input is given to the decision to initiate certain actions and analyses in order to either prove that sufficient safety margins already exist, or to show that additional SMs needs to be installed in the plant in order to reach sufficient safety margins.
- Relative CDF value of the GCS to the total plant CDF, prior to any installed SMs, in order to show the GCS significance in the plants actual risk profile, or relative to the Safety Target, e.g., 1E-04/year, in order to address safety margins and show the GCS significance in relation to probabilistic safety requirements.
- Change in CDF of the GCS due to the installment of safety measures, relative to the total plant CDF or the Safety Target. This measure addresses that the justification for spending certain efforts on safety verification can be argued to not only depend on the initial risk significance but also on what is gained by applying the efforts, i.e., the larger risk reduction that is achieved by installing a safety measure (e.g., changes in plant configuration and/or procedures), the more efforts can be justified to use in the safety verification.

These measures can of course also be applied to the Unacceptable Release Frequency (and/or LERF) relevant to the GCS.

The choice of measure to use ultimately depends on national and plant specific safety targets and risk related decision making criteria. It is hence not obvious which measure to use in Task 4.3 to evaluate the case studies and consequently, Task 4.3 applied several different measures of risk significance, see Table 3.

Table 3. GCSs Risk Significance

	a. Relative to CDF Safety Target	b. Relative to total CDF	c. Relative to total LERF
Risk Significance prior to installing safety measures[1]			
Risk Significance after installing safety measures[2]			
Relative change in Risk Significance[3] due to safety measures			

1. Calculated as: a) $\frac{CDF_{Prior\ SM}}{CDF_{ST}}$; $b)$ $\frac{CDF_{Prior\ SM}}{\Sigma CDF_{Prior\ SM}}$; $c)$ $\frac{LERF_{Prior\ SM}}{\Sigma LERF_{Prior\ SM}}$ Eq. 1.a to 1.c.

2. Calculated as: $a)$ $\frac{CDF_{After\ SM}}{CDF_{ST}}$; $b)$ $\frac{CDF_{After\ SM}}{\Sigma CDF_{After\ SM}}$; $c)$ $\frac{LERF_{After\ SM}}{\Sigma LERF_{After\ SM}}$ Eq. 2.a to 2.c.

3. Calculated approximative as: $Eq. 1.x - Eq. 2.x$ Eq. 3.a to 3.c.

Where
$SM_{\square}$ = Safety Measures
CDF_{ST} = Core Damage Frequency Safety Target
$CDF_{Prior\ SM}$ = Core Damage Frequency attributable to the external event(s) addressed in GCS prior to installing Safety Measures
$LERF_{Prior\ SM}$ = Large Early Release Frequency attributable to the external event(s) addressed in GCS prior to installing Safety Measures
$CDF_{After\ SM}$ = Core Damage Frequency attributable to the external event(s) addressed in of GCS after installing Safety Measures
$LERF_{After\ SM}$ = Large Early Release Frequency attributable to the external event(s) addressed in GCS after installing Safety Measures
$\Sigma CDF_{Prior\ SM}$ = Total Plant Core Damage Frequency prior to installing Safety Measures
$\Sigma LERF_{Prior\ SM}$ = Total Plant Large Early Release Frequency prior to installing Safety Measures
$\Sigma CDF_{After\ SM}$ = Total Plant Core Damage Frequency after installing Safety Measures
$\Sigma LERF_{After\ SM}$ = Total Plant Large Early Release Frequency after installing Safety Measures

It is recognized that the PSA can mainly give information on the significance of elements included in the PSA, such as external events, accident scenarios, SSCs, human actions and potential safety measures to be installed, and only to a limited extent can give information on the need for performing analyses within the different disciplines, i.e., DSA, PSA and HFE.

3.3. Risk Significance Compared with Efforts

The objective of comparing the level of efforts spent on the SEP with the risk significance is to evaluate whether spent efforts commensurate with the change in risk significance of the external event(s) and/or safety margins due to the installed safety measures (plant change). The hypothesis is that there should be a positive correlation between the two features. In BESEP Deliverable 4.1 [5] an attempt was made to use evaluation matrices for the comparison, where the effort needed for the case study elaboration was clustered into several grades. This matrice-approach was further developed in Task 4.3 to account for the method development performed for evaluation of amount of labour and risk significance.

Table 4 presents the primary evaluation matrix for Task 4.3 based on the estimation of effort (for each analysis discipline PSA, DSA and HFE) and the risk significance described by the relative change in risk contribution to the Safety Target due to installed safety measures. The matrix diagonal is marked in green which indicates a balance between achieved risk reduction compared to spent efforts, while the sections above the diagonal indicate an unbalance with too much resources spent compared to the risk reduction. The red sections of the matrix indicate a significant unbalance.

In general, all sections below the diagonal indicate an effective analysis process, although it could also mean that very large conservatisms have been applied in the analyses. This can result in that unnecessarily extensive and expensive safety measures are applied, which could have been avoided if more detailed safety analyses were performed. Due to this reason the sections below the diagonal are marked with yellow. Similar matrixes were developed for the alternative risk significance measures in Table 3, and also for the total amount of efforts spent in the SEP, i.e. the sum of efforts applied for each analysis discipline (PSA, DSA and HFE).

It should be noted that the scales in the matrix in Table 4 are based on estimates from the expertise of the BESEP project team and their experience from previously performed analyses. If other scales are used, both for the level of effort and for the risk significance the results from the comparison could be different.

Table 4. Matrix for Risk Significance vs. efforts study for each analysis discipline.

	Level of effort Y [h][2]			
Risk Significance Change in CDF/FDF relative to Safety Target[1]	Y < 500	500 < Y < 1500	1500 < Y < 5000	X > 5000
X < 0.1%				
0.1% < X < 1%				
1% < X < 50%				
X > 50%				

1.According to value given by Eq. 3.a.
2. According to estimated sums in Table 2.

4. CROSS-CASE COMPARISON

The cross-case comparison in BESEP Task 4.3 was performed by mapping the estimates of labour and risk significance for each GCS into the same matrix. To increase the depth of the evaluation the mapping is performed for a selection of the different risk significance measures identified in Table 3, and also for the absolute CDF of the GCS. The mapping is performed both for effort estimates for each analysis discipline (DSA, PSA and HFE), and for the total amount of efforts spent in the GCS.

To increase the depth of the evaluation the mapping was performed for the following risk significance measures:

1. Change in CDF/FDF relative to Safety Target due to installed safety measures
2. Change in CDF/FDF relative to Total CDF/FDF due to installed safety measures
3. Initial CDF/FDF
4. Initial CDF/FDF relative to Safety Target
5. Initial CDF/FDF relative to Total CDF/FDF

The threshold values for the risk significance are different depending on which risk measure is used whereas the threshold values for level of effort is the same (only differs if it is the total amount of work that is considered or the individual disciplines). It should be noted that the (risk) significance of each discipline (PSA, DSA and HFE) in the GCS cannot be estimated, hence it is difficult to make any deeper analysis on the balance between different analysis disciplines without looking further into the types of safety measures considered in each GCS and corresponding risk importance measures. Table 5 to 9 gives examples of the different matrix evaluations performed in Task 4.3, where “STIN”, “EIIC”, “LUHS” and “PVES” are the abbreviations for the evaluated GCS.

Table 5. Comparison of risk significance vs efforts between GCSs. Amount of efforts for each analysis discipline. Change in CDF/FDF relative to the safety target due to installed safety measures.

	Level of effort Y [h]			
Risk Significance Change in CDF/FDF Relative to Safety Target	Y < 500	500 < Y < 1500	1500 < Y < 5000	X > 5000
X < 0.1%		STIN^{HFE} EIIC^{HFE}	STIN^{DSA} EICC^{PSA}, EICC^{DSA}	STIN^{PSA}
0.1% ≤ X < 1%				
1% < X < 50%	LUHS^{DSA}	LUHS^{PSA} LUHS^{HFE}		
X > 50%			PVES^{HFE}	PVES^{DSA} PVES^{PSA}

Table 6. Comparison of risk significance vs efforts between GCSs. Amount of efforts for each analysis discipline. Change in CDF/FDF relative to total CDF/FDF due to installed safety measures.

	Level of effort Y [h]			
Risk Significance Change in CDF/FDF Relative to Total CDF/FDF	Y < 500	500 < Y < 1500	1500 < Y < 5000	X > 5000
X < 0.1%				
0.1% < X < 1%				
1% < X < 50%	LUHS^{DSA}	STIN^{HFE} LUHS^{PSA} LUHS^{HFE}	STIN^{DSA}	STIN^{PSA}
X > 50%			PVES^{HFE}	PVES^{DSA} PVES^{PSA}

Table 7. Comparison of risk significance vs efforts between GCSs. Amount of efforts for each discipline. Risk significance is expressed as the initial CDF/FDF.

	Level of effort Y [h]			
Risk Significance CDF/FDF prior to SM	Y < 500	500 < Y < 1500	1500 < Y < 5000	X > 5000
X < 1E-8				
1E-8 < X < 1E-7		STIN^{HFE} EIIC^{HFE}	STIN^{DSA} EIIC^{PSA} EIIC^{DSA}	STIN^{PSA}
1E-6 < X < 1E-7	LUHS^{DSA}	LUHS^{PSA} LUHS^{HFE}		
X > 1E-6			PVES^{HFE}	PVES^{DSA} PVES^{PSA}

Table 8. Comparison of risk significance vs efforts between GCSs. Total amount of efforts for each GCS. Risk significance is expressed as the initial CDF/FDF relative to the Safety Target.

	Level of effort Y [h]			
Risk Significance Initial CDF/FDF Relative to Safety Target	Y < 1500	1500 < Y < 4500	4500 < Y < 15000	X > 15000
X < 0.1%				
0.1% < X < 1%			STIN, EIIC	
1% < X < 50%		LUHS		
X > 50%				PVES

Table 9. Comparison of risk significance vs efforts between GCSs. Total amount of efforts for each GCS. Risk significance is expressed as the initial CDF/FDF relative to the initial Total CDF/FDF.

	Level of effort Y [h]			
Risk Significance Initial CDF/FDF Relative to Total CDF/FDF	Y < 1500	1500 < Y < 4500	4500 < Y < 15000	X > 15000
X < 0.1%				
0.1% < X < 1%				
1% < X < 50%		LUHS	STIN	
X > 50%				PVES

5. RESULTS AND CONCLUSIONS

BESEP Task 4.3 investigated the possibilities to use a matrix-based approach to evaluate reasonable efforts to be spent on safety verification given a certain risk significance of accident sequences following an external event, which makes out one of the trademarks of a balanced SEP. The evaluation was performed based on Generalized Case Studies (GCSs) developed in previous tasks of BESEP project.

A number of challenges with the chosen methodology were identified during the work. Although proving a sufficiently low level of risk may require a significant amount of analytical effort, risk significance as measured by probabilistic risk metrics is not the only way to characterize the value of the effort expended. Efforts spent on pure safety verification is also of value but not covered by used risk metrics. Furthermore, the total investment value spent on the plant modifications may also be an important factor in evaluating the resource effectiveness.

The used scales for risk significance vs. amount of efforts are quite wide and solely based on engineering judgement. The scales should be seen as a hypothesis and needs further justification, e.g., by more cases to compare with. Another challenge is that the current matrix-approach do not indicate the risk change that is attributable to a particular analysis discipline, hence the balance between different disciplines cannot be evaluated.

Also, there are several potential risk metrics that may be applicable measures to describing risk significance. The made comparison shows that different features are addressed using different risk significance measures:

- Change in CDF relative to Safety Target due to installed safety measures.
  This approach with the used threshold values, seems to give guidance for a balanced SEP for cases where actual safety improvements are installed, but not for other cases. The bigger effect a safety measure has on the safety margin, the more efforts is motivated to put into the SEP.
- Change in CDF relative to total CDF due to installed safety measures.
  When applying this measure of risk significance, the decision making will be more focused on spending efforts on achieving a balanced plant risk profile, than just meeting safety requirements. The approach is more useful in the GCS where safety improvements have been installed, but not necessarily in order to meet any safety target and is probably most relevant to risk informed decision making for plants where safety targets are already met.
- Initial CDF.
  This type of measure for risk significance has a key role in safety verification, i.e., in the GCSs where the main goal is to demonstrate a sufficient existing risk level, rather than to evaluate proper safety measures to implement in order to reach an acceptable risk level.
- Initial CDF relative to Safety Target.
  This approach is of importance mostly in decision making concerning cases where safety improvements might be necessary to achieve sufficient safety margins. The approach does not address the efficiency of the SEP.
- Initial CDF relative to Total CDF.
  This approach has relevance to both safety verification cases and cases where safety improvements are introduced in order to improve the balance of the plants risk profile. The approach does not address the efficiency of the SEP.

The studied set of measures is not exclusive. There are several other possible measures to use, e.g., measures covering release frequency or measures covering the risk significance of individual SSCs and manual actions. The cross-case comparison performed here also shows that the purpose of the SEP is of high importance. The evaluated GCSs describe at least two different reasons for a SEP; 1) actual need for safety improvements in the plant due to insufficient/unsatisfying safety margins, and 2) the need for safety verification (against requirements) when existing safety margins are acceptable (e.g., new build).

The cross-case comparison has been performed on only four different examples of the SEP, where all cases were considered balanced in verification efforts by the partners in each GCS group, and where very limited information was given on the possible benefits that could be gained by a different allocation of analysis efforts. Also, the choice of the risk significance measures to use to evaluate the balance in verification efforts ultimately depends on national Safety Targets and the specific risk related decision making criteria of individual utilities. There might also be significant differences in what is considered a reasonable amount of efforts between different countries and/or organizations, due to different regulations, methodologies, capacities, financing and so on. It is hence difficult to draw any detailed conclusions on the benefits of a graded deployment of safety verification efforts, and further investigation based on a much larger data-set would be needed in order to develop more conclusive results.

Despite the above challenges and different perspectives of risk importance, the approach of using a matrix to map the risk significance of accident sequences against verification efforts seems to be able to provide high level guidance for a graded deployment of safety analysis resources, given that adaptation to a national and/or utility specific set of decision-making criteria, risk significance measures and threshold values is performed.

Acknowledgements

The BESEP project has been co-funded by the European Commission and performed as part of the Euratom Horizon 2020 Programmes respectively, under contract 945139 (BESEP).

References

[1] Sunde C, Brådenmark E, Authén S. BESEP Deliverable 4.3: Benchmark Exercise on Safety Engineering Practices, Risk Pilot AB, Sweden, 2023.
[2] Cederlöf N. BESEP Deliverable 3.5: Description of generalized case studies, VTT Technical Research Centre of Finland Ltd, Finland, 2022.
[3] Bareith A, Siklossy T. BESEP Deliverable 3.1: Definition of a Pool of Case Studies, NUBIKI Nuclear Safety Research Institute Ltd, Budapest, 2022.
[4] Bareith A, Siklossy T. BESEP Deliverable 3.2: Description of Case Study Groups, NUBIKI Nuclear Safety Research Institute LTD, Budapest, 2022.
[5] Sedlák J, Holý j. BESEP Deliverable 4.1: Comparison criteria, ÚJV Řež, a. s., Husinec, 2023.
[6] Kovacs Z, Hlavac P. BESEP Deliverable 4.2: Results of cross-case comparison between case study groups, RELKO spol. s r.o. Bratislava, 2023.