Advances in Reliability, Safety and Security, Part 8 – Kołowrocki, Magryta-Mut (eds.)
 ISBN 978-83-68136-20-3 (printed), ISBN 978-83-68136-07-4 (electronic)

Advances in Reliability, Safety and Security

ESREL 2024
Monograph Book Series

Benchmark Exercise On Safety Engineering Practices: Results And Recommendations

Atte Helminen[a], Essi Immonen[a], Joonas Linnosmaa[b], Jari Laarni[a]

[a] *VTT Technical Research Centre of Finland, Espoo, Finland*
[b] *VTT Technical Research Centre of Finland, Tampere, Finland*

Abstract

This paper describes the results and recommendations of the Euratom research project Benchmark Exercise on Safety Engineering Practices (BESEP). The role of safety engineering as a bridging element between plant-level systems engineering and discipline-specific safety assessments is discussed and studied through the variety of the performed benchmark exercises. Recommendations and preliminary results are presented under the three main topics of the project, which are the efficient and integrated safety engineering process, the closer connection of deterministic and probabilistic safety analysis and human factors engineering, and the creation of a graded approach. In addition, an example diagram of the nine main steps of efficient and integrated safety engineering is presented to visualize interconnections between safety analyses, and how the analyses contribute to the overall safety assessment and the verification of safety requirements.

Keywords: nuclear safety, safety engineering process, probabilistic safety analysis, human factors engineering

1. Introduction

This paper describes the results and recommendations of the Euratom research project Benchmark Exercise on Safety Engineering Practices (BESEP) that has been conducted between several European countries. The BESEP project and its first and midterm results have been introduced in the previous ESREL papers by the authors (Immonen et al., 2022, Immonen et al., 2023).

The BESEP project aims to develop best practices for the verification of stringent safety requirements against external hazards. The aim is achieved using an efficient and integrated set of safety engineering practices and probabilistic safety assessment. The efficient and integrated set of safety engineering practices supports the safety margins determination and safety requirement verification helping the licensing process of nuclear power plant new builds and upgrades.

BESEP is an on-going project and will soon be concluded. The final results and recommendations will be presented in one of the BESEP deliverables (EU BESEP, 2024) later in 2024. In this paper, some preliminary results and recommendations from the project are presented under three topics.

i) The first topic is the efficient and integrated safety engineering process. An illustrative example diagram to carry out an efficient and integrated safety engineering process is presented. The example diagram tries to encapsulate the key features and success factors identified in the benchmark exercise for the verification of evolving and stringent safety requirements of nuclear power plants against external hazards.

ii) The second topic is the closer connection of deterministic and probabilistic safety analysis and human factors engineering. A good level of coordination and supervision between the different disciplines of a safety assessment can greatly improve the effectiveness and usefulness of the safety engineering process. This can be supported, for example, by the creation of a multi-disciplinary team from various disciplines to establish a unified understanding of the accident scenario and relevant safety margins, and to support the efficient resource usage and definition of workflow between different safety analyses.

iii) The third topic is the creation of a graded approach. To promote efficient use of resources, the amount of effort to be spent on the analysis of accident scenarios should be structured and rigorous. The level of detail in the analysis and the deployment of more sophisticated safety analysis methods should be based on criteria such as risk significance, novelty, complexity, and uncertainty. To support this, a graded approach should be created and integrated as part of the efficient safety engineering process.

Before going to the results and recommendations, the theoretical features of safety engineering and its relationship to systems engineering and nuclear safety assessments are discussed from the project's perspective. Also, a brief recap to the benchmark exercise concept including a list of involved case studies in the benchmarking is described.

2. Systems engineering, safety engineering, and nuclear safety assessment

Traditionally, the nuclear industry has an extensive collection of safety analysis methods to take care of the safety requirements and analyze, evaluate, and justify the safety of the plant. Managing this interaction between the main elements of safety design (safety requirements, safety analyses, and plant design) is a complicated process that needs to be integrated across many disciplines, methods and processes. This integration is typically handled in safety engineering. Thus, efficiency can be seen coming from better safety engineering practice, which handles changes in any of the main elements of safety design. The continuous improvement principle of nuclear safety creates a need to develop each other element, and in case there is a change in one of the main elements, the change should be reflected in the two others. The aspects of safety integration were discussed in the authors' previous work (Immonen et al., 2022) and illustrated in Fig. 1.

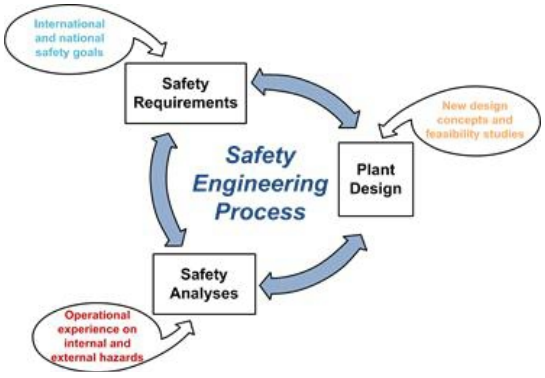

Fig. 1. Main elements of nuclear safety design.

During the project, a three-tiered approach to efficiently manage the plant's safety design was identified (depicted in Fig. 2). The approach is based on a structured and integrated interplay of three methodologies: Systems engineering, safety engineering, and safety assessments.

On the top level, there is systems engineering methodology, which is a holistic, interdisciplinary, and cooperative approach used for large systems over their entire life cycles, which is increasingly considered by many industrial sectors to address the daunting challenges to the development and utilization of modern systems caused by ever-increasing complexity in the face of acute competition and rising societal expectations. Systems engineering defines the common process framework applicable to different engineering domains. There generally exists several international standards describing the main components needed to develop and perform a well-structured systems engineering. Different systems engineering processes are described e.g., in ISO/IEC/IEEE 15288 Systems and software engineering — System life cycle processes (ISO/IEC/IEEE, 2023).

On the bottom level, there is the safety assessment, which include the conduct of different safety analyses. There is a great variety of plant and system-level analyses needed during the life cycle of the plant, including deterministic (DSA) and probabilistic (PSA) safety analysis and human factors engineering (HFE). Generally, the nuclear safety analyses are rather specific to the nuclear domain, for example, seismic analyses, level 1 PSA, level 2 PSA, etc., and are well-known only to the domain experts. An example on the safety assessment process for nuclear facilities can be found in IAEA Safety Standard GSR Part 4 – Safety Assessment for Facilities and Activities (IAEA, 2016).

What can be seen as currently lacking structure and guidance, or even missing, is the middle level, which is the connecting element between the whole plant engineering level and the safety assessments. In BESEP, we call this layer the safety engineering level, as it plays an integrating role between the plant design, safety requirements, and safety assessments. It helps the organization to carry out rigorous and comprehensive safety engineering. It can include, for example, a life cycle model, a description of safety engineering processes (e.g., requirement management, configuration management, and system analysis), the organizational model, and a selection of tools to implement the safety design principles in practice. Through these topics safety engineering layer will help to plan and manage the different safety analysis disciplines (i.e. DSA, PSA, and HFE), their interactions, and the interplay between safety requirements and plant design. (Immonen et al., 2022, Linnosmaa et al., 2021)

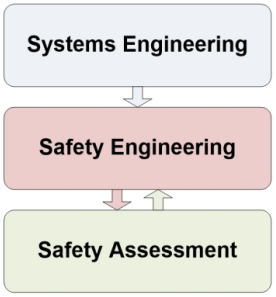

Fig. 2. A three-tiered approach to safety with Systems Engineering, Safety Engineering, and Safety Assessments.

Specifically for safety engineering purposes the current systems engineering guidance and standards are rather high-level and can be vague at times, as their purpose is to provide an overarching and interdisciplinary approach, which is needed for system-level coordination. On the other hand, the safety assessments give domain specific guidance focusing on the management of lower-level analyses. As proposed in (Immonen et al., 2022), safety engineering encompasses an extensive number of engineering activities essential for the safe operation of the plant. We see that the safety engineering process covers all the actions made during the plant's lifecycle that keep it safe to operate.

3. Benchmark exercise concept and case studies

The working method of BESEP project was a benchmark of case studies. Case studies were collected from partner organisations. In the benchmark exercise, the benchmarked case studies were subject to consecutive comparisons, evaluations, and improvements to reach a consensus on what the participants consider an integrated safety engineering process. This process of learning and improvement using structured and systematic evaluations of basically existing case studies was understood as benchmarking in the BESEP project (as opposed to performing a benchmark using pre-set, uniform initial and boundary conditions). Details of the benchmark process and one example case have been described in earlier papers (Bareith et al., 2023, Immonen et al., 2022). The final case studies included a variety of topics which were grouped according to safety requirements to be met, safety analyses performed, and similarities in external hazards or structures, systems and components (SSCs). The resulting groups of cases can be seen in Table 1.

The case studies were first compared within each of the groups to evaluate e.g., verification of safety requirements, assessment of safety margins as well as the role and interactions of safety analyses. Safety engineering approaches of the cases were also studied to identify success factors of integrated and efficient safety engineering processes. Secondly, the case studies in each of the groups were merged into a single representative case. The representative cases were further analyzed with probabilistic risk assessment methods to evaluate the balance between the spent efforts in safety verification, and the risk significance of the case study. Another aspect of the analyses was the quality of HFE contribution, including identification and treatment of human actions and tasks, dialogue of human reliability analyses and human factors engineering, and the evaluation of procedures. Together these comparisons provided answers for the three main topics of BESEP project: The integrated safety engineering process; closer connection of the PSA, DSA, and HFE; and the creation of the graded approach.

Table 1. Case studies.

ID	Case study topic
Structural Integrity – Requirement-based case study group	
1	Collapse of venting stack due to high wind
2	Probabilistic analysis of aircraft crash risk for NPP Dukovany
3	Loss of heat removal of spent fuel pool due to external impact
Loss of Ultimate Heat Sink – Safety function-based case study group	
4	Loss of ultimate heat sink (frazil ice or oil spill)
5	Loss of the service water system due to extremely low temperature
6	Blockage of (water) intake building
7	Evaluation of plant vulnerabilities to riverine events
Plant Vulnerability to Extreme Snow – Hazard-based case study group	
8	Extreme snow and wind affecting diesel generators
9	Protection of the reactor hall from the effects of extreme snow
10	Analysis of extreme snow for NPP Dukovany
External Impact on Safety Classified I&C Systems (SSC-based case study group)	
11	Loss of I&C due to high ambient temperature
12	Loss of on-site power supply and control due to lightning

4. Efficient and integrated safety engineering process

The concept of Safety Engineering Management Plan (SaEMP) was introduced in the previous ESREL 2023 paper (Immonen et al., 2023). SaEMP is a common planning and management document to guide and bring structure and integration to the safety engineering process. The diagrams and tools to support the efficient and integrated safety engineering process are presented in SaEMP. These can be, for example, accident sequence presentations, linking the accident sequences to safety analyses, V-model presentation, flow of information chart, etc. The diagrams help visualize interconnections between safety analyses, and how the analyses contribute to the overall safety assessment and to the verification of safety requirements.

Based on the learnings from the benchmark exercise and to endorse the SaEMP concept, an example diagram of an efficient and integrated safety engineering process is presented in Fig. 3. The purpose of the example diagram, and the safety engineering process in general, is not to replace the standard procedure of conducting the safety assessment of a nuclear power plant, but to support and complement the safety assessment. The safety assessments can be seen as the core technical activities performed within the safety engineering process to help to assess plants' safety level, decide on the need for modifications and/or corrective actions, as well as to assess the effectiveness of the implemented safety measures.

The assessment steps (ellipse steps) of the example diagram reflect the generally acknowledged phases of nuclear safety assessments. The assessment steps are complemented with additional steps (boxed steps) to expand the safety assessment process to cover the wider spectrum of the safety engineering process. Below, the different steps are briefly summarised.

In step 1, the safety engineering process is typically initiated by the identification of change. The change may be needed due to new regulations, design concepts, or operational experience (see the balloons of Fig. 1). Regardless of the source, the change is typically associated with one or more accident scenarios, which are then subject to study when estimating the impact of the change on the plant's safety design.

In step 2, the challenge to the plant's safety design is evaluated. Using the associated accident scenarios, the challenges the change imposes on the plant's safety margins or fulfilment of safety requirements are evaluated. Also, the urgency of the change needs to be evaluated. Some changes can evolve slowly, giving time for the safety engineering process to react to them, while some changes can be abrupt, putting extra stress on the performance and timing of the safety engineering process.

In step 3, an approximate safety assessment is performed to help decide on the continuation of the assessment of accident scenarios and the safety engineering process. In addition to continuing the assessment, it is possible to postpone the decision or to judge the change as irrelevant or insignificant. The postponing is often caused by an indication of insufficient data, which is needed to make a detailed and meaningful analysis so that more data needs to be collected to continue the process creating possibly an iterative loop into the step. The screening of a change

can be done as rule-based or risk-informed decisions. For the risk-informed decisions, the results of probabilistic safety assessment (PSA) are typically applied.

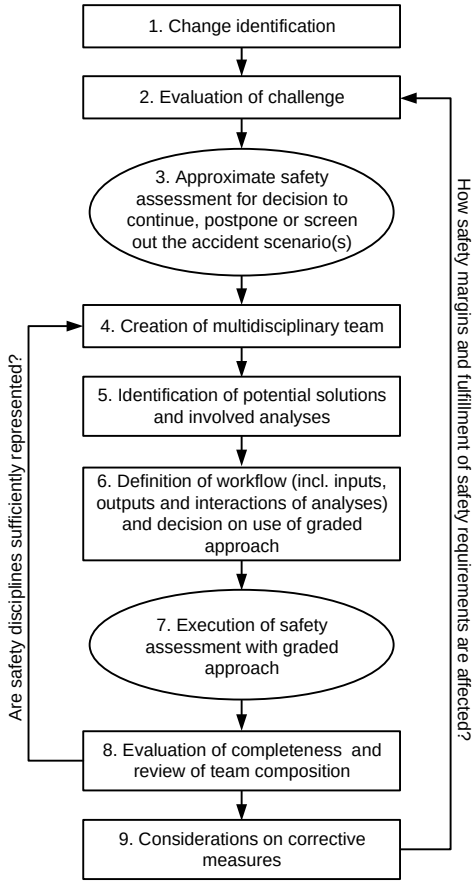

Fig. 3. Example diagram on the main steps of efficient and integrated safety engineering process.

After continuing with the assessment, a multi-disciplinary team is created in step 4. Experts from various disciplines are brought together to establish a unified understanding of the accident scenario. The team should have sufficient competence for the management of the safety engineering process.

In step 5, potential solutions are identified to respond to the change. Multiple potential solutions can be generated and conceived by the team experts involving different safety analysis disciplines (i.e. DSA, PSA and HFE). Each potential solution is accompanied by elements supporting decision-making, such as the quantity of resources needed and the risk reduction potential. In addition to the team experts' inputs, experience from (international) peers and sharing information with them is valuable at this stage. The impact of potential solutions to the acceptance criteria and different levels of Defense-in-Depth (DiD) is evaluated.

In step 6, the workflow and use of the graded approach are defined. The definition of workflow is most conveniently carried out in SaEMP. SaEMP includes example diagrams and suggestions for tools to support the requirements verification and the management of different levels of safety assessment and safety engineering process. The different levels were discussed previously in the ESREL 2022 paper (Immonen et al., 2022). For the use of graded approach, the tools and metrics of PSA can be applied.

In step 7, the safety assessment is executed following the potential solutions and SaEMP practices defined in the preceding steps. Depending on the complexity of the assessment, its uncertainties, and available assessment resources, a graded approach is applied to support the decision-making, multi-objective optimization, and risk estimation.

In step 8, the assessment completeness is evaluated by taking into account the sufficiency of expertise in the assessment team. The results are compared against the acceptance criteria and safety requirements to evaluate what kind of safety measures are necessary for the plant's safety design to respond to the change, which initiated the safety engineering process. In the evaluation, it is also important to recognize potential shortcomings in the expertise of a multi-disciplinary team. If the safety analysis disciplines have not been sufficiently represented in the assessment, it is possible to return to step 4.

In step 9, the corrective measures to improve the plant's safety design are considered. The measures should reflect the acceptance criteria and safety margins, and the fulfilment of safety requirements. If the measures are not in line with the evaluated significance of the change, it is possible to return to step 2. After step 9, the potential implementation of corrective measures is carried out. It is an own process itself, and not considered here.

5. Closer connection of deterministic and probabilistic safety analysis and human factors engineering

The ESREL 2023 paper (Immonen et al., 2023) gives an example on the closer connection of different analyses. In the example, the performance shaping factors (PSFs) of human reliability analysis (HRA), which is a specific analysis of PSA, feeds information to HFE and vice versa. Based on the experiences from the benchmarking exercise, it can be concluded that, even though, the value of HFE has been widely recognised, HFE's role in safety management needs clarification. There is a need for an integrated, holistic process to tackle human factors consistently and systematically in deterministic and probabilistic safety analysis activities. Especially, there should be an active dialogue between HFE and experts responsible for probabilistic analyses (PRA and HRA), since probabilistic analyses and HFE provide together a basis for implementing a risk-informed design program. For example, there is a two-way interaction between probabilistic analyses and some HFE analyses such as identification and treatment of important human actions. Similarly, HRA should provide input to planning of verification and validation activities, and the results of verification and validation should provide input, e.g., to the calculation of human error probabilities.

The role and the expected interactions of DSA, PSA and HFE should be defined at an early stage of the overall safety engineering process. Multi-disciplinary team on the safety analysis disciplines participating to the safety assessment should be defined early enough to allow efficient resource usage already at the planning phase. SaEMP reflects these aspects, and the necessary interactions are ensured throughout the process. Additionally, guidelines for conducting a complex assessment involving different safety analysis disciplines could be defined within SaEMP.

To further support and endorse the closer connection of safety analyses, it might be a good idea to introduce novel safety margin concepts to the field of nuclear safety. Typical safety margins of a nuclear power plant are, for example, the reactor power level and the pressure of reactor coolant boundary. However, to help prevent and manage nuclear accidents the human interactions have typically significance influence. The management of design basis events is included in the plant's safety design. Often these design basis events are controlled by automated systems without direct human intervention. For the beyond design-basis events the situation is more complex. Since it is difficult to create automated systems against most of these events, human participation is inevitable. Therefore, one step towards improving the integration of human actions in the plant's safety design would be to create novel safety margin concepts addressing human actions for the early intervention of accident scenarios.

These novel safety margin concepts would not be tied only to physical quantities but could also involve more abstract quantities and qualities. These more abstract safety margins could be associated, for example, with PSFs, e.g., workload, stress, fatigue and situation awareness that shape human performance in complex situations. These limits can be called psychological safety margins, of which the human operator can be more or less conscious. In PSA context, PSFs are studied when creating human reliability estimates for human actions included in the PSA model. Combining the quantitative features of PSA with the qualitative features of HFE would provide a fruitful breeding ground for novel safety margin concepts, which could help assess and credit the accident management of design exceeding external events.

6. Creation of graded approach

Overall, a graded approach is a structured method used to determine that resources and controls are commensurate with the risk level (e.g., IAEA, 2014). Resources and controls denote here the scope, level, and detailedness of analysis activities needed to comply with safety requirements. The graded approach means that more effort is put into those activities that have a larger impact on safety and productivity. 'More effort' means here that analyses are carried out more extensively, thoroughly and comprehensively.

One lesson learned in BESEP was that the approach for grading the amount of effort to be spent on analyzing accident scenarios should be structured and rigorous enough. In the beginning, some preparatory tasks have to be conducted. First, relevant criteria have to be selected for grading. In addition to expected safety significance, the selection of the level of analysis could be based on criteria such as novelty, complexity, and uncertainty. Second, we have to specify the number of grading levels. Regarding risk significance, the levels are associated with the potential consequences of the risks. The number of levels should be quite small; typically, three levels are a good choice. The third task is to determine analysis activities for each significance level. Examples of general analysis activities are listed in TE-1740 (IAEA, 2014, p. 12). In HFE, acitivities can be selected from the HFE program's review elements presented in NUREG-0711 (O'Hara et al., 2012).

The main idea is to apply a graded approach hierarchically and iteratively. Two levels of iterations are typically at least required: first, an overall level for control efforts is determined on the basis of risk significance; second, a more detailed assessment is conducted in which several other factors such as novelty, complexity, and uncertainty are considered. If several criteria are used, ratings based on the criteria are combined to specify the overall risk significance level of the scenario.

The risk matrix can be applied to identify the risk level of each activity/task, and suitable controls for the activity/task. The approach of using the risk matrix to map the risk significance of accident sequences against analysis efforts seems to be able to provide high-level guidance for effective resource allocation.

Careful application of the graded approach leads to a bounded safety engineering process in which appropriate analysis activities are conducted for the target system in accordance with their potential effect on safety (e.g., EPRI, 2021). The bounded approach thus ensures that our analysis efforts are in alignment with safety objectives, and our resources are applied in an effective manner.

7. Recommendations and conclusions

Some preliminary recommendations collected from the benchmark exercise, and from the BESEP project in general, are listed below. The list of preliminary recommendations are activities and concepts aiming to help in achieving an efficient and integrated set of safety engineering practices and probabilistic safety assessment to support the safety margins determination and verification of stringent safety requirements against external hazards.

Safety engineering process – Systems engineering defines a common process framework applicable to different engineering domains. The safety engineering process complements the standard procedure of conducting a safety assessment by introducing the common, and rather high-level, systems engineering process framework to the domain specific safety assessment. At the same time, a formal safety engineering process functions as the integrating layer between the plant design, safety requirements, and safety assessment.

Safety Engineering Management Plan (SaEMP) – A common planning and management document to guide and bring structure and integration to the safety engineering process. The diagrams and tools to support the efficient and integrated safety engineering process are presented in SaEMP. Additionally, guidelines for conducting a complex assessment involving different safety analysis disciplines could be defined within SaEMP.

Team building – In order to promote coordination and careful supervision of different activities, an expert panel should be established. The expert panel should perform its tasks in accordance with the Safety Engineering Management Plan. The panel should be made up of experts from different disciplines, and its leader should possess both technical and managerial skills.

Novel safety margins – The concept 'safety margin' should be seen from a wider perspective, and it would be necessary to better understand the complexities associated with it. For example, in order to better consider the impact of human actions on the accident management of design exceeding external events, novel, more abstract safety margin concepts are needed. The more abstract safety margins could be associated, for example, with performance shaping factors that alter human performance in complex situations.

Formal and systematic way of doing graded approach – To make the safety engineering process bounded and more effective, analysis activities should be tailored to fit the potential consequences of the risks at hand. The grading approach has to be structured and rigorous, and it should be applied in a hierarchical and iterative fashion. A risk matrix is a suitable aid in the identification of the risk levels of tasks and activities and in the selection of controls for them.

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 945138 (BESEP).

References

Bareith, A., Siklossy, T., Hlavac, P., Kovacs, Z. 2023. Grouping and Initial Evaluation of Case Studies for Integrated Safety Assessment in the European BESEP Project. Proceedings of 18th International Probabilistic Safety Assessment and Analysis (PSA 2023) (pp. 394-403). American Nuclear Society.

EU BESEP. 2024. Recommendation report on the utilization of more sophisticated safety analysis methods. Benchmark Exercise on Safety Engineering Practices. To be published.

Electric Power Research Institute (EPRI). 2021. HFAM - Human Factors Analysis Methodology for Digital Systems. A Risk-Informed Approach to Human Factors Engineering. 3002018392. Palo Alto, CA: EPRI.

International Atomic Energy Agency (IAEA). 2014. Use of a Graded Approach in the Application of the Management System Requirements for Facilities and Activities. IAEA-TECDOC-1740. Vienna: IAEA.

Immonen, E., Helminen, A., Linnosmaa, J., & Laarni, J. 2023. Benchmark Exercise on Safety Engineering Practices: Management Plan Concept. In 33rd European Safety and Reliability Conference, ESREL 2023 (pp. 684-691). European Safety and Reliability Association (ESRA).

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

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.

ISO/IEC/IEEE. 2023. IEC 15288:2023 Systems and software engineering — System life cycle processes. Geneva.

O'Hara, J.M., Higgins, J.C., Fleger, S.A., & Pieringer, P.A. 2012. Human Factors Engineering Program Review Model, NUREG-0711, Revision 3. Washington, District of Columbia: NRC.