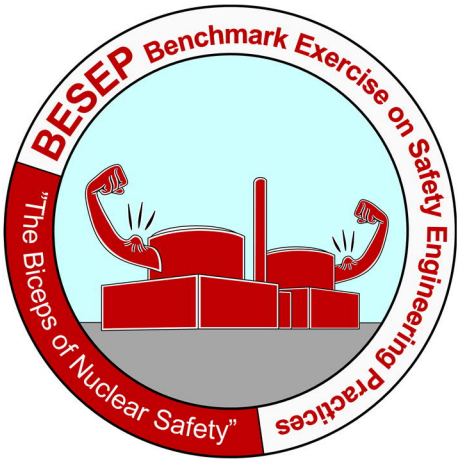
VTT Technical Research Centre of Finland

Specification on the key features of efficient and integrated safety engineering process: Deliverable 2.3

Linnosmaa, Joonas; Alanen, Jarmo; Helminen, Atte; Immonen, Essi; Holy, Jaroslav

Published: 01/08/2021

Document Version
Publisher's final version



BESEP

Deliverable 2.3
Specification on the key features of efficient and integrated safety engineering process

August 2021
Version 1.2

Public

Joonas Linnosmaa
VTT Technical Research Centre of Finland Ltd
P.O. Box 1000, FI-02044 VTT
Finland
joonas.linnosmaa@vtt.fi

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 945138.

Project acronym	Project title	Grant agreement No.
BESEP	Benchmark Exercise on Safety Engineering Practices	945138

Deliverable No.	Deliverable title	Version
D2.3	Specification on the key features of efficient and integrated safety engineering process	1.2

Type	Dissemination level	Due date
Report	Public	M12

Lead beneficiary	WP No.
VTT	2

Main author	Reviewed by	Accepted by
Joonas Linnosmaa	Carl Sunde, Elias Brådenmark	Essi Immonen

Contributing author(s)	Pages
Jarmo Alanen, Atte Helminen, Essi Immonen, Jaroslav Holy	48

Abstract

This report is the deliverable of the task 2.3, a specification on the key features of efficient and integrated safety engineering process in the scope of the BESEP project. Safety engineering processes in the scope of BESEP support the safety design of the plant, special focus given to the assessment of the safety margin. The project focuses on finding the most efficient safety engineering practices to support safety margins determination and safety requirement verification for design basis exceeding external hazards. This task supports the overall aim of the project by describing the basis of the safety engineering.

The report suggests basic properties related to a structured safety engineering process in the scope of systems engineering (and the related standard ISO/IEC/IEEE 15288). A high-level safety engineering process is described through different system engineering workflow models, like the V-model, consisting of the system structure, the system life cycle stages and the systems engineering workflow phases.

The safety engineering process is also approached from a different angle by describing the safety margins concept and the failure analyses. Safety margins in the context of deterministic, probabilistic, and human reliability analyses are defined. Failure analyses are discussed in the context of the safety margin verification and in regards with the interaction between safety analyses, such as deterministic and probabilistic safety analyses and human factors engineering.

The report identifies the key aspects of an efficient and integrated safety engineering process, listing them to be used in later tasks of the project.

Coordinator contact

Atte Helminen
VTT Technical Research Centre of Finland Ltd
P.O. Box 1000, 02044 VTT, Finland
E-mail: atte.helminen@vtt.fi
Tel: +358 20 722 6447

Acknowledgement

This project has received funding from the Euratom research and training programme 2014-2018 under grant agreement No. 945138.

HISTORY OF CHANGES

Date	Version	Author	Comments
15.7.2021	1.0	Joonas Linnosmaa, Atte Helminen, Essi Immonen, Jarmo Alanen, Jaroslav Holy	
12.8.2021	1.1	Joonas Linnosmaa, Atte Helminen, Essi Immonen, Jarmo Alanen, Jaroslav Holy	Changes due to comments.
31.8.2021	1.2	Joonas Linnosmaa, Atte Helminen, Essi Immonen, Jarmo Alanen, Jaroslav Holy	Peer review modifications.

LIST OF ABBREVIATIONS

BESEP	Benchmarking Exercise on Safety Engineering Practices
CDF	Core damage frequency
DBA	Design basis accident
DiD	Defence-in-Depth
DSA	Deterministic Safety Analysis
EU	European Union
FMEA	Failure mode and effect analysis
FSAR	Final Safety Analysis Report
HFE	Human Factors Engineering
HRA	Human Reliability Analysis
IAEA	International Atomic Energy Agency
I&C	Instrumentation and Control
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
ISO	International Organization for Standardization
LERF	Large early release frequency
NPP	Nuclear power plant
PSA/PRA	Probabilistic Safety/Risk Analysis
PSAR	Preliminary Safety Analysis Report
PWR	Pressurized water reactor
RCS	Reactor coolant system
SC	Safety Class
SE	Systems engineering
SSM	Swedish Radiation Safety Authority
STUK	Radiation and Nuclear Safety Authority in Finland
U.S.NRC	United States Nuclear Regulatory Commission
V&V	Verification and Validation
WP	Work Package
YVL	Finnish Regulatory Guide on Nuclear Safety

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1 Introduction

Development and utilization of large and complex systems, such as nuclear power plants (NPP), require a rigorous and a well-organised approach to keep managing the project in a safe and economically feasible manner through its long, now in many cases approaching 60 years, life span. As the pressure grows to get more value out of the resources available, the engineered plant systems become more numerous, ambitious, complex, and interdependent over the previous generation to achieve increased efficiency and performance. This can lead attaching to the original system a subsystem upon subsystem, immensely complicating the design. However, this increase in complexity through innovation cannot come at the cost of safety or security. This is supervised by the safety authorities by reviewing and assessing the fulfilment of plants' safety criteria. Over time, as more knowledge of the technical and physiological limitations of the systems, materials, humans, or environment becomes available, the safety criteria and requirements are updated to correspond with it. These changing 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 analyse, evaluate and justify the safety of the plant. 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 seen coming from better safety engineering practice, which handles changes in any of the main elements of safety design. NPPs are in a competitive environment, and meeting tight budgets and schedules is important to remain viable as an energy production source. New builds and modifications have struggled to meet these goals, and one reason for this has been the tightened safety requirements and thus the prolonged licensing period. To improve the situation, requirement management and plant design processes need to be integrated to work seamlessly together, and with the safety analysis methods. The robustness of the safety engineering practices is especially challenged in the case of sudden and significant changes in the safety requirements.

This raises the need for rigorous and well-organised approach for design and operation. Even though each EU member has its own country-specific nuclear safety requirements, which have led to different safety engineering practices, they still have the same goal of showing the fulfilment of the safety requirements in the plant design. This report explores the possibilities offered by systems engineering (SE). Systems engineering is a holistic, interdisciplinary and cooperative approach of large systems over their entire life cycles, which is increasingly considered by many industrial sectors as a mean 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. The main reference is ISO/IEC/IEEE 15288 (ISO/IEC/IEEE, 2015) standard, Systems and software engineering – System life cycle processes, which was published in 2015 to provide a common overall background and a common process framework. ISO/IEC/IEEE 15288 is applicable to any engineering domains, including the specialty engineering disciplines, such as safety engineering.

Project BESEP focuses on finding the most efficient safety engineering practices to support the safety margins determination and safety requirement verification for design basis-exceeding external hazards. The background is in the plant lifecycle model. The scope of Task 2.3 is to describe a safety engineering process and to identify the failure analyses involved and their interaction points. The outcome of this report is a specification of key features of an efficient and integrated safety engineering process.

The structure of this report is as follows. In Chapter 2, we introduce the safety design and safety engineering processes in the scope of the BESEP-project in top-down manner. Chapter 3 suggests a systematic approach to safety engineering through core systems engineering processes. The safety margin determination and assessment as a safety engineering activity are explored in Chapter 4. Chapter 5 discusses failure tolerance analysis in the scope of safety margin assessment. Chapter 6 gathers the key features of an efficient and integrated safety engineering process backed-up by the previous chapters. Conclusions are finally given in Chapter 7.

2 Safety engineering in BESEP project

2.1 Background

In Benchmark Exercise on Safety Engineering Practices (BESEP) project, the safety engineering processes of several countries are benchmarked to support safety margins determination and safety requirements verification against external hazards using an efficient and integrated set of safety engineering practices. The integrated set of safety engineering practices should be optimised to support all main elements of safety design. In this section, nuclear safety engineering in the context of BESEP project is defined. We start with a broader view to safety engineering in general and move towards the narrower scope of this particular project. This sets the background for our approach of the referenced safety engineering process.

According to the IAEA (IAEA, 2000): "*In relation to design, the safety provisions of the 'defence in depth' approach include: an adequate design for the site characteristics, multiple physical barriers to the release of radioactivity, and the application of strong safety requirements and proven engineering practices to ensure adequate safety margins and a high reliability of design features that preserve the integrity of these barriers*". As this definition, for example, describes, safety engineering encompasses an extensive number of engineering activities essential for running 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. Thus, the safety engineering process can be defined as a set of activities over the lifetime of a plant or a system aiming at assuring, that critical systems behave as required even in cases of failure. There are numerous international standards, guidelines, and requirements for covering all the manifold safety engineering activities like IAEA regulations, IEC/ISO standards and European Utility Requirements (EUR). Noteworthy are specific IAEA requirements defined in the Safety Standards and Nuclear Security Series publications. In addition to these, most countries have national regulators that have developed country-specific principles like the Finnish YVLs, Swedish SSM FSs and French RCCs.

Safety engineering is an overarching continuous process starting with the very idea of building a plant and ending to the commission of plant and the disposal of the used nuclear fuel. In this project, we focus 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. Our view to the main elements of safety design are shown Figure 1. As shown, we approach safety engineering process as an iterative way connecting together the main elements of safety design: safety requirements, safety analyses and plant design.

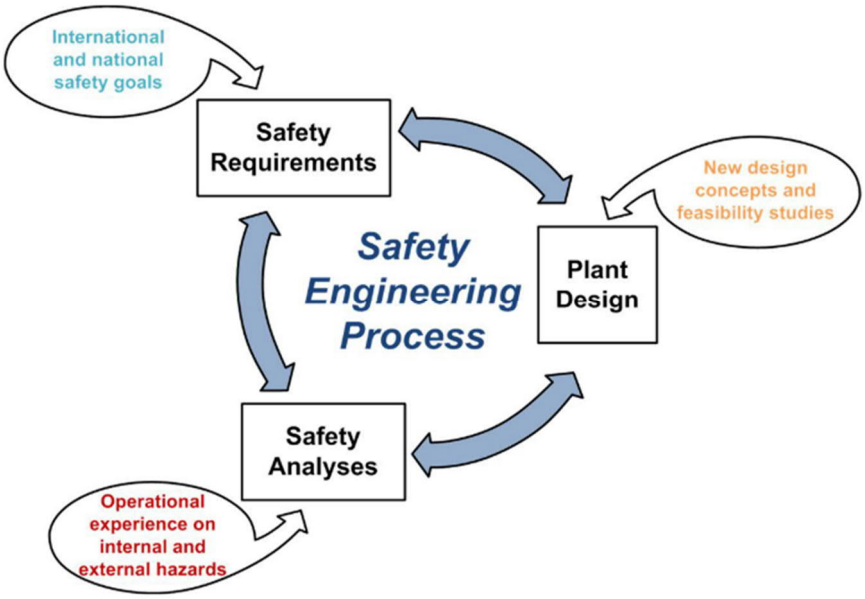


Figure 1. The main elements of safety design.

In an ideal situation, these three main elements should be in balance, and there is a general consensus, that based on the safety analyses the current plant design fulfils the given safety requirements. 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. Indeed, during the plant's lifecycle, there will be various changes to each element, as shown in Figure 1, 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.

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.

In addition to focusing on the design phase, we will further limit our scope to the system analysis activities, specifically on the assessment of safety margins (safety margins are further discussed in Chapter 4). The most important of system analyses regarding the safety engineering process of safety margin assessment are the analyses focusing on safety, shortly safety analyses. Traditional nuclear safety analyses can be categorised 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 between the different safety analyses and the other two main elements of safety design. The safety engineering process is, therefore, not only limited to the main elements of safety design (plant design and safety requirements), but it has an important role also in ensuring the information flow and utilisation inside each element. The situation is illustrated for the safety analyses element in Figure 2.

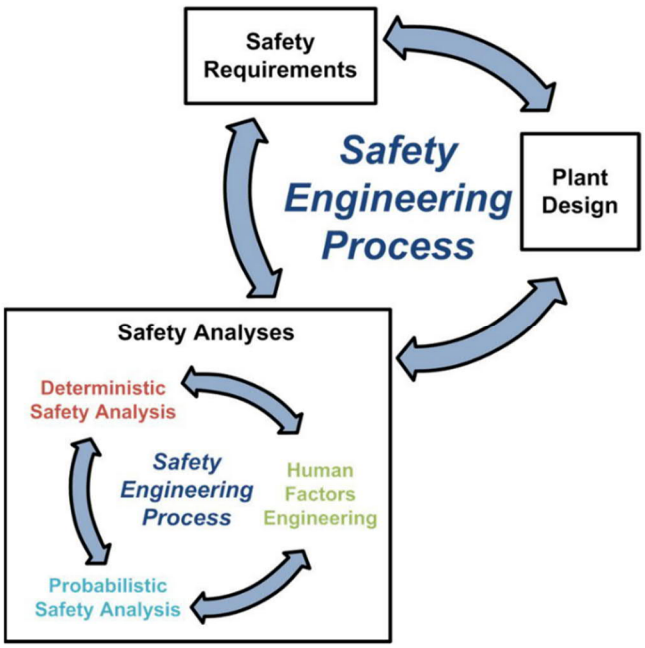


Figure 2. The safety analyses element of safety design.

The benchmark exercise, which is carried out in the later tasks of the project, is executed in the comparisons of several, different case studies. The case studies evaluate the fulfilment of safety requirements based on the results of involved safety analyses, which can be from different safety analysis areas and may include different methods. The safety requirements for the benchmarking, also called as BESEP requirements, have been initially defined in Task 2.2 (Rein, 2021). One focus area for the comparison is the safety margin assessment (and associated failure tolerance analysis) carried out in the case studies. The overall objective of BESEP project is to develop best practices for safety requirements verification against external hazards using efficient and integrated set of Safety Engineering practices and probabilistic safety assessment.

For this purpose, it is important to identify the different methods involved in the different safety analysis areas (i.e. DSA, PSA and HFE) 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. The situation is illustrated in Figure 3.

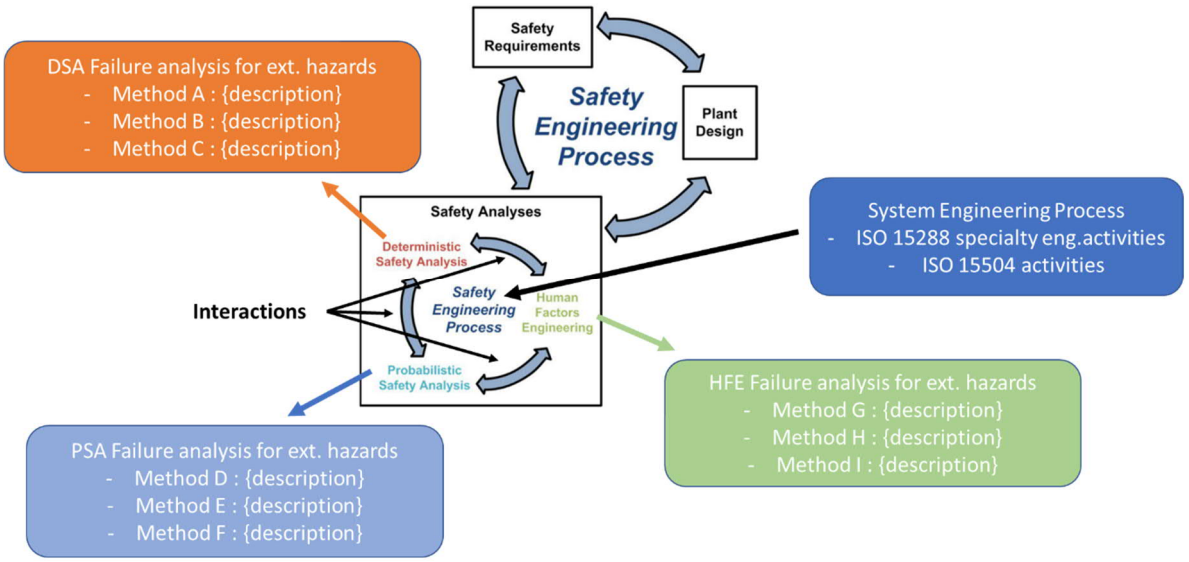


Figure 3. Methods involved in safety analysis areas and their interactions.

The most relevant system engineering standards for the project are discussed in detail in Chapter 3. Safety analyses regarding the safety margin assessment are discussed in Chapters 4 and 5.

2.2 Safety engineering topics in BESEP

The benchmark baseline of BESEP is defined within the Work Package 2 (WP2 - Benchmark baseline). WP2 contains the following main tasks:

- Task 2.1 Assignment of safety requirement topics for selected external hazards
- Task 2.2 Creation of benchmark baseline by definition of detailed safety requirements
- Task 2.3 Specification of key features of efficient and integrated Safety Engineering Process (deliverable: this report)
- Task 2.4 Identification of general risk significance thresholds of external hazards.

Relevant to this deliverable, during the work on Task 2.2 a set of requirement topics related to safety engineering was developed/listed to support the creation of the requirement baseline. The topics and short descriptions on the focus of each topic are given below. The presented list is not trying to be a comprehensive representation of safety engineering topics. The purpose is to identify safety engineering topics of interest supporting the benchmark and the objectives of BESEP project.

1 **Safety engineering management,** this topic concerns the processes and models regarding the general structured management of safety engineering activities of NPP license holders;

2 **Safety design and requirement management for external hazards**, this topic concerns managing the balance between the plant safety design and the allocated safety requirements;

3 **Flow of information between safety analyses**, this topic concern interactions and interconnections between the three analysis areas (DSA, PSA, HFE);

4 **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;

5 **System modification and configuration management,** this topic concerns system modification configuration management;

6 **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.

3 Systematic approach to safety engineering

3.1 Safety engineering through systems engineering

Safety engineering can be thought as a slice of the overall systems engineering, which can be defined to be systematic safety related engineering of a system through its whole life cycle. The most popular systems engineering base standard is ISO/IEC/IEEE 15288 (ISO/IEC/IEEE, 2015). It defines the systems engineering processes depicted in Figure 4.

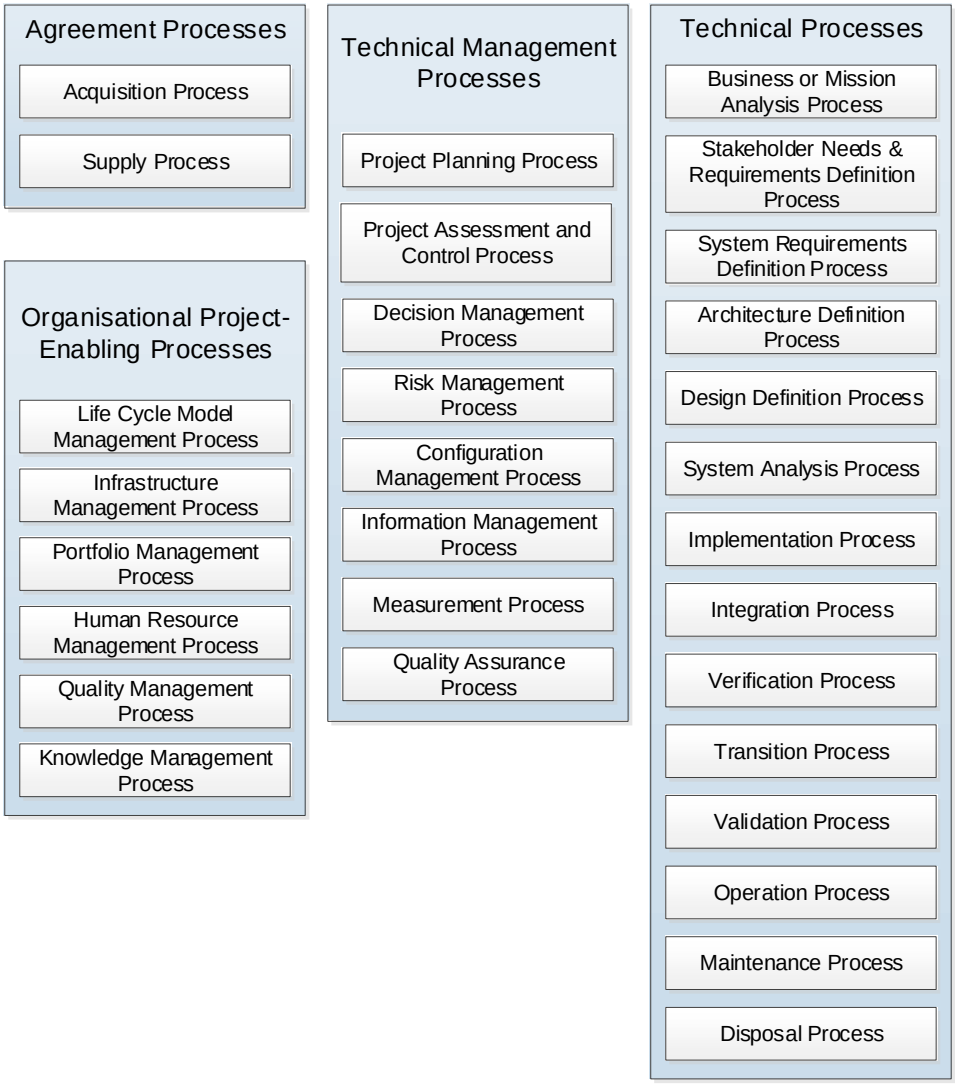


Figure 4. ISO/IEC/IEEE 15288:2015 systems engineering processes.

Another important aspect of ISO/IEC/IEEE 15288 is its model of a **system structure**: A System-of-interest consists of System Elements; a System Element can be a sub-system or an atomic component. From the point-of-view of the producer of a system element, that system element is the System-of-interest, which again can consist of System Elements, i.e. of sub-systems and components. The system structure thus introduces only two modelling elements, System and System Element. The same set of ISO/IEC/IEEE processes presented in Figure 4 can be applied in all the hierarchy levels.

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 organised 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, utilisation, support, and retirement. The fact that utilisation and support are named as different life cycle stages suggests that the life cycle model behind it is not linear, and, in fact, ISO/IEC/IEEE 24748-1 (ISO/IEC/IEEE, 2018), a daughter standard of ISO/IEC/IEEE 15288, presents an iterative life cycle model with the particular life cycle stages listed above. We do not advocate iterative life cycle models, but require the life cycle model to be linear, i.e. the system cannot go back in time, not even in the recall cases in which the infancy SE processes are applied again; in such cases an additional, unexpected, life cycle stage is added. Hence, we define here a generic linear life cycle model with the following stages: *concept, development, implementation, deployment, operation and support, and retirement*; see Figure 5 below.

Figure 5. A generic, linear, system life cycle model.

An NPP I&C systems life cycle model is depicted in Figure 6. The life cycle model is created based upon the Finnish YVL B.1 [STUK 2013a], YVL E.7 [STUK 2013b] and YVL D.4 [STUK 2013c] and the life cycle concepts presented in (Alanen and Salminen, 2016).

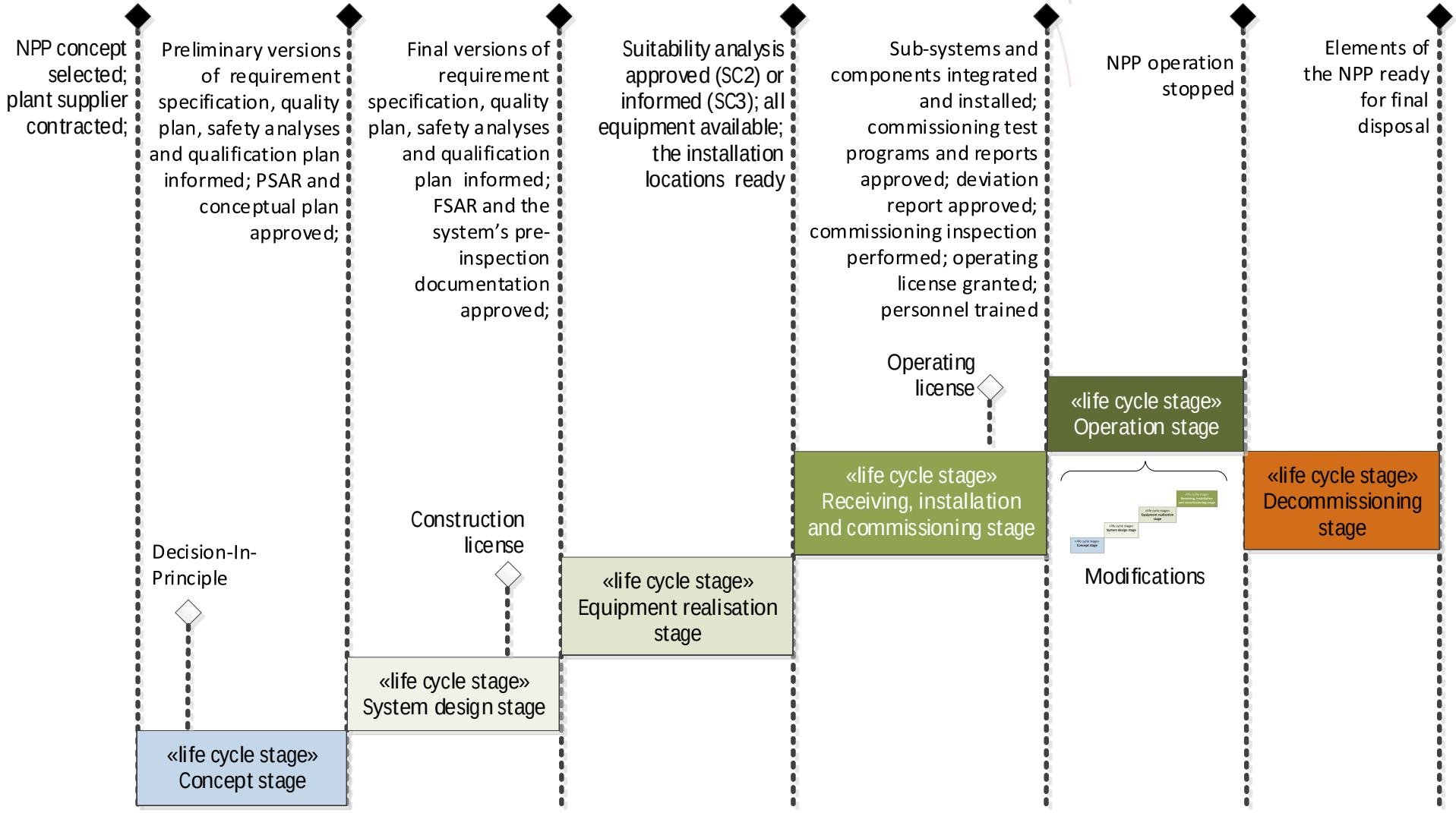


Figure 6.NPP system life cycle model. (The empty diamonds denote the licensing milestones of the whole NPP facility.) Modified from (Alanen and Salminen, 2016).

ISO/IEC/IEEE 15288 does not explicitly define the **systems engineering workflow** either, i.e. the order of activities of the processes, but it only defines the processes, their activities, and their tasks. Typically, the systems engineering workflow is represented as a V-shape model called V-model. A good example of a V-model representation is provided in Figure 7.

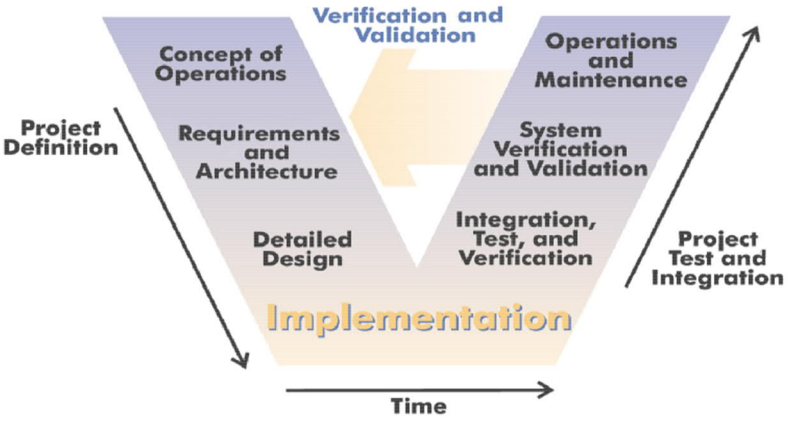


Figure 7. A V-model example (Osborne et al., 2005)

The particular example in Figure 7 quite well follows the order of technical processes of ISO/IEC/IEEE 15288 as depicted in Figure 4, but the 'waterfall' model (as V-model also is) is not required by ISO/IEC/IEEE 15288. The systems engineering workflow is, in practise, more iterative, see for example Figure 8.

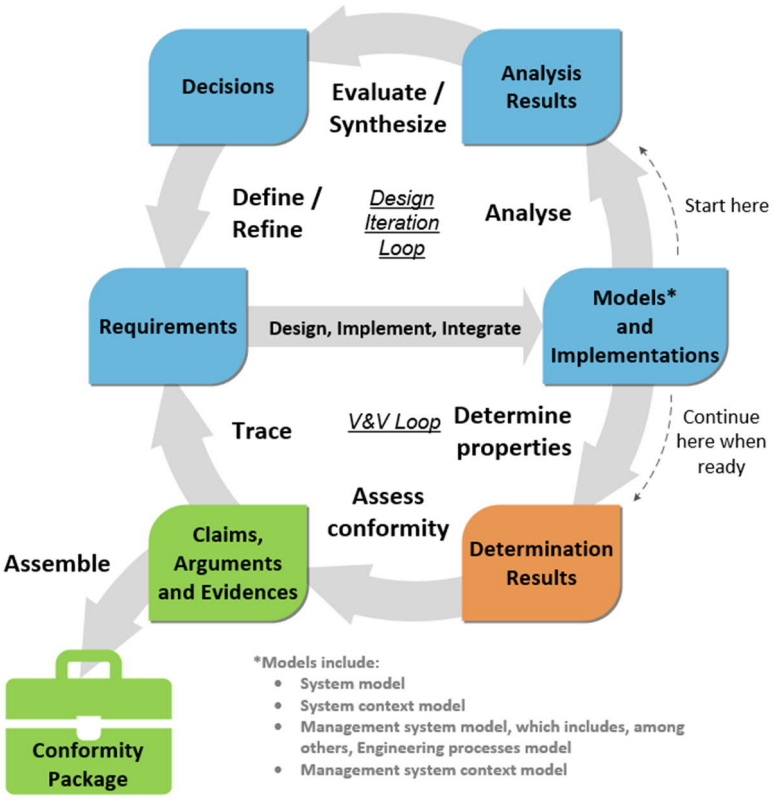


Figure 8. Systems Engineering core activities and artefacts within design iteration loop and Verification and Validation loop (1st party conformity assessment loop); 'determination' means testing, analysis, review, etc.; an update of (Alanen, Linnosmaa and Tommila, 2017).

The process flow in Figure 8 continues with third party, such as nuclear regulators, activities to qualify the system-of-interest; see Figure 9.

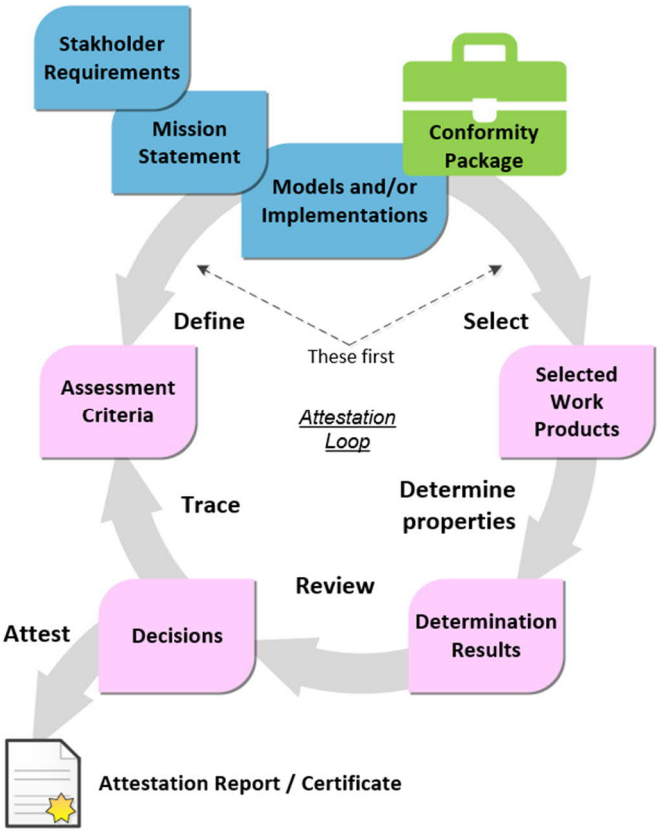


Figure 9. Systems Engineering core activities and artefacts within attestation loop (3rd party conformity assessment loop); an update of (Alanen, Linnosmaa and Tommila, 2017).

Whatever the model of the systems engineering workflows is, waterfall, iterative, agile, etc., it is up to the organisation to allocate the relevant ISO/IEC/IEEE 15288 tasks to:

- the system structure (hierarchy)
- the system life cycle stages
- the systems engineering workflow phases.

This means that, for example, the V-model in Figure 8 may be manifested at different system hierarchy levels and in different system life cycle stages, although it best fits only to concept and development life cycle stages.

Furthermore, also the enabling systems are engineered by the systems engineering processes. Enabling systems typically are the following: Concept System (the system to create concepts of the system-of-interest), Development System, Production System, Support System, and Retirement System. (ISO/IEC/IEEE, 2018)

In this context, we do not try to cover the whole Systems Engineering realm, but focus on things relevant to BESEP; see Section 3.4 for details about the focus.

3.2 Specialty engineering process view from ISO/IEC/IEEE 15288

We selected the ISO/IEC/IEEE 15288:2015 standard to be our reference model for the Systems Engineering (SE) processes. It was selected because it is the most popular SE standard in use and is selected by IAEA in the upcoming IAEA technical report on Systems Engineering (IAEA, 2021).

ISO/IEC/IEEE 15288 introduces in its Annex E a concept called 'Process views'. The concept allows engineers to pick up process activities and their tasks from the pool of ISO/IEC/IEEE 15288 processes for the engineering theme of their concern. Typically, such needs come from the speciality engineering areas, such as safety engineering, security engineering, dependability engineering, usability engineering and environmental sustainability engineering. ISO/IEC/IEEE 15288 provides a list of specialty engineering process view activities. In this context, we can use that list as a reference model for the nuclear safety engineering process we aim to provide in this project. The list of specialty engineering processes, their activities, and their tasks is supplied in Appendix A Table 2 with indication about the relevant tasks in this context. Detailed descriptions about the

processes, activities and tasks is supplied by ISO/IEC/IEEE 15288. Appendix A works as a checklist to ensure that the safety engineering process we define in Section 3.4 covers all the relevant activities.

To complement the ISO/IEC/IEEE 15288 speciality engineering processes, we also introduce three safety engineering focused processes provided by ISO/IEC TS 15504-10:2011 (ISO/IEC TS, 2011). The processes with their task are listed in Appendix A Table 3. Developing safety-related systems requires specialized processes, techniques, skills and experience. Thus, ISO/IEC TS 15504-10, presents additional safety amplifications to ISO/IEC/IEEE 15288 in forms of safety extensions in the areas of safety management, safety engineering and the safety qualification.

In Appendix B, we introduce a tool for assessment of capability to provide suggestions and hopefully helpful references as to how to evaluate the safety engineering processes of the organizations participating in the benchmark exercise. It can also be used to create assessment criteria in other tasks of the BESEP project.

Furthermore, typically to nuclear domain, there are two additional processes, Qualification process and Licensing process. In this report, we will not elaborate the Licensing process and Qualification process; further details about them can be found in (IAEA, 2021) and (Alanen and Tommila, 2016) respectively.

3.3 Systems engineering management

Based on the studies by (Honour, 2013), the optimum level of Systems Engineering (SE) effort is about 14 % of the total costs of median sized engineering projects. The results of the studies by (Elm and Goldenson, 2012) indicate that "*For lower challenge projects, although SE improves the likelihood of project success, success remains somewhat feasible without good SE deployment. For higher challenge projects, good SE deployment is critical to project success*". Definitely, large NPP projects fall to the category of 'higher challenge project', even 'complex projects'. Hence good systems engineering deployment and management is highly relevant also in case of NPP safety engineering. But as systems engineering is quite a formal engineering method, it also adds complexity. Nevertheless, Niklas Luhmann, a sociologist, philosopher of social science and systems theorist has said: "Only complexity can reduce complexity". Hence, we believe that formal systems engineering provides a good return on investment (ROI) in achieving the NPP program goals. To achieve the SE benefits, it is important to manage the systems engineering program well to make it fluent and effective.

The systems engineering management cornerstones are the following: the system lifecycle model, the process model, the organisation (roles) model and the set of engineering management tools (see Figure 10). Our focus in this context is in the systems engineering process model.

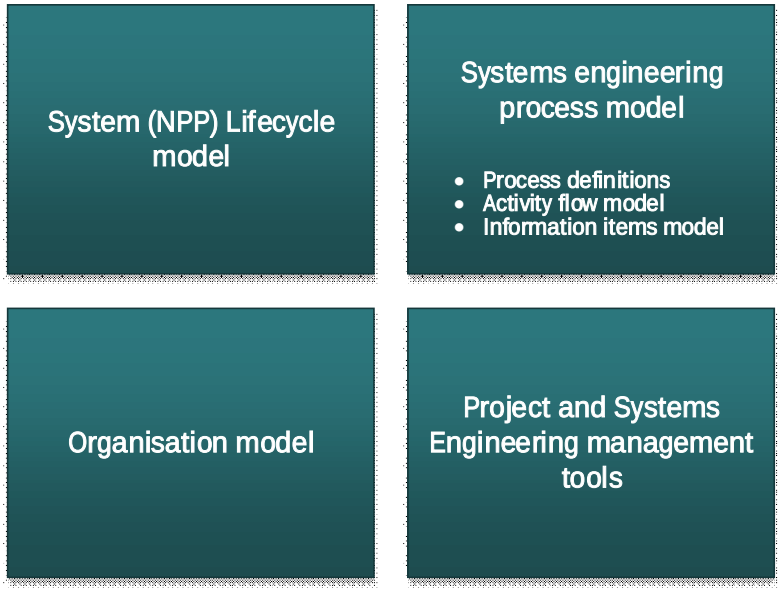


Figure 10. The cornerstones of systems engineering management.

The **lifecycle model,** and an example of it in case of NPP I&C systems, was discussed in Section 3.1.

The **systems engineering process model** consists of the definitions of processes, their activities, and their tasks to carry out the engineering work. As presented in Section 3.1, ISO/IEC/IEEE 15288 provides a good

reference model for this. The process model shall also define the systems engineering flow, such as a V-model, iterative or other. The process model shall also include the information items model. The information items model consists of descriptions for the engineering work product types and their relations. Typically such work products are word processing documents, but we aspire more structured, model-based, work product repository by defining ontology based data models for systems engineering artefacts (Tommila and Alanen, 2015; Alanen, Linnosmaa and Tommila, 2017); we call this model SEAModel (Systems Engineering Artefacts Model).

The **organisation model** is vital to optimally allocate and utilize the human resources. The model shall address at least the following:

- well-defined roles (like systems engineer, requirements engineer, etc.)
- well-defined communication and collaboration model (to facilitate consistent view in all involved organisations on the goal, data and state of the development).

Project and Systems Engineering management tools are the interface between the engineers and the systems engineering program. If the tools are not engineer friendly, the engineers will soon start to dislike the whole systems engineering philosophy and will stop following the formal systems engineering processes. Hence to effectively carry out systems engineering, well-planned use of project management and systems engineering tools is a necessity. It involves at least the following:

- a good selection of tools (model-based tools advocated)
- a flexible tool integration model (to allow integration of various tools used by the collaboration partners)
- a tool to orchestrate all the systems engineering work (such as a PLM tool).

All the four success factors presented in Figure 10 above are reflected to all the engineering disciplines, such as requirements engineering, configuration management, safety engineering, and other.

3.4 Focus of the proposed safety engineering process for nuclear power plants

As stated in Sections 3.1 and 3.2, we do not try cover all ISO/IEC/IEEE 15288 systems engineering processes, not at all NPP hierarchy levels, and not for all NPP life cycle stages. We narrow our scope as follows:

- We concentrate on development stage,
- We concentrate on the nuclear power plant on the plant level (we do not focus on sub-systems, such as instrumentation and control (I&C) architecture, nor do we consider the enabling/supporting systems),
- We concentrate on safety engineering,
- We concentrate on the following systems engineering processes:
    - system analysis (especially safety analyses)
    - requirements definition
    - architecture design
    - detailed design
    - implementation
    - integration
    - system verification
    - system validation
    - information management
    - and decision management.

Note that we do not narrow our scope to external events due to the fact that the safety engineering processes defined at the level provided by ISO/IEC/IEEE 15288 do not take a stand on selection of the safety analysis tools and methods for different types of hazards.

Figure 11 depicts our scope.

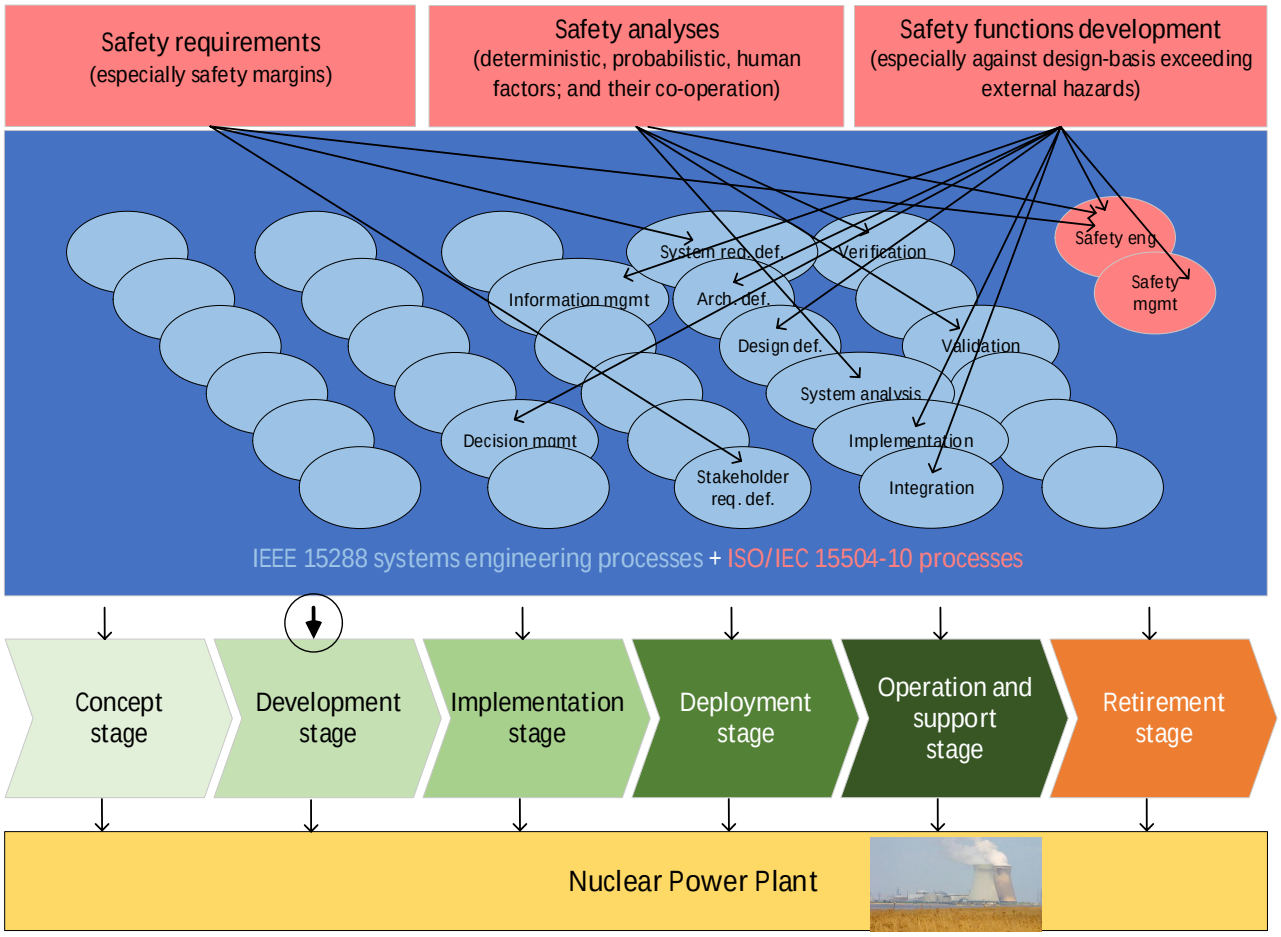


Figure 11. BESEP project scope of the safety engineering process.

To carry out the safety engineering activities in a sequential or iterative matter, the companies need to define their own engineering flow model. In Figure 12, an overall engineering workflow model by Fortum (Nuutinen, Sipola and Rantakaulio, 2017) is illustrated.

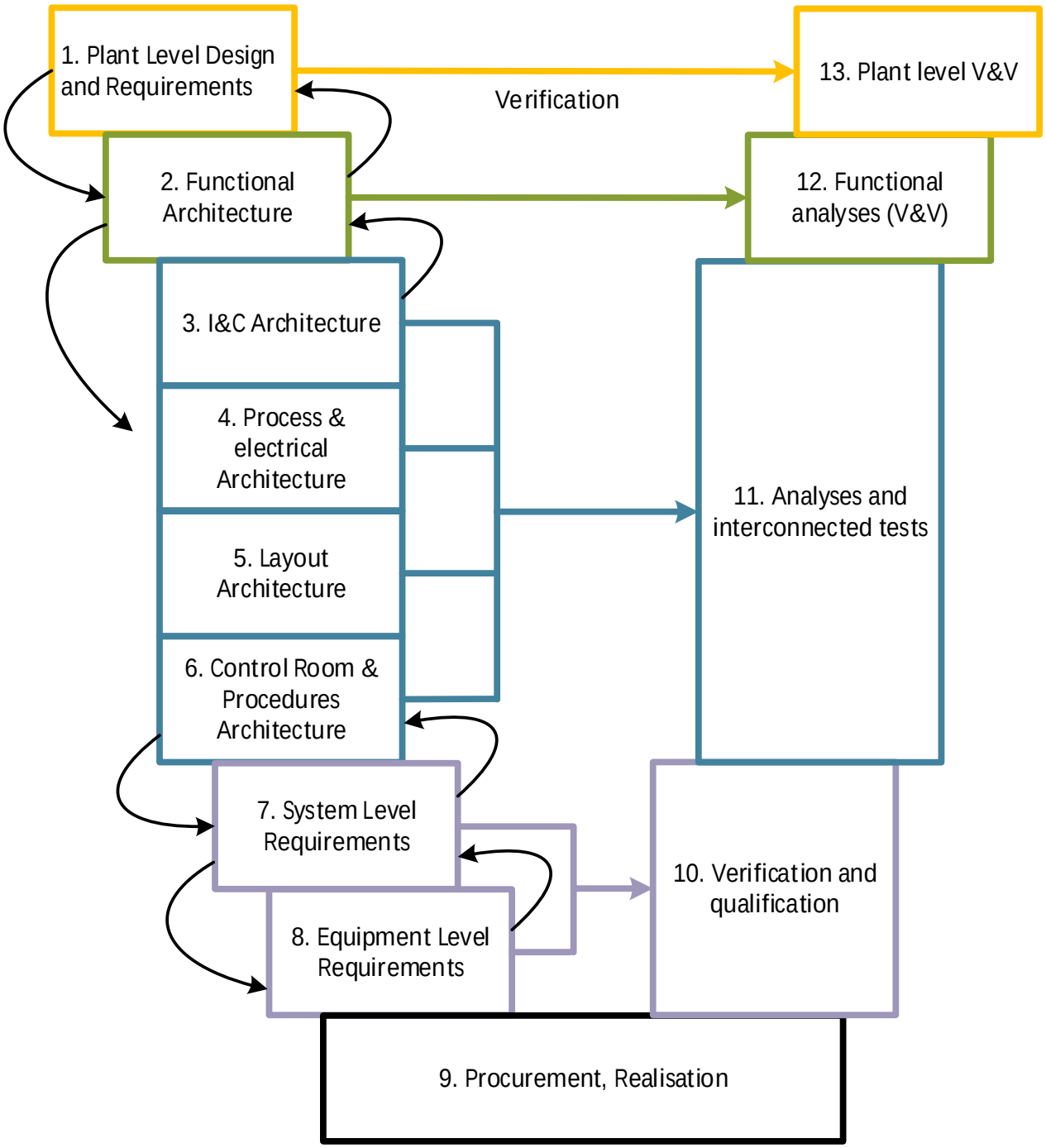


Figure 12. NPP V-model by (Nuutinen, Sipola and Rantakaulio, 2017).

We will use the V-model of Figure 12 as a reference model to allocate the safety analysis activities presented in Chapter 5 to the different engineering workflow steps. (Therefore, we have numbered the workflow steps in Figure 12). Nevertheless, below in Figure 13 another V-model by Fortum is provided to illustrate the overall mapping of safety analyses to the different levels of the design activities.

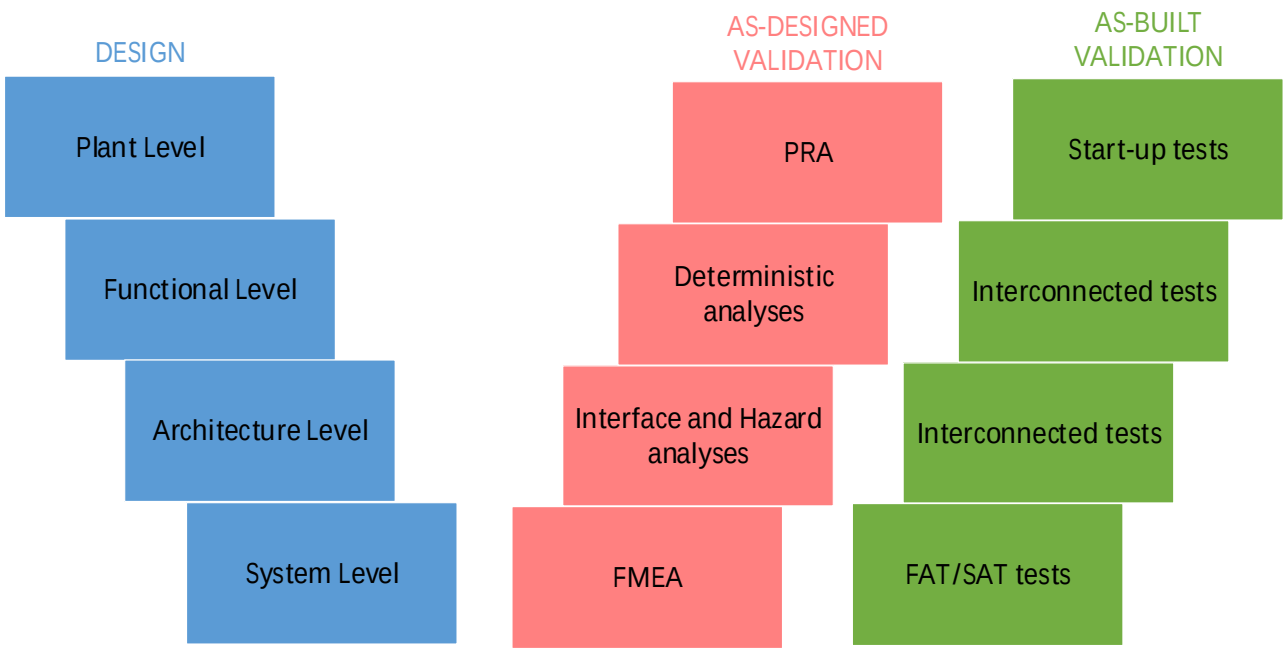


Figure 13. NPP V-model by (Nuutinen, Sipola and Rantakaulio, 2017).

The safety engineer process we define here is at an abstract level; we define the processes, but not the work flow (except by presenting the iterative work flow examples in Figure 8 and Figure 9, and the V-model examples in Figure 7, Figure 12 and Figure 13), neither the information ontology, but we stick to the level that is relevant for the process capability assessment; and we suggest the method of Appendix B as the capability assessment tool. The other way around would have been to define a theoretically optimum workflow and information ontology, but it would have needed to be tested in a real industrial context, before it could have been used in BESEP as a reference model of the safety engineer process. The abstract level has the advantage, that it enables evaluation of different kinds of engineering practises (such as workflow and information management) and cultures.

4 Safety margins assessment

4.1 Safety margin concept and load-strength interference

As pointed out in (Hrehor et al., 2007), the concept of safety margin is not exclusive to the nuclear industry. The concept of safety margin has been formalized through the work on load-strength interference developed in civil engineering applications, where a safety margin is typically connected to the probability of failure and referred as “margin to damage”. In the nuclear industry, the term “safety margin” is more commonly applied. IAEA (IAEA, 2003) defines the safety margin as “the difference or ratio in physical units between the limiting value of an assigned parameter the surpassing of which leads to the failure of a system or component, and the actual value of that parameter in the plant”. Therefore, in comparison to the margin to damage where an inference is drawn directly from the failure distribution of a system or component, the safety margin sets special emphasis on a predefined limiting value and on the exceedance of this limiting value.

In the load-strength interference of traditional structural-mechanics analyses, the load L is described by a probability density function that captures all the variabilities expected during the operation of the system. The strength S, or sometimes called capacity or resistance, represents the probability density function obtained when the system is tested to failure a sufficiently large number of times or by evaluation of other statistical methods.

Recognizing the fact that both load L and strength S are parameters with uncertainties described by probabilistic functions, the bases for the general definition of margin to damage can be formed by the interference of these two distributions. The situation is illustrated in Figure 14. Probability densities for load and strength of safety variable. Two distributions usually overlap each other, but for clarity reasons they are drawn separate in the figure.

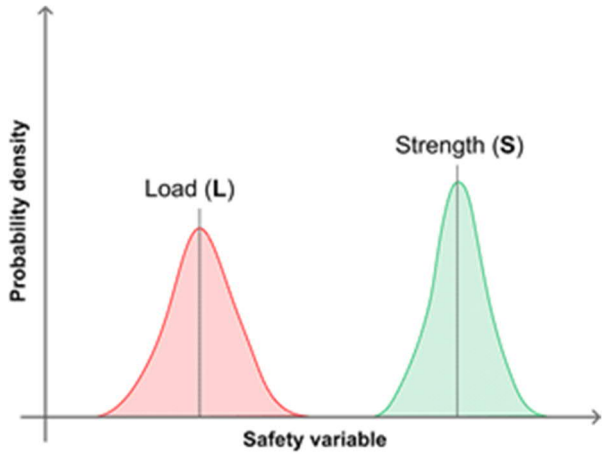


Figure 14. Probability densities for load and strength of safety variable.

Given sufficient information on the load, strength and their standard deviations, the safety margin can be estimated with sufficient level of confidence. However, such information is often difficult and expensive to obtain even for a relatively simple system. Not to mention, for a complex system ensemble involving human interactions. Therefore, instead of calculating the actual probability of failure for structures, systems and components, nuclear industry leans more on examining the probability of exceeding the safety limits set in a two-phase approach described in (Hrehor et al., 2007) and summarised below.

The first phase of ensuring adequate safety margin is to set safety limits such that the probability of loss of function is negligible, so long as operating conditions stay within defined criteria. One or more safety variables can be used for characterising the operating conditions. Good examples of safety variables are the integrity of reactor coolant system (RCS) boundary or the functioning of specific safety systems. The left side of Figure 15 illustrates this concept.

The second phase of ensuring adequate safety margin is to keep operating conditions within safety limits. The load is the probability density function obtained in a particular scenario for the safety variable by propagating contributing uncertainties. The right side of Figure 15 illustrates this concept.

Since the distributions of load and strength parameters often overlap, one of the goals in the safety limit setting and the consequential safety analysis is to show that such overall overlap is very small producing negligible risk to the plant.

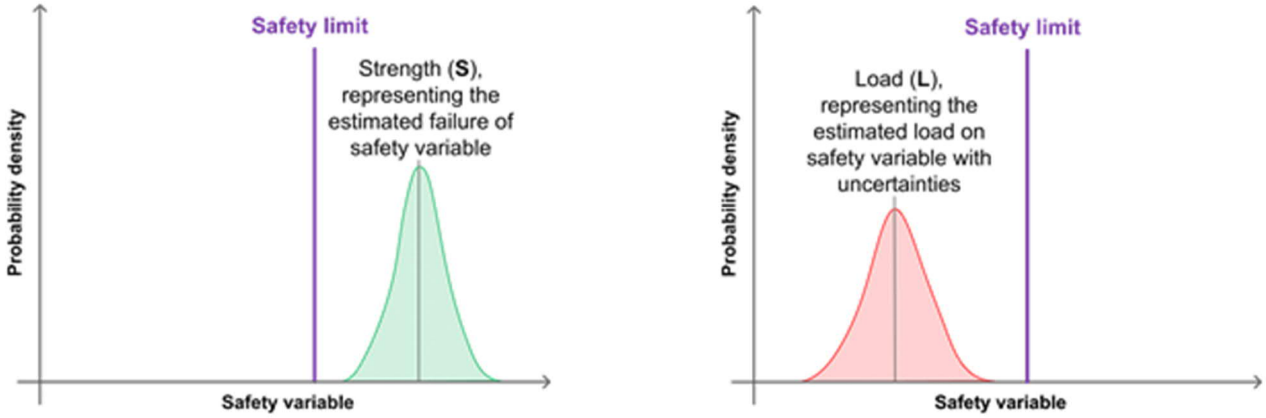


Figure 15. Setting safety limit and keeping operating values below the safety limit.

A safety margin concept is applied explicitly to either barrier or system losses. Therefore, in a complex facility like a nuclear power plant and a complex situation like a design-basis exceeding external event there will be as many safety margins as barriers or systems whose loss is considered to be a safety problem. This requires to clearly define the concept of a safety variable, and how safety variables relate with barriers or system function losses. Whether the loss of a particular system or barrier is a safety problem or not, depends on the possible accident scenarios and their expected consequences. Since the ultimate goal of nuclear safety is to prevent unacceptable radiological releases to the public or to the environment, safety limits and margins should

be considered at least for those systems and barriers whose failure could potentially contribute to unacceptable radiological releases.

Conceptualisation and calculation of margins for safety variables composed of several safety margins from different structures, systems and components is not generally feasible for the deterministic approaches. The best way of obtaining representative values on the total safety status, and therefore on the safety margin, of a nuclear power plant has to be done by probabilistic terms using risk analysis approaches. Distances to different risk limits can give insight regarding the total safety margins of the plant. This also allows ranking different safety issues against each other. (Cronvall, 2016)

4.2 Deterministic safety margins

The safety limits are usually conservatively set below the probability density functions of strength parameters described above. The setting of safety limits are typically based on the common understanding of scientific community reinforced with physical experiments when applicable. For design basis accidents (DBA), acceptance limits, or criteria, are stipulated by national regulatory bodies. These regulatory acceptance criteria may be the same as the safety limits or more restrictive. Therefore, for practical purposes the safety margin is usually understood as the difference in physical units between the regulatory acceptance criteria and the results provided by the calculation of the relevant plant parameter. The deterministic safety margin can be expressed as a value indicating the difference or as a ration of capacity to load.

In the licensing of a nuclear power plant, the acceptance criteria are challenged by calculating the plant parameters with conservative assumptions. In these calculations, the licensee has to provide analytical and experimental evidence to the regulatory body that the acceptance criteria are fulfilled with sufficient margins. If the safety margins are not satisfied in the conservative assumptions, the analysis may be complemented by best estimate calculations with uncertainty analysis to assure to be below the regulatory acceptance criteria.

The safety limit concept and the role of conservative and best estimate calculations to verify sufficient safety margins in the deterministic safety analysis are illustrated in Figure 16.

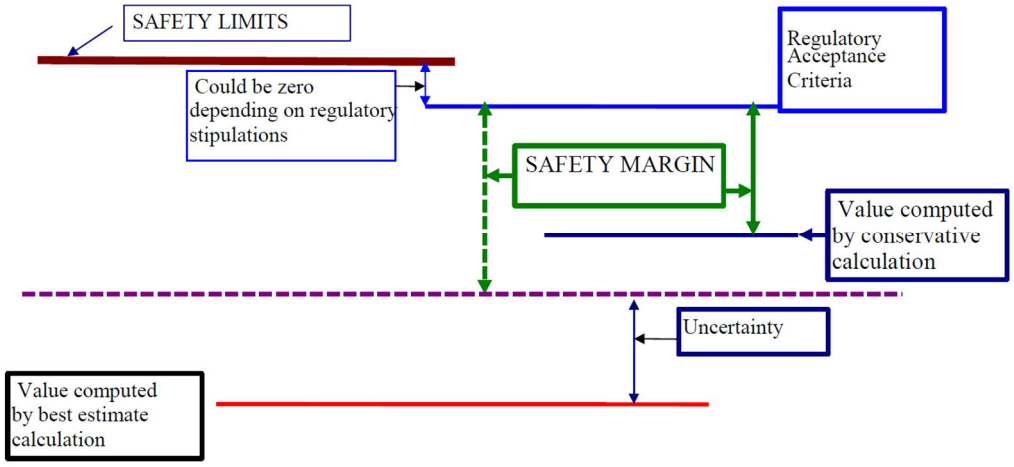


Figure 16: Safety limit and safety margin concepts in deterministic safety analysis (IAEA, 2003).

The deterministic acceptance criteria and safety margins are typically associated with the following physical phenomena and plant parameters (IAEA, 2004):

a. Preventing inadvertent core criticality and excessive power increase;
b. Preventing or reducing the possibility of fuel cladding damage;
c. Limiting damage to the nuclear fuel, including structural damage;
d. Preventing loss of leak tightness or damage to the integrity of RCS boundary;
e. Preventing damage to the integrity of the containment;
f. Limiting radiological impact of the accident within a prescribed period under given conditions;
g. Providing sufficient time for accident management or for emergency response.

4.3 Probabilistic safety margins

In a common view of probabilistic safety assessment (PSA), the safety margins can be defined as the difference between the established probabilistic safety targets acceptable to the regulatory body and the calculated value of the risk parameter taking into account uncertainties addressed in detail in a specific area of PSA scope called uncertainty analysis. The probabilistic safety margin concept is illustrated in Figure 17.

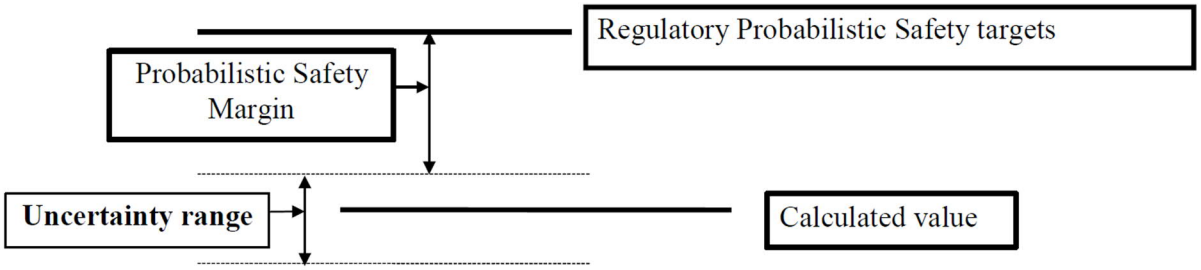


Figure 17: Probabilistic safety margin (IAEA, 2003).

PSA can be used in various risk-informed applications to show compliance with numerical risk criteria and to evaluate and compare different design alternatives. The probabilistic safety margin concept has similarity to deterministic safety margin concept. However, instead of calculating the difference or ration of capacity to load, the probabilistic safety margin is expressed as the probability that a load exceeds the capacity. Also, since the risk parameters are abstract measures, and not physical quantities to be measured in real life, some flexibility is needed in the interpretation of load and capacity parameters in the context of probabilistic safety margins compared to the load and capacity parameters in the context of deterministic safety margins.

The high-level risk parameters most often considered for the evaluation of probabilistic safety margins are the core damage frequency (CDF) in Level 1 PSA and large early release frequency (LERF) in Level 2 PSA. Other quantitative parameters specified by PSA model quantification can be considered in a more detailed analysis of safety margins and the factors decreasing (or increasing) it. For example, minimum cut sets can be used to define the absolute or relative contributions of different components, systems and human failures to the overall risk, and therefore can be used to specify which scenarios, components, systems and human failures represent biggest challenges to the probabilistic safety margin. The risk importance measures of components, systems and human actions can be used for the same purpose. By using these risk parameters specified in PSA outputs, it is possible to verify that the probabilistic safety targets have been maintained.

A very important part of the probabilistic analysis may be providing evidence that the plant design and the ways, the plant is operated, is well balanced. Such premise can be supported by showing that there are no uniquely dominating minimum cut sets covering significant part of the overall risk. If this is the case and the safety margin is sufficiently large, the plant has got a very good perspective in not losing safety margin. If there are some clearly dominating risk contributors in the spectrum of minimum cut sets (and in particular, if the corresponding risk parameters values are connected with high level of uncertainty), probabilistic safety margin could be challenged in future and measures should be taken to eliminate the highest risk peaks.

The advantage of probabilistic safety analysis (PSA), as mentioned above, is the possibility to study safety margins for a broad spectrum of initiating events altogether, involving multiple safety barriers and mutually redundant and diverse systems in consistent and coherent manner. PSA provides tools for evaluating complex accident scenarios where the actuations of the protective functions are not taken for granted, and instead, the protection functions can be assumed to fail with some probability. This way, the design basis assumptions transmitted from the deterministic safety analysis can be challenged and the risk significance of beyond design basis accidents can be estimated. PSA gives opportunity to study, for example, following complex situations (IAEA, 2003):

- The initiating event occurs from initial conditions not considered in the selection of the design basis events.
- There are concurrent “initiating” events, either simultaneous or subsequent.
- There are more than one failure additional to the initiating event, and the protective function does not work or fails to arrest the transient.

- Human intervention takes the evolution of the transient away from the design conditions.

It should be pointed out, that all four cases of complex situations just mentioned may belong to the typical ways, accident scenarios started by external hazards impact can develop. Thus, these situations, which are typical for external hazards scenarios, will be subjects of demonstration of PSA applications in many of the case studies, which will be selected and analysed in Work Packages 3 and 4 of BESEP project.

4.4 Safety margins for human actions

According to IAEA (IAEA, 2019), Human Factors Engineering (HFE) is an engineering discipline “in which factors that could influence human performance and that could affect safety are understood and are taken into account, especially in the design and operation of facilities”. Guidance for the standard review of applicants (i.e. licensees) HFE program is presented in the U.S.NRC guideline NUREG-0711 (NUREG, 2012).

On safety margins regarding human actions NUREG-0711 states the following: “Safety margins often used in deterministic analyses to account for uncertainty and provide an added margin to provide adequate assurance that the various limits or criteria important to safety are not violated. Such safety margins are typically not related to human actions, but the reviewer should take note to see if there are any that may apply to the particular case under review. It is also possible to add a safety margin (if desired) to the human action by demonstrating that the action can be performed within some time interval (or margin) that is less than the time identified by the analysis.”

The guideline leaves it open how and what parameters should be applied when defining safety margins for human actions. Below the topic is discussed by trying to relate the safety margins for human actions to the process of deterministic and probabilistic analysis. The emphasis of the discussion is in human reliability analysis (HRA), which is a specific analysis of PSA and one element of HFE program. In the relation to safety margins in HFE the one identified method is *treatment of important human actions,* which HRA is a part of.

In order to include human actions among the subjects considered in safety margin evaluations, human actions need to be interpreted by means of qualitative or quantitative attributes. In other, more concrete words, the potential for occurrence of human failure contributing to possible decreasing of safety margin has to be treated in some way, either deterministic or probabilistic. As a matter of fact, the approach to human factors is, to some level, similar in the process of deterministic or probabilistic analysis focussing on safety margins.

In deterministic analysis, the first step is identification of those human actions (and corresponding errors), which could lead to significant decreasing (and possible loss) of safety margin. This effect can be caused by initiating accident scenarios with strong impact on the typical parameters representing deterministic safety margins. If the operator unintentionally close or drain the residual heat removal circuit during shutdown, the primary circuit coolant temperature may rise up to the point, safety margin is decreased significantly. Another way how to decrease safety margin significantly by human factor is wrong response to accident scenario already occurred (which could be solved without loss of safety margin by correct action of the operator). If the operator of PWR is not able to balance the primary circuit cooling and depressurization process in the steam generator tube rupture scenario, primary circuit parameters may develop in a way, safety margin is threatened or lost.

The second step of human factor related deterministic safety analysis with possible impact on safety margin is evaluation of the factors contributing to the human errors identified in the first step. There is a number of such factors, as, for example:

- insufficient time for the action;
- level of stress;
- level of experience;
- quality of training, including operational feedback;
- quality of procedures;
- HSI (Human System Interface) attributes
- (bad) teamwork;
- psychological profiles of the operators etc. etc.

Some of these factors are (at least in theory) measurable (time, level of stress, level of experience), some not (quality of procedures, overload). Anyway, each factor can be analysed from point of view of its potential contribution to the occurrence of the human error under concern, which may represent, correspondingly, the importance of the given factor regarding safety margin (for the given human error or in total).

The probabilistic safety margins are related to the metrics, which are specified, for specific NPP, by plant probabilistic safety model, where human factors are addressed by human error related basic events. It is a goal of human reliability analysis (HRA) to cover human factor contribution to the risk of plant operation sufficiently completely and in a proper way. The basic process applied in HRA was described, for example, in SHARP (Hannaman, 1984) and later updated in ATHEANA (ATHEANA, 2001). SHARP is divided into seven steps, where the most important are:

- identification;
- qualitative analysis;
- quantification;
- integration.

The first two steps are similar to the deterministic analysis (identification of human actions important for deterministic safety margins, evaluation of contributing factors). The new step, which is not part of deterministic approach and is enforced by the needs of PSA, is quantification of probabilities of human failures. That means, in fact, transformation of the results of qualitative analysis carried out in the previous step to the numerical values of HEPs (human error probabilities). There is a number of methods how to do that used in PSAs worldwide, for example THERP (Swain, 1990), EPRI CBDT (EPRI, 2014) or SPAR-H (Gertman et al 2005). Various HRA methods were compared in (Forester et al. 2014), where a large study is described devoted to comparison of methods applied by fourteen HRA teams worldwide for the quantification of error probabilities for equally defined human actions performed under the same circumstances and providing evidence about the strengths and weaknesses of these HRA methods.

The last important step of HRA is a full integration of quantitative models of the individual human actions into the PSA model, which includes analysis of the effects of coincidence of various human actions (and possible errors) in the same scenario (human error dependence analysis). As a matter of fact, dependence among human action/errors may have big impact on PSA results and on the conclusions made regarding safety margins, as well.

HRA concentrates on human actions that are important to reactor safety, which belong to the following categories:

1. actions causing PSA initiating events;
2. actions causing failures in safety-related systems with possible latent effect on system availability (as soon as the system is demanded after initiating event occurrence);
3. actions taken in response to initiating event occurrence.

The process of quantification of PSA model produces several categories of results related to human factors engineering typical by different levels of impact on safety margin:

- human error probabilities - without direct relation to safety margins, because a high human error probability does not necessarily indicate big safety impact (a problematic human action may have several back-ups);
- human error elements (basic events) in minimum cut sets, which may provide some inputs for the discussions of safety margin, but in general, are not the most direct indications of human error impact on safety margin (the presence of human error related basic event in the minimum cut set does not necessarily mean that the operator or the conditions of his work are bad, but may represent just the importance of the action for plant safety);
- importance measures of primary events modelling human actions, which may directly indicate the impact of concrete human action on probabilistic (and also deterministic, indirectly) safety margin; in particular, the value of RIF (risk increase factor) may work like that.

5 Failure tolerance analysis as safety engineering activity

5.1 Background

Failure tolerance analysis is a concept, that has been recently defined from the regulatory perspective in Finland by STUK. Failure tolerance analysis in short, is a set of failure analyses, that are chosen to study the failure tolerance of a NPP as a whole, instead of treating the different systems and aspects of the plant as separate entities. Failure tolerance means that the plant can operate safely despite certain failures, and that the faults cannot spread across the system. The target of failure tolerance analysis is to ”reach traceability and sufficient coverage of analyses, without overlapping of work”.(Humalajoki & Niemelä, 2018)

The purpose of failure analyses is to identify failure causes and their effects to structures, systems or components. Failure analyses are best used in combination with safety analyses, as they provide necessary information back and forth. Failure analyses are described in this chapter to support better integration of the three main safety analyses types, DSA, PSA and HFE, that are in the focus of this project.

5.2 Failure analyses

Failure analyses have a fundamental role in the independency and strength analysis of Defence-in-Depth (DiD) levels. They also provide valuable inputs to the safety analyses that are performed during the design and operation of an NPP, and thus are a part of a safety engineering process. In a way, failure analyses are used to challenge the fulfilment of the acceptance criteria and safety margins. Failure tolerance of systems, functions and the entire NPP has to be ensured in the design of the plant. A means to do that, is by conducting a failure tolerance analysis. The aim of failure tolerance analysis is to show that systems performing safety functions and their support systems satisfy the failure criteria, that are related to the defence-in-depth requirements.

Failure tolerance analysis is an integrated set of failure analyses chosen to demonstrate the acceptability of failure of safety functions. Acceptability is demonstrated through sufficient redundancy, diversity and separation of safety functions. Various types of failure analyses are listed in table 1. Failures, failure modes and their effects on the plant functions are recognized with the analyses. Failure tolerance analysis results are also a proof of safety. If the failure criteria of single systems are met, the failure tolerance of the whole plant is confirmed.

The advantages of using a well-defined failure tolerance analysis set are, that the analysis consists of diverse failure analyses, that cover the topic of the study sufficiently, but without significant overlap of work. If the responsibilities are optimally divided, the analyses also save time and resources. Also, the approach considers the whole plant instead of a single system or area of expertise, which intends to ensure that all possible failures are recognized.

Failure tolerance analysis aims to demonstrate the fulfilment of DSA based failure criteria, requirements and analyses. Using DSA, PSA and failure analyses together, can also be used to recognize failures that should be practically eliminated, or on the other hand to show that all failure potentials are eliminated. Failure analysis is used in all steps of the design, and based on the results, design of the systems and selection of components can be modified to ensure better failure tolerance and safety. Failure analyses have a strong effect to the licensing of the plant, in design of safety systems and components, but also in the architectural level, for example in the redundancy and diversity design principles.

Table 1: Failure analyses

Topic of architecture level design:	Topics of system level design:	Examples of failure analyses (some analyses can be classified under several topics):
Independency of DiD levels	Physical separation	internal hazard analysis external hazard analysis physical separation of safety divisions
	Functional separation	initiating event effect analysis consequential failures independency of electric systems

		I&C separation
Strength of DiD levels	Redundancy	failure mode and effect analysis human error analysis spurious actions N+1, N+2 failure criteria
	Diversity	common cause failure analysis diversity analysis (of systems, automation, measurement systems)

5.3 Interaction of analyses with safety margin and connection to V-model

Failure analyses are closely linked to deterministic safety analyses, probabilistic safety analyses and human factors engineering, and the analyses types provide support to each other. Both deterministic and probabilistic analyses get inputs from failure analyses. Probabilistic safety analysis combines the deterministic and failure analysis results to a detailed model of the plant. Still, the cooperation of the different analyses could be better defined to achieve a well-defined flow of analyses from the recognition of the failure to the effects and probabilities of events. One view of the relation of the PSA, DSA and failure analyses is the one of (Humalajoki and Niemelä, 2018) in Figure 18. In this view, failure analyses recognize the faults and failure modes, which are an input to deterministic and probabilistic analyses. In the figure this is the “assumptions of faults”, for example FMEA. DSA demonstrates the capability of the safety functions, also using the known information of the failure modes. Deterministic safety analyses set the failure tolerance requirements, which are verified with failure analyses. PSA then ties all the information from the failure and deterministic analyses together to a plant model, iteratively providing information back to deterministic analyses. DSA provides success criteria, parameters to construct fragility curves and timing of human interactions to PSA. Inputs from PSA to DSA are mainly information on complex combinations of faults leading to core damage or large release.

A questionnaire was sent to the BESEP project partners to collect information regarding the integration of PSA, DSA and HFE. According to the answers of several BESEP partners, no formal process of integration of different analyses such as PSA, DSA and HFE exist. From the project partners’ views, in many cases deterministic analyses and probabilistic analyses are used together and to support each other, but specific processes to integrate the analyses are not in place. Probabilistic analyses are sometimes used to support planning of emergency operation procedures and operator training, and to evaluate the risk impacts of certain HFE solutions. Also, human reliability analysis included in PSA touches the human factors side of the safety analyses.

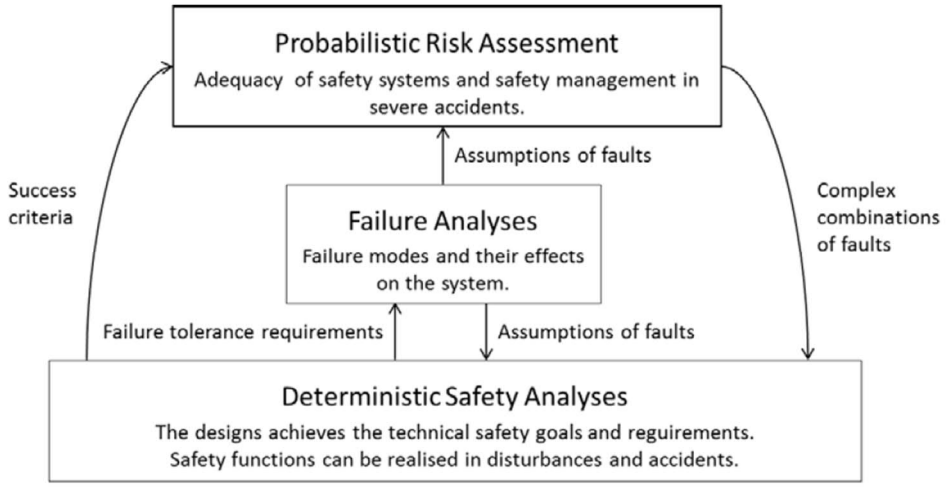


Figure 18: Relation of PSA, DSA and failure analyses (Humalajoki and Niemelä, 2018).

Failure analyses and safety margins come together in the safety engineering process. From one end, the safety requirements determine the safety and acceptance criteria applied for the plant design. These safety and acceptance criteria are determined in separate safety analysis conducted usually by the regulatory body for a nonspecific plant design. From the other end, plant design defines the system and building configuration. The failure analyses are conducted for the system and building configurations of the specific plant design in

order to verify the fulfilment of safety margins for different failure situations with a sufficient failure tolerance. Increasingly stringent safety and licensing requirements and new design solutions cause challenges on how to actually demonstrate the safety margins. An integrated safety engineering process can help with these challenges by introducing more efficient integration between the different safety analyses and the underlying failure analyses.

To finally tie the failure analyses and safety analyses to a general safety engineering process, the link to a V-model approach is discussed next. The engineering workflow steps of a reference V-model are presented as in Figure 12. For the purpose of demonstration of the safety engineering process and later assessment of case studies, that are in the scope of this project, it is useful to think of the allocation of the failure and safety analyses to the different workflow steps. In the V-model, the stages of the design lifecycle on the left side of the V are divided to functional, architectural, system and equipment levels. On the right side of the V are the stages of verification and validation (10.), and analyses and interconnection tests (11.), where failure and safety analyses are located. Typically in the system and equipment design stages, the failure analyses performed in step 10 of the V-model include for example failure mode and effect analysis, initiating event effect analysis, common cause failure analysis, analyses of spurious actions and human errors as well as N+1, N+2 failure criteria analysis. During the functional or architectural design stages, the analyses performed in steps 11 and 12 of the V-model, typically include failure analyses such as hazard and interface analyses, separation analysis, analyses of consequential failures, safety divisions and independency of electric systems. In the functional level, analyses include also deterministic and probabilistic safety analyses, as well as human factors. At the highest stage, the plant level analysis in step 13 of the V-model, PSA can be used to analyse the plant as whole. Many of the safety and failure analyses are applicable in more than just one phase of the safety engineering process. The analyses can also be applied both in the design phase of the plant as well as in the changes made in the operational phase, for example due to changes in regulation.

6 Recommendations based on this deliverable: key features of efficient and integrated safety engineering process

This chapter summarizes the main points from the previous chapters and tries to identify the key features impacting the efficient and integrated safety engineering processes in the scope of safety requirement verification and safety margin assessment.

BESEP-project sets out to benchmark and further define an integrated set of safety engineering practices that should be optimised to support all main elements of safety engineering process: plant design management, safety requirement and safety analyses. Any change in one of these elements needs to be considered in the other two, and a balance should be reached between the elements, wherever they are connected together ensuring the information flow and utilisation inside and between each element. In an ideal situation, there is a general consensus that, based on the safety analyses, the current plant design fulfils the given safety requirements. To summarize, from the BESEP project point-of-view, an efficient and integrated safety engineering process should include at least the following actions:

- Connecting together the main elements of safety engineering process: safety requirements, safety analyses and plant design
- Safety analyses (probabilistic, deterministic and human factor engineering) providing feedback and information to the other analyses and to the overall safety design.

From the more general safety engineering processes point-of-view, it is suggested to apply the ISO/IEC/IEEE 15288 processes, especially its specialty engineering view. Supplemented by the ISO/IEC 15504-10 safety engineering process model, a sound and well recognized framework for the safety engineering activities can be established. After the processes for the engineering work are defined, it is equally important to define the information model to store the outcomes of the processes in a structured and traceable manner. To define these processes, resources (money and workforce) shall be allocated to the systems engineering management (maybe even 14% of the project budget, as suggested by Eric Honour (Honour, 2013)), not only to the systems engineering technical activities. To effectively utilise the workforce, the roles of the engineering team and managers must be carefully planned. Finally, the engineering, engineering management and project management tools must be selected such that the gained formalism of well-structured processes and information is not undermined by cumbersome and ineffective software tools. To summarize, safety engineering process should include at least the following actions:

- Lifecycle model acting as the framework of processes and activities concerned within the life cycle that may be organised into stages, which also acts as a common reference for communication and understanding
- Comprehensive and documented set of safety engineering processes to ensure that the design meets all the safety requirements throughout the lifetime of the plant.

From the safety margin assessment point-of-view, it is important for the safety engineering process to define the assessment scope and safety variables of interest. In BESEP, some of the most important factors defining the scope are the initiating events, event classes and acceptance criteria applied for the assessment. A safety margin assessment is always linked to certain event classes where the acceptance criteria for safety variables of interest have been defined. The acceptance criteria for different event classes are listed in Task 2.2 (Rein, 2021). Therefore, by defining the reference event class, the initial and boundary conditions and objectives of the assessment should become more evident.

External hazards are a common cause of SSCs failures, and therefore, potential sources of initiating events for the plant. An efficient safety engineering process should support the identification and connection of external hazards with potential initiating events. Single external hazards and some combinations of two or more external hazards relevant for the BESEP partner countries have been collected in Task 2.1 (Kovacs, 2021).

Potential consequences of accident scenarios caused by the initiating events are classified according to national event classification requirements. The event classes and associated acceptance criteria for the event classes applied in the BESEP partner countries have been summarised in Task 2.2 (Rein, 2021). As it can be noted, the classes definitions and associated acceptance criteria are similar when grouped based on IAEA classification.

After defining the scope for the safety margins assessment, different safety analyses (deterministic, probabilistic and human factors engineering analysis) are carried out to investigate the sufficiency of safety margins in the accident scenario. The different accident scenarios identified and analysed by the safety analyses form the so-called design basis of the plant. The safety analysis should be carried out in an integrated efficient manner to save analysis resources as well as to reach a common and broad understanding on the issues important to safety. The logic model of PSA is a powerful tool for complementing the deterministic assessments. An integrated safety engineering process should support the integration of the deterministic and probabilistic approaches.

From the safety margins assessment point-of-view, an efficient and integrated safety engineering process should include at least the following actions:

- Determine the event classes and associated acceptance criteria for the accident scenarios under study
- Define all safety variables useful for the evaluation of intermediate and final states of accident scenario
- Support the integration of safety analysis methods to obtain more accurate estimates and to save resources
- Help to reach common understanding on the importance of different factors influencing safety and to apply graded approach, i.e. perform more detailed analysis for more important factors

From the failure analyses point-of-view, it is useful for the safety engineering process to use a well-defined set of failure analyses systematically and comprehensively throughout the process. Comprehensive failure analysis, in combination with deterministic and probabilistic safety analyses, illustrates the fulfilment of safety margins and demonstrates the failure tolerance of the plant by analysing the strength and independence of the defence in depth levels.

As the failure analyses along with deterministic and probabilistic safety analyses have a fundamental role in the safety assessments of nuclear power plants, it is essential to recognize the usage of the analyses in the different stages of design workflow.

From the failure analyses point-of-view, an efficient and integrated safety engineering process should include at least the following actions:

- Use failure analyses systematically and comprehensively
- Identify which failure or safety analyses are used in each stage of plants lifecycle

7 Conclusions

This report summarizes the work performed within Task 2.3 of the BESEP project. The goal of the Task 2.3 was to explore, identify and discuss key features of efficient and integrated safety engineering process in the scope of BESEP project.

Typical safety analysis methods applied in the scope of analysis of external hazards were studied to support the description and creation of a standard safety engineering process. For a standard safety engineering process, the failure analyses involved and the interaction points between different safety analysis methods (i.e. deterministic safety analysis, probabilistic safety analysis and human factors engineering) were discussed. Using such standard safety engineering process as a reference, the key features of efficient and integrated safety engineering process were suggested in Chapter 6. The main points were:

- Connecting together the main elements of safety engineering process: safety requirements, safety analyses and plant design
- Safety analyses (probabilistic, deterministic and human factor engineering) providing feedback and information to the other analyses and to the overall safety design.
- Lifecycle model acting as the framework of processes and activities concerned within the life cycle that may be organised into stages, which also acts as a common reference for communication and understanding
- Comprehensive and documented set of safety engineering processes to ensure that the design meets all the safety requirements throughout the lifetime of the plant.
- Determine the event classes and associated acceptance criteria for the accident scenarios under study
- Define all safety variables useful for the evaluation of intermediate and final states of accident scenario
- Support the integration of safety analysis methods to obtain more accurate estimates and to save resources
- Help to reach common understanding on the importance of different factors influencing safety and to apply graded approach, i.e. perform more detailed analysis for more important factors
- Use failure analyses systematically and comprehensively
- Identify which failure or safety analyses are used in each stage of plants lifecycle

As mentioned in Section 3.4, the safety engineering process provided in this report is at quite an abstract level to be compliant with the level of typical process capability assessment. Hence, the ideas and suggestions listed above in this chapter should be developed further in Work Packages 3 and 4 to identify the more specific safety engineering and safety margin assessment criteria in the scope of BESEP project.

REFERENCES

Alanen, J., Linnosmaa, J. and Tommila, T. (2017) 'Conformity assessment data model'. Finland: VTT Technical Research Centre of Finland (Research report).

Alanen, J. and Salminen, K. (2016) 'Systems Engineering Management Plan template V1', VTT-R-0015. VTT Technical Research Centre of Finland, p. 78 p. + app. 12 p.

Alanen, J. and Tommila, T. (2016) 'A reference model for the NPP I&C qualification process and safety demonstration data'. Espoo: VTT.

ATHEANA (2000) Technical Basis and Implementation Guidelines for A Technique for Human Event Analysis, NUREG-1624, Rev. 1, Washington, D.C.: U.S. Nuclear Regulatory Commission.

Cronvall, O. (2016) 'Study on Status of Safety Margins Assessment Practices', in BALTICA X - International Conference on Life Management and Maintenance for Power Plants. VTT Technical Research Centre of Finland.

Elm, J. P. and Goldenson, D. R. (2012) The Business Case for Systems Engineering Study: Results of the Systems Engineering Effectiveness Survey.

EPRI (2014), The EPRI HRA Calculator® Software Manual, EPRI 3002004030, Palo Alto, CA: Electric Power Research Institute.

Forester, J., Dang, V. D., Bye, A., Lois, E., Massaiu, S. Broberg, H., Braarud, P. Ø., Boring, R., Männistö, I., Liao, H., Julius, J., Parry, G., Nelson, P. (2014) 'The International HRA Empirical Study, Lessons Learned from Comparing HRA Methods Predictions to HAMMLAB Simulator Data', August.

Gertman, D., Blackman, H., Marble, J., Byers, J. and Smith, C. (2005) 'The SPAR-H Human Reliability Analysis Method', NUREG/CR-6883, Washington, D.C.: U.S. Nuclear Regulatory Commission.

Hannaman G.W., Spurgin A.J. (1984) 'Systematic Human Action Reliability Procedure (SHARP)', EPRI-NP-3583, Electric Power Research Institute, Palo Alto.

Hämäläinen, J. and Suolanen, V. (2014) 'SAFIR2014 The Finnish Research Programme on Nuclear Power Plant Safety 2011 – 2014', VTT Technology 213. Edited by J. Hämäläinen and V. Suolanen. VTT Technical Research Centre of Finland Ltd.

Honour, E. C. (2013) Systems engineering return on investment. University of South Australia. Available at: http://www.hcode.com/seroi/documents/SE-ROI Thesis summary-distrib.pdf.

Hrehor, M., Gavrilas, M., Belac, J., Sairanen, R., Bruna, G., Reocreux, M., Touboul, F., Krzykacz-Hausmann, B., P., Seuk, J., Prosek, A., Hortal, J., Sandervaag, O. and Zimmerman, M. (2007) Task Group on Safety Margins Action Plan (SMAP) Safety Margin Action Plan - Final report. NEA-CSNI-R--2007-09.

Humalajoki, P. and Niemelä, I. (2018) 'NPP failure analyses in Finland', PSAM 2018 - Probabilistic Safety Assessment and Management U6.

IAEA (2000) 'SSR-2-1: Safety of nuclear power plants: design', Safety Standards, 1, p. 73.

IAEA (2003) 'Tecdoc-1332: Safety margins of operating reactors', Tecdoc Series, (January), p. 143.

IAEA (2004) 'Tecdoc-1418: Implications of power uprates on Safety Margins of nuclear power plants', Tecdoc Series, (September).

IAEA (2019) 'IAEA Safety Glossary: Terminology Used in Nuclear Safety and Radiation Protection', 2018 Edition.

IAEA (2021) DRAFT: Introduction to Systems Engineering – Nuclear Power Plant Instrumentation and Control Aspects / Perspectives.

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

ISO/IEC/IEEE (2018) ISO/IEC/IEEE 24748-1: Systems and software engineering — Life cycle management — Part 1: Guidelines for life cycle management.

ISO/IEC (2019) ISO/IEC 33020 Information technology — Process assessment — Process measurement framework for assessment of process capability.

ISO/IEC TS. (2011). IEC 15504-10: Information technology - Process assessment — Part 10: Safety extension (No. 15504-10:2011).

Kovacs, Z. (2021) 'BESEP Deliverable 2.1 Assignment of safety requirement topics of selected external hazards', (945138).

Nuutinen, P., Sipola, S. and Rantakaulio, A. (2016) 'Advanced Licensing and Safety Engineering Method-ADLAS®', in Nuclear Science and Technology Symposium - NST2016. Helsinki, p. 5.

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.

NUREG (2012) 'Human Factors Engineering Program Review Model'. United States Nuclear Regulatory Commission, Office of Nuclear Regulatory Research, NUREG-0711 (Rev. 3), 2012.

Osborne, L., Brummond, J., Hart, R. and Zarean, Mohsen (Moe) Conger, S. (2005) Clarus: Concept of Operations. U.S. Department of Transportation - Federal Highway Administration (FHWA).

Rein, S. (2021) 'BESEP Deliverable 2.2 Requirement baseline for BESEP', (945138).

Swain, A. and Guttman, H. (1983) 'Handbook of Human Reliability. Analysis with Emphasis on Nuclear Power Plant Applications', NUREG/CR-1278.

Tommila, T. and Alanen, J. (2015) 'Conceptual model for safety requirements specification and management in nuclear power plants', VTT Technology 238. VTT Technical Research Centre of Finland, p. 26.

APPENDIX A: SPECIALTY ENGINEERING ACTIVITIES

The list of specialty engineering processes, their activities, and their tasks are supplied in Table 2 with indication about the relevant tasks in this context. Detailed descriptions about the processes, activities and tasks is supplied by ISO/IEC/IEEE 15288. The table works as a checklist to ensure that the safety engineering process we define in Section 3.4 covers all the relevant activities.

To complement the ISO/IEC/IEEE 15288 speciality engineering processes, we also introduce three safety engineering focused processes provided by ISO/IEC TS 15504-10:2011. The processes with their task are Table 3. Developing safety-related systems requires specialized processes, techniques, skills and experience. Thus, ISO/IEC TS 15504-10, presents additional safety amplifications to ISO/IEC/IEEE 15288 in forms of safety extensions in the areas of safety management, safety engineering and the safety qualification.

Table 2. Speciality engineering processes, activities, and tasks (ISO/IEC/IEEE 15288:2015). In this context, our scope is focused on the tasks that are marked with an X in the first column.

Relevant for BESEP	**PROCESS** ***Activity*** **Task**
BUSINESS OR MISSION ANALYSIS PROCESS	
Define the problem or opportunity space.	
	Analyse the problems and opportunities in the context of relevant trade-space factors.
	Define the mission, business, or operational problem or opportunity.
Characterize the solution space.	
	Define preliminary operational concepts and other concepts in the life cycle stages.
Evaluate alternative solution classes.	
	Assess each alternative solution class.
STAKEHOLDER NEEDS AND REQUIREMENTS DEFINITION PROCESS	
Prepare for stakeholder needs and requirements definition.	
	Identify the stakeholders who have an interest in the system throughout its life cycle.
	Define the stakeholder needs and requirements definition strategy.
Define stakeholder needs.	
	Identify stakeholder needs.
	Prioritize and down-select needs.
	Define the stakeholder needs and rationale.
Develop the operational concept and other life cycle concepts.	
	Define a representative set of scenarios to identify all required capabilities that correspond to anticipated operational and other life cycle concepts.
	Identify the interaction between users and the system.
Transform stakeholder needs into stakeholder requirements.	
	Identify the constraints on a system solution.
	Identify the stakeholder requirements and functions that relate to critical quality characteristic, such as assurance, safety, security, environment, or health.
X	Define stakeholder requirements, consistent with life cycle concepts, scenarios, interactions, and critical quality characteristics.
Analyze stakeholder requirements.	
X	Define critical performance measures that enable the assessment of technical achievement.

SYSTEMS REQUIREMENTS DEFINITION PROCESS	
Prepare for system requirements definition.	
X	Define the functional boundary of the system in terms of the behavior and properties to be provided.
Define system requirements.	
X	Define each function that the system is to perform.
X	Define necessary implementation constraints.
X	Identify system requirements that relate to risk, criticality of the system, or critical quality characteristics.
X	Define system requirements and rationale.
Analyse system requirements.	
X	Define critical performance measures that enable assessment of technical achievement.
ARCHITECTURE DEFINITION PROCESS	
Prepare for architecture definition.	
X	Identify stakeholder concerns.
X	Define evaluation criteria based on stakeholder concerns and key requirements.
Develop architecture viewpoints.	
X	Select, adapt, or develop viewpoints and model kinds based on stakeholder tasks.
Develop models and view of candidate architectures.	
X	Identify architectural entities and relationships between entities that address key stakeholder concerns and critical system requirements.
X	Allocate concepts, properties, characteristics, behaviours, functions, or constraints that are significant to architecture decisions of the system to architectural entities.
X	Select, adapt, or develop models of the candidate architectures of the system.
X	Compose views from the models in accordance with identified viewpoints to express how the architecture addresses stakeholder concerns and meets stakeholder and system requirements.
Relate the architecture to design.	
X	Identify system elements that relate to architectural entities and the nature of these relationships.
Assess architecture candidates.	
X	Assess each candidate architecture against stakeholder concerns using evaluation criteria.
DESIGN DEFINITION PROCESS	
Prepare for design definition process.	
X	Determine the necessary design characteristics types.
Establish design characteristics and design enablers related to each system element.	
X	Allocate system requirements to system elements.
X	Transform architectural characteristics into design characteristics.
X	Define the necessary design enablers.
X	Examine design alternatives.
X	Establish the design artifacts.
Assess alternatives for obtaining system elements.	

X	Assess each candidate Non-Developmental-Items (NDI) and new design alternative against criteria developed from expected design characteristics or system element requirements to determine suitability for the intended application.
SYSTEM ANALYSIS PROCESS	
Prepare for system analysis.	
X	Identify the problem or question that requires system analysis.
X	Identify the stakeholders of the system analysis.
X	Define the scope, objectives, and level of fidelity of the system analysis.
X	Select the system analysis method.
X	Define the system analysis strategy.
X	Identify and plan for the necessary enabling systems or services needed to support system analysis.
X	Obtain or acquire access to the enabling systems or services to be used.
X	Collect the data and inputs needed for analysis.
Perform system analysis.	
X	Identify and validate assumptions.
X	Apply the selected analysis methods to perform the required system analysis.
X	Review the analysis results for quality and validity.
X	Establish conclusions and recommendations.
X	Record the results of the system analysis.
IMPLEMENTATION PROCESS	
Perform implementation.	
X	Record objective evidence that the system element meets system requirements.
INTEGRATION PROCESS	
Prepare for integration.	
X	Identify and define check points for the correct operation and integrity of the assembled interfaces and the selected system functions.
Perform integration – Successively integrate system element configurations until the complete system is synthesized.	
X	Perform check of interfaces, selected functions, and critical quality characteristics.
Manage results of integration.	
X	Record integration results and any anomalies encountered.
VERIFICATION PROCESS	
Prepare for verification.	
X	Identify the verification scope and corresponding verification actions.
X	Select appropriate verification methods or techniques and associated criteria for every verification action.
Perform verification.	
X	Define the verification procedures, each supporting one or a set of verification actions.
X	Perform the verification procedures.
Manage results of verification.	

X	Record verification results and any anomalies encountered.
X	Record operational incidents and problems and track their resolution.
TRANSITION PROCESS	
Prepare for the transition.	
	Identify system constraints from transition to be incorporated in the system requirements, architecture or design.
Perform the transition.	
	Demonstrate proper installation of the system.
	Perform activation and check-out of the system.
	Demonstrate the installed system is capable of delivering its required functions.
VALIDATION PROCESS	
Prepare for validation.	
X	Identify the validation scope and corresponding validation actions.
X	Select appropriate validation methods or techniques and associated criteria for each validation action.
Perform validation.	
X	Define the validation procedures, each supporting one or a set of validation actions.
X	Perform the validation procedures in the defined environment.
Manage results of validation.	
X	Record validation results and any anomalies encountered.
X	Record operational incidents and problems and track their resolution.
OPERATION PROCESS	
Perform operation.	
	Monitor system operation.
	Identify and record when system service performance is not within acceptable parameters.
Manage results of operation.	
	Record results of operation and any anomalies encountered.
	Record operational incidents and problems and track their resolution.
Support the customer.	
	Provide assistance and consultation to the customers as requested.
	Record and monitor requests and subsequent action for support.
MAINTENANCE PROCESS	
Perform maintenance.	
	Review incident and problem reports to identify future corrective, adaptive, perfective and preventive maintenance needs.
	Record maintenance incidents and problems and track their resolution.
	Implement the procedures for correction of random faults or scheduled replacement of system elements.
	Upon encountering random faults that cause a system failure, deploy actions to restore the system to operational status.

	Perform preventive maintenance by replacing or servicing or servicing system elements prior to failure, according to planned schedules and maintenance procedures.
	Perform failure identification actions when a non-compliance has occurred in the system.
	Identify when adaptive or perfective maintenance is required.
Perform logistics support.	
	Perform acquisition logistics.
	Perform operational logistics.
	Implement any packaging, handling, storage and transportation needed during the life cycle.
	Confirm that logistics actions satisfy the required replenishment levels so that stored system elements meet repair rates and planned schedules.
	Confirm that logistics actions include supportability requirements that are planned, resourced, and implemented.
Manage results of maintenance and logistics.	
	Record maintenance and logistics results and any anomalies encountered.
	Record operational incidents and problems and track their resolution.
DISPOSAL PROCESS	
Prepare for disposal.	
	Identify system constraints from disposal on the system requirements, architecture and design characteristics, or implementation techniques.
Perform disposal.	
	Deactivate the system or system element to prepare it for removal.
	Remove the system, system element, or waste material from use of production for appropriate disposition and action.
Finalize the disposal.	
	Return the environment to its original state or to a state that [was] specified by agreement
	Achieve information gathered through the lifetime of the system to permit audits and reviews in the event of long-term hazards to health, safety, security and the environment, and to permit future system creators and users to build a knowledge base from past experiences.
PROJECT ASSESSMENT AND CONTROL PROCESS	
Assess the project.	
	Assess progress using measured achievement and milestone completion.
	Conduct required management and technical reviews, audits and inspections.
	Analyze measurement results and make recommendations.
	Record and provide status and findings from assessment tasks.
DECISION MANAGEMENT PROCESS.	
Analyze the decision information.	
	Select and declare the decision management strategy for each decision.
	Determine desired outcomes and measurable selection criteria.
X	Identify the trade space and alternatives.
X	Evaluate each alternative, against the criteria.
Make and mange decisions.	
X	Determine preferred alternative of each decision.

RISK MANAGEMENT PROCESS	
Plan risk management.	
	Define the risk management strategy.
	Define and record the context of the Risk Management process.
Manage the risk profile.	
	Define and record the risk thresholds and conditions under which a level of risk may be accepted.
	Establish and maintain a risk profile.
	Periodically provide the relevant risk profile to stakeholders based upon their needs.
Analyze risk.	
	Identify risks in the categories described in the risk management context.
	Estimate the likelihood of occurrence and consequence of each identified risk.
	Evaluate each risk against its risk thresholds.
	For each risk that does not meet its risk threshold, define and record recommended treatment strategies and measures.
Treat risks.	
	Identify recommended alternatives for each risk treatment.
	Implement risk treatment alternatives for which the stakeholders determine that actions should be taken to make a risk acceptable.
	When the stakeholders accept a risk that does not meet its threshold, consider it a high priority and monitor it continually to determine if any future risk treatment actions are necessary.
	Once a risk treatment is selected, coordinate management action.
Monitor risks.	
	Continually monitor all risks and the risk management context for changes and evaluate the risks when their state has changed.
	Implement and monitor measures to evaluate the effectiveness of risk treatments.
	Continually monitor for the emergence of new risks and sources throughout the life cycle.
INFORMATION MANAGEMENT PROCESS	
Prepare for information management.	
X	Define the strategy for information management.
X	Define the items of information that will be managed.
X	Designate authorities and responsibilities for information management.
X	Define the content, formats and structure of information item.
X	Define information maintenance actions.
Perform information management.	
X	Obtain, develop, or transform the identified items of information.
X	Maintain information items and their storage records, and record the status of information.
X	Publish, distribute or provide access to information and information items to designated stakeholders.
X	Archive designated information.
X	Dispose of unwanted, invalid or unavailable information.

MEASUREMENT PROCESS	
Prepare for measurement.	
	Define measurement strategy.
	Describe the characteristics of the organisation that are relevant to measurement.
	Identify and prioritize the information needs.
	Select and specify measures that satisfy the information needs.
	Define data collection, analysis, access, and reporting procedures.
	Define criteria for evaluating the information items and the Measurement process.
	Identify and plan for the necessary enabling systems or services to be used.
Perform measurement.	
	Integrate procedures for data generation, collection, analysis and reporting into the relevant processes.
	Collect, store, and verify data.
	Analyze data and develop information items.
	Record results and inform the measurements users.
QUALITY ASSURANCE PROCESS	
Prepare for Quality Assurance strategy.	
	Define a Quality Assurance strategy.
	Establish independence of quality assurance from other life cycle processes.
Perform product or service evaluations.	
	Evaluate products and services for conformance to established criteria, contracts, standards, and regulations.
	Perform verification and validation of the outputs of the life cycle processes to determine conformance to specified requirements.
Perform process evaluations.	
	Evaluate project life cycle processes for conformance.
	Evaluate tools and environments that support or automate the process for conformance.
	Evaluate supplier processes for conformance to process requirements.
Manage quality assurance records and reports.	
	Create records and reports related to quality assurance activities.
	Maintain, store, and distribute records and reports.
	Identify incidents and problems associated with product, service, and process evaluations.
Treat incidents and problems.	
	Incidents are recorded, analyzed and classified.
	Incidents are resolved or elevated to problems.
	Problems are recorded, analyzed and classified.
	Treatments for problems are prioritized and implementation is tracked.
	Trends in incidents and problems are noted and analyzed.
	Stakeholders are informed of the status of incidents and problems.
	Incidents and problems are tracked to closure.

Table 3. Safety engineering processes, activities, and tasks (ISO/IEC TS 15504-10:2011). In this context, our scope is focused on the tasks that are marked with an X in the first column.

Relevant for BESEP	**PROCESS** ***Activity*** **Task**
SAFETY MANAGEMENT PROCSS	
Define safety objectives and criteria.	
X	The limits of acceptable risk associated with a hazard are defined externally as imposed safety targets or developed from analysis or development policy.
X	Safety targets and/or acceptable levels of risk are determined.
Define safety life cycle.	
X	The safety life cycle is defined, which is appropriate to the context, complexity, safety criteria and targets for the project.
Perform safety planning.	
X	Safety engineering and management activities are to be implemented in order to meet and verify that safety requirements are identified, their dependencies are determined, their implementation planned, and the resource needs are identified.
Define safety activities integration.	
X	Safety activities integration with product development, project life cycle and support process is determined.
Define skills requirements and allocate responsibility.	
	Skills needs for carrying out planned safety activities are identified and responsibilities, authorities, and independence of involved roles are defined and allocated accordingly.
Implement planned safety activities.	
X	The activities defined in the safety planning are implemented.
Monitor the deployment of the safety activities.	
	Monitor the deployment of the safety activities and act to correct deviations: safety activities of the project are monitored, and safety-related incidents identified in work products, and safety activities are reported, analyzed, managed to closure and further prevented.
Define and agree safety policy and safety requirements with suppliers.	
	Methods and techniques to monitor supplier's safety activities are agreed with the customer.
	Define an agreement on how the supplier assures safety of the supplied product.
Monitor the safety activities of the supplier.	
	Supplier's safety activities to meet the safety requirements are monitored and reported.
Implement an escalation mechanism.	
	Develop and maintain the escalation mechanism that ensures that safety issues may be escalated to appropriate levels of management to resolve them.
SAFETY ENGINEERING PROCESS	
Identify hazard sources and hazards.	
X	Hazard sources and hazards of relevant operational conditions and for foreseeable misuse are identified.
Analyze hazards and risks.	

X	For each hazard, analyze likelihood and severity of impact, and evaluate the risk of the hazard.
Establish and maintain hazard log.	
	Status of hazards is maintained throughout the whole product life cycle.
Establish and maintain safety demonstration.	
X	Safety demonstration is created and maintained during the life cycle of the product.
X	Process and product documentation is collected for safety demonstration evidence.
Establish and maintain safety requirements.	
X	Establish and maintain throughout the life cycle safety requirements based on the results of hazard and risk analysis and any other applicable sources.
Determine safety integrity requirements.	
X	Safety integrity requirements for each safety requirement based on the risk evaluation of their hazards are determined.
Allocate safety requirements and safety integrity requirements.	
X	Safety requirements and safety integrity requirements are allocated to architecture, subsystems and components.
Apply safety principles to achieve safety integrity requirements.	
X	Principles and methods relevant for achieving the required safety integrity requirements are applied during the product life cycle.
Perform safety impact analysis on changes.	
	Analyse the impact of the change requests on hazards and risks.
	Traceability between a change request and the affected safety work products is established.
Perform safety validations on product.	
X	Safety validations should be based on the outcomes of hazard analysis and risk analysis and performed against safety targets.
Perform independent assessments.	
X	Assessments of product and processes are performed in preset points during the product life cycle according to the required level of independence.
SAFETY QUALIFICATION PROCESS[1]	
Develop a safety qualification strategy.	
	Develop a qualification strategy. The qualification strategy shall consider the quality requirements of the external resources (reflecting the safety requirements determined for the safety-related software or system). The qualification strategy includes criteria for selecting qualification methods.
Plan the safety qualification of external resources.	
	Plan the qualification activities for the external resources.
	Select the appropriate qualification method for each external resources
Qualify the external resources.	
	Execute qualification according to the qualification methods chosen.
Record the safety qualification results.	
	Record the results of the safety qualification and disseminate the results from the qualification to interested parties.
Maintain and update the safety qualification results.	

	Maintain and update the safety qualification results and documentation throughout the usage of the external resources.

1) Note that this process concerns qualification of external resources, such as engineering and engineering support tools.

APPENDIX B: PROCESS CAPABILITY ASSESSMENT

This appendix gives brief introduction to process capability assessment based on the process measurement framework for assessment of process capability presented in ISO/IEC 33020:2019 (ISO/IEC, 2019). If needed, this appendix can be used to help the benchmarking of safety engineering processes in the case studies in BESEP project.

In Chapter 3, we have described a systematic approach to safety engineering processes through systems engineering. With to help of standards ISO/IEC/IEEE 15288 and ISO/IEC TS 15504-10, in Appendix A we have selected the main processes required for safety engineering activities in the scope BESEP project. This chapter gives suggestions and hopefully helpful references on how to evaluate the safety engineering processes of the organizations participating in the benchmark exercise. It can also be used to create assessment criteria in other tasks of the BESEP project.

The ISO/IEC 330xx is a series of technical standards originally developed for the computer software development process assessment and related business management functions. However, it has been updated to described process assessment models for systems and software too. It has superseded the ISO/IEC 155xx family (also termed Software Process Improvement and Capability Determination (SPICE). The documents act as a reference model for the process maturity models (consisting of capability levels which in turn consist of the process attributes and further consists of generic practices). ISO/IEC 330xx / ISO/IEC 155xx have been used also to support the process assessment in the nuclear scope, for example in Nuclear SPICE assessment method (Hämäläinen and Suolanen, 2014).

Process capability assessment according to ISO/IEC 33020

The following sections reference the main points from the standard ISO/IEC 33020 Information technology — Process assessment — Process measurement framework for assessment of process capability.

Within this process measurement framework, the measure of capability is based upon a set of process attributes. Each process attribute defines a measurable property of process capability. The extent of process attribute achievement is characterised on a defined rating scale. The process capability level for an assessed process is derived from the set of process attribute ratings represented in the process profile. The achievement of one process attribute may be associated with the achievement of another process attribute within the process measurement framework (ISO/IEC, 2019).

Process attributes

The capability of processes is measured using process attributes. ISO/IEC 33020 defines nine process attributes.

Table 4. Process attributes (according to ISO/IEC 33020)

ID	Attribute	Description
PA 1.1	Process performance	The process performance process attribute is a measure of the extent to which the process purpose is achieved. As a result of full achievement of this process attribute: a) The process achieves its defined process outcomes.
PA 2.1	Performance management	The performance management process attribute is a measure of the extent to which the performance of the process is managed with necessary resources and competences. As a result of full achievement of this process attribute: a) results to be achieved are determined and communicated; b) risks that can affect performance of the process are determined and addressed; c) performance of the process is planned, monitored, measured, evaluated and adjusted (as needed); d) responsibilities and authorities for performing the process are determined, assigned and communicated; e) resources necessary for performing the process are determined, provided and maintained (as needed);

		f) person(s) performing the process are competent on the basis of appropriate education, training, or experience; g) interfaces between the involved parties are managed to ensure both effective communication and the level of control expected.
PA 2.2	Documented information management	The documented information management process attribute is a measure of the extent to which the documented information produced internally or acquired from an external source when performing the process is appropriately managed. As a result of full achievement of this process attribute: a) requirements for the documented information of the process are determined; b) requirements for control of the documented information are determined; c) documented information is appropriately identified, and controlled according to requirements; d) documented information is reviewed and approved for suitability and adequacy in accordance with planned arrangements and adjusted as necessary to meet requirements; e) documented information is determined, maintained and retained to the extent necessary to have confidence that the process has been performed as planned and to demonstrate the conformity of products and/or services to their requirements.
PA 3.1	Process definition	The process definition process attribute is a measure of the extent to which a standard process is established and maintained. As a result of full achievement of this process attribute: a) a standard process, including appropriate tailoring guidelines, is established and maintained that describes the fundamental elements that must be incorporated into a defined process; b) the required inputs and the expected outputs for the standard process are determined; c) sequence and interaction of the standard process with other processes is determined; d) roles, competences, responsibilities and authorities for performing the standard process are determined; e) resources for performing the standard process are determined; f) knowledge necessary for the operation of the standard process is determined and maintained.
PA 3.2	Process deployment	The process deployment process attribute is a measure of the extent to which a standard process is deployed as a defined process. As a result of full achievement of this process attribute: a) a defined process is deployed based upon an appropriately tailored standard process; b) required roles, responsibilities and authorities necessary for performing the defined process are assigned and communicated;

		c) required person(s) necessary for performing the defined process are competent on the basis of defined education, training and experience; d) required resources necessary for performing the defined process are made available, monitored and measured; e) documented information is available to ensure that the defined process achieves its intended results.
PA 3.3	Process assurance	The process assurance process attribute is a measure of the extent to which the defined process is assured and continually improved. As a result of full achievement of this process attribute: a) appropriate data and information are collected and analysed from monitoring and measurement of the process to evaluate the effectiveness and risks of the process, and to identify needs and opportunities for improvement; b) criteria and methods needed to ensure effective operation and control, and continuing suitability, adequacy, effectiveness and risks of the process are determined and evaluated; c) conformity of the defined process (and associated activities, outputs and documented information) is objectively assured; d) action is taken on any nonconformity, based on its nature and effect, and tracked to closure; e) the standard process is continually improved based on identified needs and opportunities. Documented information should be retained of any nonconformities describing actions taken, concessions obtained, and authority deciding action in respect on the nonconformity. Documented information reviews include management reviews.
PA 4.1	Quantitative analysis	The quantitative analysis process attribute is a measure of the extent to which information needs are defined, relationships between process elements are identified and data are collected. As a result of full achievement of this process attribute: a) process information needs in support of relevant defined quantitative business goals are established; b) process measurement objectives are derived from process information needs; c) measurable relationships between process elements that contribute to the process performance are identified; d) quantitative objectives for process performance are established to support relevant business goals; e) appropriate measures and frequency of measurement are identified and defined in line with process measurement objectives and quantitative objectives for process performance; f) techniques for analysing the collected data are selected; g) results of measurement are collected, validated and reported in order to monitor the extent to which the quantitative objectives for process performance are met.
PA 4.2	Quantitative control	The quantitative control process attribute is a measure of the extent to which objective data are used to manage and control

		process performance that is predictable. As a result of full achievement of this process attribute: a) assignable causes of process variation are determined through analysis of the collected data; b) distributions that characterize the performance of the process are established; c) corrective actions are taken to address assignable causes of variation; d) separate distributions are established (as necessary) for analysing the process under the influence of assignable causes of variation; e) process performance data are used to develop predictors of process outcomes.
PA 5.1	Process innovation	The process innovation process attribute is a measure of the extent to which changes to the definition, management and performance of the process are identified and effectively implemented from identified innovative approaches for process innovation using internal resources and/or using external ideas according to defined process innovation objectives. As a result of full achievement of this process attribute: a) process innovation objectives for the process are defined that support the relevant business goals; b) appropriate data are analysed to identify opportunities for best practice and innovation; c) innovation opportunities derived from new technologies and process concepts are identified; d) an implementation strategy is established to achieve the process innovation objectives; e) impact of all proposed changes is assessed against the objectives of the defined process and standard process; f) implementation of all agreed changes is managed to ensure that any disruption to the process performance is understood and acted upon; g) effectiveness of process change on the basis of actual performance is evaluated against the defined product requirements and process and innovation objectives.

Each process attribute consists of one or more generic practices, which are further elaborated into practice indicators to aid assessment performance.

Process attribute rating scale

Table 5. Process attribute rating scale (according to ISO/IEC 33020:2010).

Process attribute ratings values	Levels of achievement	Corresponding achievement percentages
N (Not achieved)	There is little or no evidence of achievement of the defined process attribute in the assessed process.	0-15%
P (Partially achieved)	There is some evidence of an approach to, and some achievement of, the defined process attribute in the assessed process. Some aspects of achievement of the process attribute may be unpredictable.	15-50%
L (Largely achieved	There is evidence of a systematic approach to, and significant achievement of, the defined process attribute in the assessed	50-85%

	process. Some weaknesses related to this process attribute may exist in the assessed process.	
F (Fully achieved)	There is evidence of a complete and systematic approach to, and full achievement of, the defined process attribute in the assessed process. No significant weaknesses related to this process attribute exist in the assessed process.	85-100%

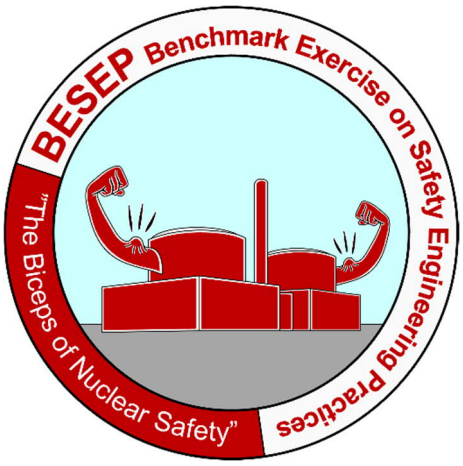
The rating is based upon evidence collected against the practice indicators, which demonstrate fulfilment of the process attribute.

Process capability level model

Process capability is defined on a six-point ordinal scale that enables capability to be assessed from the bottom of the scale, Incomplete, through to the top end of the scale, Innovating. The scale represents increasing capability of the implemented process, from failing to achieve the process purpose through to continually improving and able to respond to organizational change. For each process, ISO/IEC 33020 defines a capability level on the following scale.

Table 6. Process capability levels.

Level	Name	Explanation
0	Incomplete process	The process is not implemented or fails to achieve its process purpose. At this level there is little or no evidence of any systematic achievement of the process purpose.
1	Performed process	The implemented process achieves its process purpose.
2	Managed process	The previously described Performed process is now implemented in a managed fashion (planned, monitored and adjusted) and its documented information are appropriately established, controlled and maintained.
3	Established process	The previously described Managed process is now implemented using a defined process which is assured and continually improved.
4	Predictable process	The previously described Established process is now performed predictively. Quantitative management needs are identified, measurement data are collected and analysed to identify assignable causes of variation. Corrective action is taken to address assignable causes of variation.
5	Innovating process	The previously described Predictable process is now continually improved to respond to changes through identified innovative approaches for process innovation.



BESEP

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 945138.