VTT Technical Research Centre of Finland

Benchmark Exercise on Safety Engineering Practices: Management Plan Concept

Immonen, Essi; Helminen, Atte; Linnosmaa, Joonas; Laarni, Jari

Published in:
Proceedings of the 33rd European Safety and Reliability Conference (ESREL 2023)

DOI:
10.3850/978-981-18-8071-1_P186-cd

Published: 01/01/2023

Document Version
Publisher's final version

Proceedings of the 33rd European Safety and Reliability Conference (ESREL 2023)
Edited by Mário P. Brito, Terje Aven, Piero Baraldi, Marko Čepin and Enrico Zio
 Published by Research Publishing, Singapore.
doi: 10.3850/978-981-18-8071-1_P186-cd

Benchmark Exercise on Safety Engineering Practices: Management Plan Concept

Essi Immonen

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

Atte Helminen

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

Joonas Linnosmaa

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

Jari Laarni

VTT Technical Research Centre of Finland Ltd, Finland. Email: jari.laarni@vtt.fi

This paper continues to describe the midterm outcomes of EU research project Benchmark Exercise on Safety Engineering Practices. To further support the planning, controlling and conducting of a fully integrated safety engineering effort, the authors propose a Safety Engineering Management Plan (SaEMP), which is a document that addresses the overall safety engineering management approach. This is another step towards more efficient and integrated safety engineering process in the scope BESEP project following the possibilities offered by systems engineering (SE). As an example of the topics covered by the Safety Engineering Management Plan, this paper further focuses on the flow of information between different safety analysis disciplines, namely probabilistic safety analysis and human factors engineering.

Keywords: Safety engineering management plan, nuclear safety, human factors engineering, probabilistic safety analysis.

1. Introduction

This paper continues to describe the midterm outcomes of the EU research project Benchmark Exercise on Safety Engineering Practices (BESEP). The BESEP project and its first results have been introduced in a previous paper by the authors (Immonen et al., 2022).

The project strives to find the most efficient safety engineering practices to support the safety margins determination and safety requirement verification in order to streamline the licensing process of nuclear power plant new builds and upgrades. The expected key results of the project are:

- Best practices for the verification of evolving and stringent safety requirements against external hazards.
- Guidance on the closer connection of deterministic safety analysis (DSA), probabilistic safety analysis (PSA) and human factors engineering (HFE) for determination and realistic quantification of safety margins.
- Guidance on creation of a 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 builds up on the safety engineering process (SEP) introduced in the previous paper by the authors (Immonen et al., 2022). SEP is developed further by a conceptual definition of Safety Engineering Management Plan (SaEMP). In this paper, the safety engineering process requirement topic flow of information is used as the main application target for the SaEMP concept. Flow of information as part of SaEMP is discussed, concentrating on the closer connection

of probabilistic safety analyses and human factors, specifically the connection of human reliability analysis (HRA) and HFE. A case example of a spent fuel pool accident is used to illustrate the safety engineering methodologies.

2. Safety Engineering management plan

Safety engineering encompasses an extensive number of engineering activities essential for the safe operation of the plant. In fact, we see that safety engineering process covers all the actions made during the plant's lifecycle that keep it safe to operate.

We approach safety engineering process as an iterative way to connect the main elements of safety design: safety requirements, safety analyses and plant design. In (Linnosmaa et al., 2021), the authors presented an introduction to an efficient and integrated safety engineering process in the scope of BESEP project following the possibilities offered by systems engineering (SE). To further support the planning, controlling and conducting a fully integrated safety engineering effort, the authors propose a Safety Engineering Management Plan, which is a document that addresses the overall safety engineering management approach.

The document follows the principles set by System Engineering Management Plan (SEMP) (Alanen & Salminen, 2016) but is more tailored for the needs of nuclear industry. Just like SEMP, SaEMP details the technical and management processes that will be used and applied by program and engineering personnel on how safety engineering activities will be organized and managed during the plants lifecycle and to provide a foundation for all safety engineering activities in the organization.

SaEMP is not a system or safety specification or analysis but a plan for the organisation to carry out rigorous and comprehensive safety engineering. It can include, for example, a life cycle model, description of safety engineering processes (e.g. requirement management, configuration management, system analysis…), the organisational model and a selection of tools to implement the safety design principles in practice. Through these topics SaEMP will act as a supervisory document to manage the DSA, PSA and HFE disciplines, their interactions and the interplay between safety requirements and plant design. Each safety analysis discipline might have their own governing documents and plans, but SaEMP is meant to be an overarching document to add integration and interface layer for the disciplines.

Within BESEP project, the main effort of SaEMP is to provide support for fulfilling the safety engineering requirement topics selected in the beginning of the project to be in the focus of the work. The selected topics are related to:

- Safety engineering management.
- Safety design and requirement management for external hazards.
- Flow of information between safety analyses
- Verification and validation of design.
- System modification and configuration management.
- Validated modelling and simulation analysis tools.

These requirement topics were already introduced in (Immonen et al., 2022) and (Rein, 2022). Within BESEP project, the topic areas have been further elaborated into more specific requirements, however in this paper we only focus them on a topical level.

The visioned content of SaEMP aims to offer methods and tools for fulfilling the requirements and supporting the safety engineers in their work of managing the safety engineering in the plant. In this paper, we focus on the flow of information topic, which is further specified in the following chapter using an example case.

3. Application of SaEMP to flow of information

3.1. Case example

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). This case study has been described previously in more detail in (Immonen et al., 2022).

A generic spent fuel pool with the residual heat removal (RHR) systems is illustrated in Fig. 1. 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

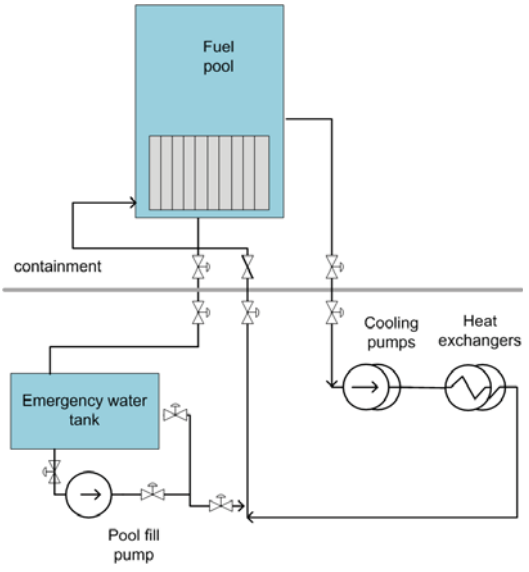

Fig 1. Generic spent fuel pool system

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 are 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.

The flowchart in Fig. 2 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. For extreme external impacts beyond the design basis acceleration levels, the integrity of the spent fuel pool can be lost, and the main interest in the analysis is how to restore the pool integrity and how to compensate the coolant leakages. For less extreme external impacts, the main focus is on ensuring the short and long-term residual heat removal of the spent fuel pool. In case the residual heat removal is lost, MELCOR analyses are performed to estimate the evolution of the pool water inventory, i.e. the water level and temperature evolution and the time points when radiation protection is lost and the fuel is damaged.

The case study is further complemented with probabilistic safety assessment and analyses of operator actions, that are discussed in more detail in chapter 4.

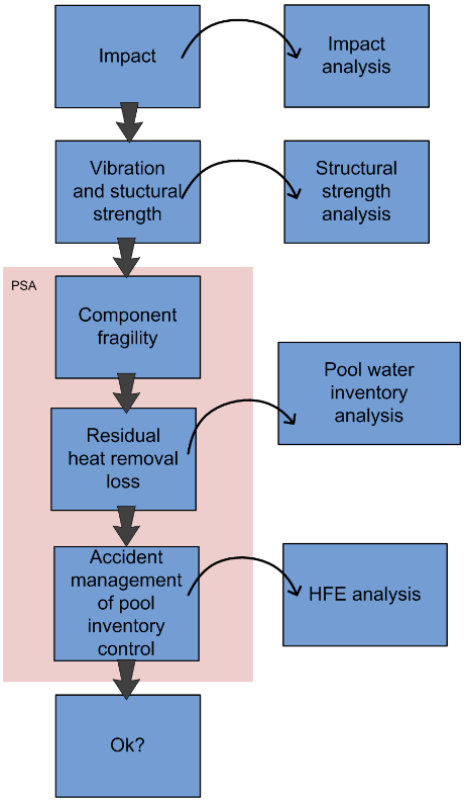

Fig. 2. Accident progression scenario

3.2. Flow of information in management plan

A conceptual flowgraph has been developed as a tool to answer the flow of information safety engineering process topic. A case specific diagram is presented in Fig. 3, using the safety requirements and analyses of the spent fuel pool case study presented previously in this paper. The diagram as a whole is one way of fulfilling the SEP requirement flow of information presented in the upper left corner of diagram.

The flow of information is illustrated using three areas of the safety engineering process: 1) safety requirements, 2) safety analyses and 3) plant design. The plant design needs to fulfil the BESEP safety requirements, which is demonstrated with deterministic and probabilistic safety analyses and human factors engineering processes.

The safety requirements of the example case are from the BESEP requirement baseline, which

has been developed for the benchmark purposes by Rein (2021), representing national and international safety requirements. The requirements typically determine which safety analyses are chosen to be performed.

The safety analyses include the DSA, PSA and HFE disciplines, and their interactions. Information from each of the analyses areas is transferred to the others, for instance, deterministic impact analysis provides inputs to seismic PSA, and pool inventory analysis to HFE analyses. Also, HFE knowledge is used in human reliability analysis in the field of PSA. Results of PSA are used to further refine and specify the other assessments. To further explain the use of the flow of information, HFE and PSA and their interrelationships are discussed in more detail in the following chapters.

In plant design, the architecture disciplines such as process and electrical, control room and procedures, and the layout, are used in the safety analyses, but also updated based on the DSA, PSA and HFE outcomes.

The presentation in Fig. 3 aims to illustrate one possible configuration of the connections between the domains and analyses. Especially between the safety analysis disciplines, there may be other ways to draw the interconnections, and for example some parts of the PSA analyses could be placed to HFE and DSA areas. Also, the diagram does not take a stand in which order the analyses should be performed.

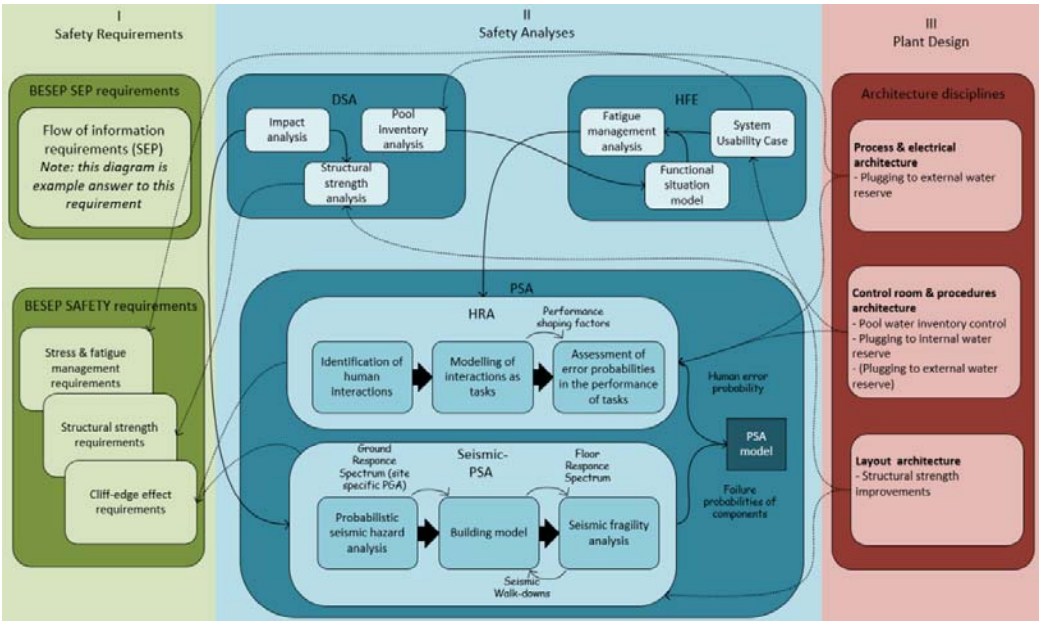

Fig. 3. Case specific flow of information diagram

4. Flow of information to support PSA with HFE

4.1. Simplified PSA model of accident scenario

The accident frequency for the loss of cooling accident of spent fuel pool due to external impact is determined using seismic PSA. The methodology was described for the case study in the previous paper of ESREL2022 conference (Immonen et al., 2022).

For the less extreme external impacts, the case study assumption was that due to impact the pool maintains its integrity. The residual heat removal of the pool is, however, lost. The residual heat removal can be restored through specific back-up systems requiring operator actions.

After the normal residual heat removal and water inventory control of the spent fuel pool has been lost, the pool is cooled by boiling and the pool's water inventory is maintained by backup systems. There are two diverse options requiring operator actions to increase the water inventory.

First option is to use the plant's internal water reserves. The second option is to plug the pool's water injection system to an external water source, e.g. from a fire truck.

The simplified PSA model created for the accident scenario is straightforward. The fuel damage is the product of three basic events: 1) Loss of residual heat removal due to external impact, 2) Failure to plug on internal water reserve, and 3) Failure to plug on external water reserve. The fault tree illustrating the accident is shown in Fig. 4.

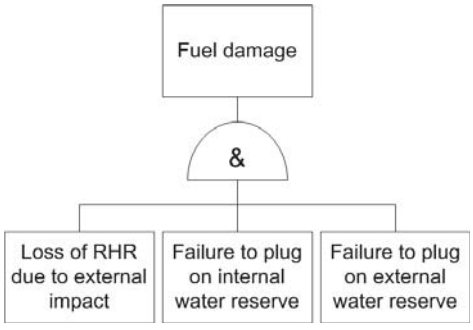

Fig. 4. Fault tree of fuel damage due to external impact induced loss of RHR

4.2. Human factors engineering in the accident scenario

The analysis of operator actions of an incident can be presented in a form of a functional situation model. Functional Situation Model (FSM) combines both chronological and functional views (Savioja, 2014). In the chronological view, the event is divided into different phases (detection, mitigation, diagnosis and stabilization; see Fig. 5) based on the goals of the operating activities; in the functional view, the critical functions of the process that are endangered in a specific situation are depicted.

Recovery of the threatened safety functions is performed through operator actions, and the time scales of the scenario set time margins (i.e. time thresholds) for successful completion of the whole scenario and for each event phase. The fear of not completing the critical actions in a scheduled time, and as a consequence, of not recovering the threatened safety functions is the main cause of stress. Since there is a lot of time to react to loss of cooling and fix the problem, it is

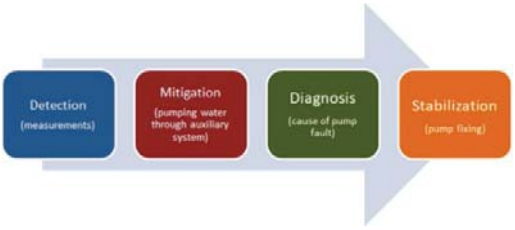

Fig. 5. Chronological view

even a bigger challenge to the operative personnel to stay vigilant throughout the recovery period.

All in all, operator stress and fatigue are prominent performance shaping factors in all four stages (detection, mitigation, diagnosis and stabilization) of the accident management. We are here mainly interested in cognitive effects, including factors such as narrowing of attention, tunnel vision, disruption of working memory and response rigidity. According to the theory of cognitive appraisal, the evaluation of the meaning and significance of the accident situation and one's capacity to meet the demands are essential steps in coping with stress and fatigue effects.

The negative effects of stress, fatigue and cognitive load in the pilot case can be mitigated by basic and refresher simulator training and carefully designed operating procedures. The development of stress and fatigue mitigation training should be based on a systematic approach, which also provides the basis for training evaluation (see Section 4.3).

4.3. Integration of PSA and HFE by flow of information

The HFE approach described above is mainly based on qualitative analyses with the aim to identify and develop improvements for the operators to operate the plant safely. However, for the PSA purposes, quantitative estimates of human errors are needed. In Fig. 3, the human error probability is the input from HRA to the actual PSA model. HRA is used to create the quantitative estimates and there is a variety of HRA methods and analysis principles that can be applied (Bell, 2009). For the quantitative estimation, it is beneficial to apply the qualitative or semi-qualitative findings of HFE in HRA.

A methodological tool that is useful in the aggregation and synthesization of collected HFE evidence is Systems Usability Case (SUC) (Koskinen et al., 2021). It can be considered as an

accumulated body of evidence of the systems usability of control room systems and procedures. There is a two-way interaction between the SUC and the HFE requirements base (incl. stress and fatigue management requirements): the HFE requirements set the reference basis for the goal structure part of the SUC, and the claim structure part of the SUC provides evidence of the fulfilment of these requirements. Stress and fatigue management analysis aims to figure out whether the operators are able to perform the critical tasks. FSM, mentioned in the previous section, is a sophisticated task analysis method explicating the connection between critical plant functions and operator actions. FSMs have input to Fatigue Management Analysis, which in turn has input to HRA activities.

For example, in HFE, safety margins can be interpreted as separation between task demands and operator capabilities, and they are mirrored in the specification of stress and fatigue management requirements. In order to assess the effect of stress and fatigue on the safety margin, we first have to analyse critical tasks by FSM, then identify potential human errors associated with each task/activity, and finally generate semi-quantitative (i.e., ordinal) estimates of probability of their occurrence.

HFE results are used as input to the quantitative estimation of failure probabilities in HRA. In the case study example, the failure probability of operator actions for the two basic events was estimated using a prior failure probability 1E-4 for the first option (Plugging to internal water reserve) run from the control room and a prior failure probability 1E-3 for the second option (Plugging to external water reserve) run from the control room and other locations of the plant. Both failure probabilities were multiplied with performance shaping factors (PSF) to achieve the posterior failure probabilities. The PSF and posterior failure probabilities for the basic events representing the operator actions are shown in Table 1.

HFE analyses are especially beneficial in the specification of the PSFs applied in the example case, most notably the factors related to stress and fatigue. As mentioned above, since the time window of the accident scenario is long, fatigue presumably poses a bigger challenge to the operative personnel than stress, that is, operators who are less alert and vigilant are more prone to make errors. This input is illustrated in Fig. 6 with an arrow from the HFE fatigue management analysis to HRA and to the evaluation of PSF in particular.

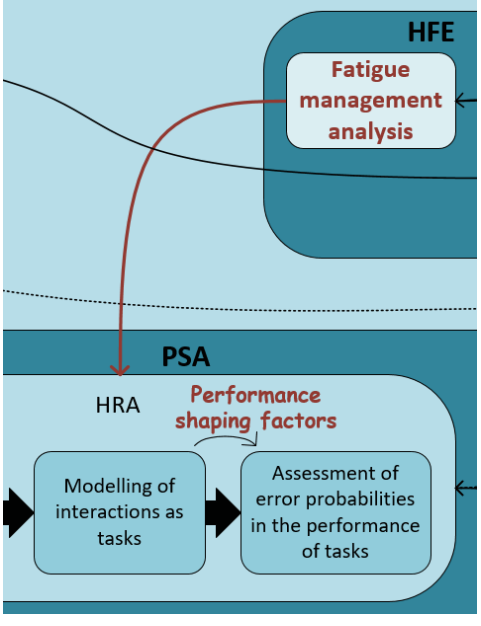

Fig. 6. Flow of information from HFE to HRA

Table 1. Failure probabilities and performance shaping factors for operator actions basic events.

Basic event	P(prior)	M(stress)	M(guidance)	M(training)	M(decision)	M(feedback)	P(posterior)
Plugging to internal water reserve	1E-4	0,5	0,2	0,5	2	5	5,0E-5
Plugging to external water reserve	1E-3	1	0,5	2	5	5	2,5E-2

5. Discussion on efficiency and integration of safety engineering process

Within the project the main research focus on the safety engineering practices is conveyed through the SEP requirement topics (as introduced in Chapter 3). Through the topics and the case studies, the different safety engineering practices of the participating partners are benchmarked, gaining insights and learning from the identified best practices. The aim is to provide support for fulfilling the selected requirement topics with methods and tools, while at the same time making way for more integrated and efficient safety engineering process between safety requirements, plant design and safety analyses.

The first SEP topic covers quite generally the management of safety engineering practices. It is seen as a high-level requirement, which encompasses the support and guidance needed for fulfilling the other requirement topics (and safety engineering in general). The BESEP approach for the safety engineering management, can be covered, for example, by the safety engineering management plan conceptualized in this paper. It will act, among other, as a high-level document supporting the planning and implementation of individual safety analysis disciplines and especially the integration between them.

The integration and interplay between analyses is covered by the second SEP requirement topic, and it can be approaches by specifying the needed information flow between the safety disciplines and the specific analysis. One attempt to visualize and further clarify the needed interaction points between them is given by flow of information diagram conceptualized in this paper. For the verification and validation of design topic, in the previous work (Immonen et al., 2022), the safety engineering process of the example case study was compared with the V-model approach by mapping the case specific safety requirements, analyses and plant design areas to the V-model widely applied in verification and validation processes.

Within the project BESEP, the plan is to cover all the other SEP topics as well, by providing similar concepts and examples and continuing to develop the current ones with the further insights gained as the benchmarking exercise continues. Some of these methods can cover, for example, using risk-informed decision making and graded approach.

6. Conclusion

This paper presents the midterm outcomes of the EU BESEP project. To further develop an integrated and efficient safety engineering process, the concept of Safety Engineering Management Plan has been introduced. In addition to SaEMP, flow of information diagram has been developed for the example case study. These safety engineering concepts and tools are examples of methods that could, after more detailed development, be used to achieve a best practice to fulfil the safety engineering requirements enabling efficient safety margins determination and safety requirement verification for nuclear power plants.

The information flow topic has been approached in more detail from the point of view of integration of HFE and PSA analyses. The use of HFE insights supports HRA development in the quantitative estimation of failure probabilities, especially through the specification of performance shaping factors such as stress and fatigue.

In future, the project aims to advance the concepts presented here, and introduce similar type of methods and concepts to the other safety engineering topics.

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

Alanen, J. & Salminen, K., (2016). Systems engineering management plan template - V1, VTT Research Report, Vol. VTT-R-00153-16, VTT Technical Research Centre of Finland. 90 p

Bell, J., & Holroyd, J., (2009). Review of human reliability assessment methods. Research report RR679. Norwich: Health and safety executive.

Immonen, E., Linnosmaa, J., Helminen, A. and Alanen, J. (2022). Benchmark Exercise on Nuclear Safety Engineering Practices. In M. Chiara Leva, E. Patelli, L. Podofillini, & S. Wilson (Eds.),

Proceedings of the 32nd European Safety and Reliability Conference (ESREL 2022) (pp. 1026-1033). Research Publishing Services.

Koskinen, H., Laarni, J., Norros, L., Liinasuo, M., & Savioja, P. (2021). Systems usability case in stepwise control room validation. Safety Science, Vol. 134, [105030].

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

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

Savioja, P. (2014). Evaluating Systems Usability in Complex Work – Development of a systemic usability concept to benefit control room design. VTT Science 2014, Aalto university, PhD thesis, VTT.