



RESEARCH REPORT

VTT-R-00153-16



Systems Engineering Management Plan template, V1

Authors: Alanen, Jarmo & Salminen, Karoliina

Confidentiality: Public

Report's title Systems Engineering Management Plan template - V1								
Customer, contact person, address SAFIR2018 programme		Order reference						
Project name Integrated safety assessment and justification of nuclear power plant automation		Project number/Short name 102392 / SAUNA						
Author(s) Alanen, Jarmo & Salminen, Karoliina		Pages 90 of which appendices 12 pages						
Keywords Nuclear, Instrumentation and control, Systems Engineering		Report identification code VTT-R-00153-16						
Summary <p>It is evident that governance of complex projects, like NPP projects, requires systematic engineering methodologies, like Systems Engineering. The main motivation for this comes from the stringent safety requirements and the long lifetime of the nuclear power plants.</p> <p>The needs and requirements for NPP I&C systems can differ in many ways depending on the country despite the fact that the IAEA regulations are aimed to be applied by all the nuclear countries globally. However, using the systems engineering principles, it is possible to use the same framework in several countries to manage the whole life cycle of a nuclear power plant I&C system. Such a framework or reference model can be issued as a systems engineering management plan template. Based on the reference model, nuclear power plant organisations can develop their management systems according to the systems engineering principles. The goals for using such a reference model are assured safety and shorter development times of NPP systems, subsystems and components.</p> <p>This report provides an overview of the systems engineering approach, and of the state-of-the-art regarding systems engineering planning. Furthermore, foundations for a well-structured SEMP are laid, and the SEMP template SharePoint implementation is presented.</p>								
Confidentiality	Public							
Tampere 4.2.2016 <table border="0"> <tr> <td>Written by</td> <td>Reviewed by</td> <td>Accepted by</td> </tr> <tr> <td>Jarmo Alanen, Senior Scientist</td> <td>Teemu Tommila, Senior Scientist</td> <td>Riikka Virkkunen, Head of research area</td> </tr> </table>			Written by	Reviewed by	Accepted by	Jarmo Alanen, Senior Scientist	Teemu Tommila, Senior Scientist	Riikka Virkkunen, Head of research area
Written by	Reviewed by	Accepted by						
Jarmo Alanen, Senior Scientist	Teemu Tommila, Senior Scientist	Riikka Virkkunen, Head of research area						
VTT's contact address Jarmo Alanen, PL 1300, FI-33101 Tampere; jarmo.alanen@vtt.fi , +358 40 501 5813								
Distribution (customer and VTT) SAFIR2018 program VTT / archive, original								
<i>The use of the name of VTT Technical Research Centre of Finland Ltd in advertising or publishing of a part of this report is only permissible with written authorisation from VTT Technical Research Centre of Finland Ltd.</i>								

Preface

This report has been written within the SAUNA project (Integrated safety assessment and justification of nuclear power plant automation) in the context of the SAFIR2018 programme (The Finnish Research Programme on Nuclear Power Plant Safety 2015–2018). The SAUNA project for year 2015 consisted of several tasks of which this report relates to Task 1.1 (Systems Engineering Management Plan [SEMP]) of Work package 1 (Safety Systems Engineering). The members of Task 1.1 were Jarmo Alanen (VTT) and Teemu Tommila (VTT). The goal of Task 1.1 was “...to define the reference model for the Systems Engineering life cycle processes in nuclear power plant automation and to describe it as a Systems Engineering Management Plan (SEMP) template.” (An excerpt of the SAUNA 2015 project plan.)

The goal of this report is to provide the background and a short state-of-the-art study to help create and understand the SEMP template.

Task 1.1 as well as the whole SAUNA project was steered by the Reference Group 1 (Automation, organisation and human factors) with the following members:

Jarmo Ala-Heikkilä (Aalto University), Janne Peltonen (Vice chair) (Fennovoima Oy), Liisa Sallinen (Fennovoima Oy), Juha Lamminen (Fortum Oyj), Sami Matinaho (Fortum Oyj), Leena Salo (Fortum Oyj), Anne Jordan (Lappeenranta University of Technology), Eetu Kotro (Lappeenranta University of Technology), Mika Johansson (STUK, Radiation and Nuclear Safety Authority in Finland), Pia Oedewald (STUK, Radiation and Nuclear Safety Authority in Finland), Mauri Viitasalo (Chair) (Teollisuuden Voima Oyj), Petri Koistinen (Teollisuuden Voima Oyj), Eija Kaasinen (VTT), Tommi Karhela (VTT) and Heli Talja (VTT).

The authors thanks the RG1 for guiding the work and Mauri Viitasalo for reviewing the report.

Tampere 4.2.2016

Authors

Contents

Preface	2
Contents	3
1. Introduction	5
1.1 Scope	5
1.2 Definitions and abbreviations	6
2. Overview and selection of the systems engineering approach.....	9
2.1 ISO/IEC/IEEE15288	9
2.2 ISO/IEC 26702	10
2.3 Systematic engineering	10
2.4 System life cycle model.....	10
2.5 System life cycle processes	14
2.6 Systems engineering artefacts model	16
2.7 Systems engineering literature	16
2.8 Requirements engineering	17
2.9 Collaboration between organisations	19
2.10 Model-based systems engineering.....	21
3. Current systems engineering practices	23
3.1 ITER–SEMP	23
3.2 Fusion for Energy (F4E) SEMP	26
3.3 Rosatom	30
3.4 U.S. Department of Defense	32
3.5 U.S. Department of Transportation Systems Engineering Guidebook	33
4. SEMP in the context of STUK and IAEA regulations.....	35
5. Foundations for the SEMP template implementation	41
5.1 Document centric vs model-based	41
5.2 Specifications, descriptions, plans and reports	41
5.3 Process vs. process views	43
5.4 Enhanced process constructs model.....	45
6. Description of the SEMP template implementation	49
6.1 Implementation platform	49
6.2 I&C systems life cycle model.....	49
6.3 Identified systems engineering processes.....	50
6.4 SEMP table of contents.....	54
6.5 Main information items	58
6.6 IEC 61513 requirements for activities.....	60
6.7 Example process	63
6.8 SEMP implementation in the context of a Management system implementation.....	75
7. Summary and conclusions.....	76
References	77
Appendix 1. ITER SEMP Table of Contents.....	79
Appendix 2. F4E SEMP Table of Contents	81
Appendix 3. DoD Systems Engineering Plan (SEP) Table of Contents	83
Appendix 4. ISO/IEC 26702 / IEEE Std 1220 example SEMP table of contents	84

Appendix 5. YVL A.3 requirements for management system processes (including project and systems engineering processes)	85
Appendix 6. YVL B.1 selected requirements for management system processes (including project and systems engineering processes)	89

1. Introduction

One of the objectives of the SAUNA project (a SAFIR2018 programme project) in year 2015 was to specify a SEMP (Systems Engineering Management Plan) template for the NPP automation sector. The aim is to help nuclear automation companies and authorities develop and assess NPP I&C systems according to the systems engineering principles. The ultimate goals are assured safety and shorter development times of NPP systems, subsystem and components.

The goal was not to define a general purpose SEMP, but to provide a template for a SEMP for the NPP domain players (see Figure 1).

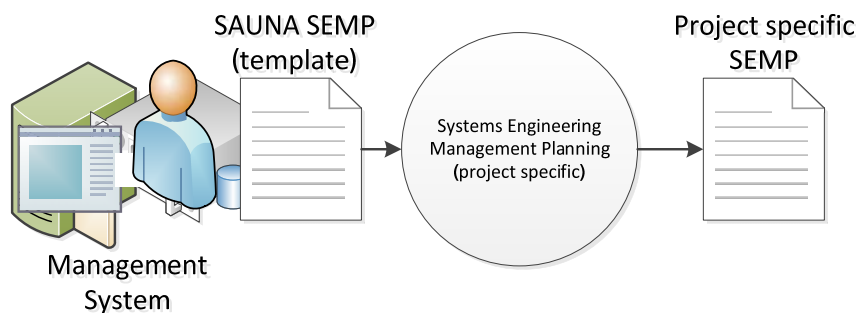


Figure 1. The targeted usage of SAUNA SEMP.

The SEMP template is provided by the management system of the organisation and is used as a reference model and starting point for a project specific SEMP. The SEMP is not a system specification but a plan for the organisation to carry out rigorous systems engineering.

The SEMP typically includes, a life cycle model and a description of the SE processes and models for the engineering work product types and their relations. The SEMP template introduced in this report concentrates on these issues.

This report provides in Chapter 2 a short description of the systems engineering approach and in Chapter 3 an overview of the state-of-the-art of the systems engineering management planning. Systems Engineering approach in the context of management systems required by STUK and IAEA is discussed in Chapter 4. To create the SEMP (template) implementation, the foundations for the SEMP are laid in Chapter 5. And the actual SEMP (template) implementation using the SharePoint content management system is presented in Chapter 6. And finally, the conclusions are provided in Chapter 7. But before we proceed to Chapter 2, the scope of work is narrowed in Section 1.1 to the I&C systems, and Section 1.2 provides the definitions for the core concepts and abbreviations.

1.1 Scope

The SAUNA project plan defines the scope of the task (the outcome of which this report is) as follows: "The purpose of this task is to define the reference model for the Systems Engineering life cycle processes in nuclear power plant automation and to describe it as a Systems Engineering Management Plan (SEMP) template." Hence we concentrate on the overall I&C architecture as depicted in Figure 2.

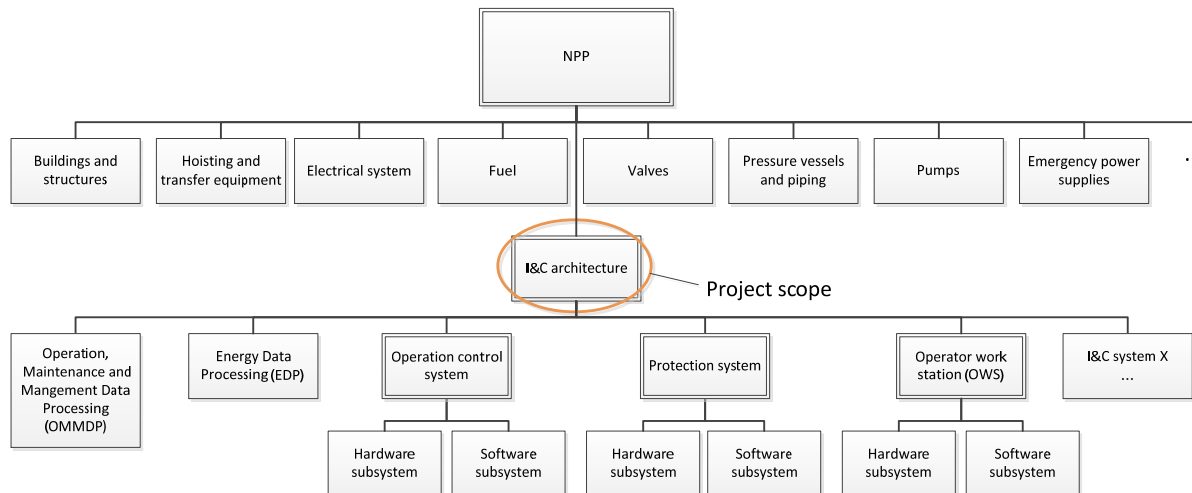


Figure 2. Scope of the SEMP: I&C systems.

The electrical part of sensors and actuators¹ are considered to belong to the scope of an I&C architecture.

In this case, we do not precisely define the organisation-of-interest (regulator, licence holder, plant supplier, automation supplier, I&C subsystem supplier, sub-contractor etc.), but try to make the SEMP template generic enough to be utilised and applied on any organisation level.

1.2 Definitions and abbreviations

Some key concepts are defined in Table 1.

Table 1. Key concepts.

Definition	Description
Artefact	A synonym to <i>Work product</i>
Configuration item	<p>Item or aggregation of hardware, software, or both, that is designated for configuration management and treated as a single entity in the configuration management process.</p> <p>NOTE 1: According to ISO/IEC TR 24774 [2010] The term ‘software’ includes e.g. computer programs, documents, information and contents.</p> <p>NOTE 2: An <i>information item</i> or a collection of <i>information items</i>, or any other engineering <i>artefact</i>, like a requirement statement or a complete list of requirements can be a CI.</p> <p>[source: ISO/IEC/IEEE 15288 2015, except the notes, which are by the authors of this report]</p>
Information item	<p>Separately identifiable body of information that is produced, stored, and delivered for human use; a special case of a <i>Work product</i></p> <p>NOTE 1: In case of documents, books, etc. the information item can be the whole document or a part of the document (chapter, section, paragraph, figure, table, etc.) or both (as separate information items).</p> <p>NOTE 2: An information item is not necessarily a <i>configuration item</i>, e.g. a paragraph of a hard copy book can be an information item, but is not a configuration item; or a document of an external organisation, such as a standard, the version management of which is not controlled by the engineering organisation (in this case the version control inside the engineering organisation is carried out through information item references).</p> <p>[source: ISO/IEC/IEEE 15289 2015 and ISO/IEC TR 24774 2010, except the notes, which are by the authors of this report]</p>
Life cycle	Evolution of a system, product, service, project or other human-made entity from conception through retirement [source: ISO/IEC/IEEE 15288 2015]

¹ And hence in practice the whole components, because the electrical parts of a sensor or actuator cannot be separated from the mechanical, optical etc. parts.

Definition	Description
Life cycle model	Framework of processes and activities concerned with the life cycle that may be organised into stages, which also acts as a common reference for communication and understanding [source: ISO/IEC/IEEE 15288 2015]
Life cycle stage	A time window within the life cycle of the system-of-interest. A life cycle stage has only one starting and one ending milestone. A life cycle stage exclusively occupies the time window assigned to it. NOTE: The consequence is that two or more life cycle stages cannot overlap. [source: the authors of this report]
Management system	Management system shall refer to a system that is used to establish policy and objectives and to achieve those objectives. [source: YVL Guide A.3; uses definition from SFS-EN ISO 9000:2005]
Process	Set of interrelated or interacting activities that transforms inputs into outputs. NOTE: In a broad sense, a process can be a system process or a systems engineering process. In the former case, the system-of-interest transforms its inputs to outputs (like sensor values to actuator actions); in the latter case, the organisation and tools that develop the system-of-interest transform input artefacts to output artefacts (like requirements specifications to architectural design). If there is a possibility to confuse with these two point of views, it is suggested to use phrases 'system process' and 'SE process' respectively. [source: ISO/IEC/IEEE 15288 2015, except the note, which is by the authors of this report]
Process view	Description of how a specified purpose and set of outcomes can be achieved by employing the activities and tasks of existing processes [source: ISO/IEC 15026-1 2013, which transcripts the definition from ISO/IEC/IEEE 15288 2015]
System	Combination of interacting elements organized to achieve one or more stated purposes NOTE 1: A system is sometimes considered as a product or as the services it provides. NOTE 2: In practice, the interpretation of its meaning is frequently clarified by the use of an associative noun, e.g., aircraft system. Alternatively, the word 'system' is substituted simply by a context-dependent synonym, e.g., aircraft, though this potentially obscures a system principles perspective. NOTE 3: A complete system includes all of the associated equipment, facilities, material, computer programs, firmware, technical documentation, services, and personnel required for operations and support to the degree necessary for self-sufficient use in its intended environment. [source: ISO/IEC/IEEE 15288 2015]
Systems engineering	Interdisciplinary approach governing the total technical and managerial effort required to transform a set of stakeholder needs, expectations, and constraints into a solution and to support that solution throughout its life cycle [ISO/IEC/IEEE 15288 2015] Interdisciplinary approach and means to enable the realization of successful systems. It focuses on defining customer needs and required functionality early in the development cycle, documenting requirements, and then proceeding with design synthesis and system validation while considering the complete problem: operations, cost and schedule, performance, training and support, test, manufacturing, and disposal. SE considers both the business and the technical needs of all customers with the goal of providing a quality product that meets the user needs. [source: INCOSE 2015]
Systems engineering management plan (SEMP)	Structured information describing how the systems engineering effort, in the form of tailored processes and activities, for one or more life cycle stages, will be managed and conducted in the organization [source: INCOSE 2015]
Work product	An artefact associated with the execution of a process. There are four generic work product categories: services (e.g. operation); software (e.g. computer program, documents, information, contents); hardware (e.g. computer, device); processed materials. [source: ISO/IEC TR 24774 2010]

The abbreviations used in the report are listed below.

Table 2. Abbreviations.

Abbreviation	Description
EU	European Union
IAEA	International Atomic Energy Association
I&C	Instrumentation and Control
INCOSE	International Council on Systems Engineering
NPP	Nuclear Power Plant
PLM	Product Life cycle Management
SE	Systems Engineering
SEMP	Systems Engineering Management Plan
V&V	Verification and Validation

2. Overview and selection of the systems engineering approach

(See the definitions of systems engineering in Section 1.2.)

2.1 ISO/IEC/IEEE 15288

In the following sections, a short overview of the systems engineering approach is provided. We select the ISO/IEC/IEEE 15288 [2015] standard to be our reference model for the systems engineering processes. ISO/IEC/IEEE 15288 is selected because it is the most popular SE standard; for example, International Council on Systems Engineering (INCOSE) applies it in its Systems Engineering Handbook [INCOSE 2015]. Another important advantage of ISO/IEC/IEEE 15288 is that it declares to be compatible with ISO 9001. Furthermore, there are several standards that accompany the ISO/IEC/IEEE 15288 standard. The list below identifies some of these:

- IEEE Std 828-2012 – IEEE Standard for Configuration Management in Systems and Software Engineering
- ISO/IEC 12207 – IEEE Std 12207-2008. ISO/IEC/IEEE Standard for Systems and Software Engineering – Software Life Cycle Processes
- ISO/IEC/IEEE 15289-2015. Systems and software engineering – Content of life-cycle information items (documentation)
- ISO/IEC 15939 – IEEE Std 15939-2008. Systems and software engineering – Measurement process
- ISO/IEC/IEEE 16326-2009. ISO/IEC/IEEE Systems and Software Engineering – Life Cycle Processes – Project Management
- ISO/IEC TR 24774-2010 Systems and Software Engineering – Life Cycle Management – Guidelines for Process Description
- ISO/IEC TR 24748-1-2010. Systems and software engineering – Life cycle management – Part 1: Guide for life cycle management
- ISO/IEC TR 24748-2-2011. Systems and software engineering – Life cycle management – Part 2: Guide to the application of ISO/IEC 15288 (System life cycle processes)
- ISO/IEC TR 24748-3-2011. Systems and software engineering – Life cycle management – Part 3: Guide to the application of ISO/IEC 12207 (Software life cycle processes)
- ISO/IEC TR 90005-2008. Systems engineering – Guidelines for the application of ISO 9001 to system life cycle processes
- ISO/IEC/IEEE 24765-2010. Systems and software engineering – Vocabulary
- ISO/IEC/IEEE 29148-2011. Systems and software engineering – Life cycle processes – Requirements engineering
- ISO/IEC 15026-1-2014. Systems and Software Engineering – Systems and Software Assurance – Part 1: Concepts and Vocabulary
- ISO/IEC 15026-2-2011. Systems and Software Engineering – Systems and Software Assurance – Part 2: Assurance Case
- ISO/IEC 15026-3-2013. Systems and Software Engineering – Systems and Software Assurance – Part 3: System Integrity Levels
- ISO/IEC 15026-4-2013. Systems and Software Engineering – Systems and Software Assurance – Part 4: Assurance in the Life Cycle

- ISO/IEC/IEEE 42010-2011. ISO/IEC/IEEE Systems and software engineering – Architecture description.

(See also http://sebokwiki.org/wiki/Systems_Engineering_Standards [referenced 20.11.2015].)

2.2 ISO/IEC 26702

ISO/IEC 26702 [2007] (issued also as IEEE Std 1220) is a ‘competitor standard’ to ISO/IEC/IEEE 15288. It introduces a process model that is different from that of ISO/IEC/IEEE 15288.

ISO/IEC 26702 / IEEE Std 1220 is under revision and will be published with a different standard number: ISO/IEC TR 24748-4 (2016²). Systems and software engineering – Life cycle management – Part 4: Systems engineering planning.

The example SEMP table of contents provided in the standard can be found in Appendix 4.

2.3 Systematic engineering

Systems engineering can be thought as systematic engineering of a system through its whole life cycle. Being effective in this, the NPP organisations should possess the following:

1. systematic processes and life cycle model (obtained e.g. from ISO/IEC/IEEE 15288 and its daughter standards)
2. a systematic information model for the information items (such as documents and CAD-models) and other engineering artefacts and their relations
3. an effective organisation model
 - a. well-defined roles (like systems engineer, requirements engineer, etc.)
 - b. well-defined communication and collaboration model (to facilitate consistent view in all involved organisations of the goal, data and state of the development)
4. well-planned use of project management and systems engineering tools
 - a. a good selection of tools (model-based tools advocated)
 - b. a flexible tool integration model (to allow integration of various tools used by the collaboration partners)
 - c. a tool to orchestrate all the systems engineering work (such as a PLM tool).

The Systems Engineering Management Plan should address each of these issues. The success factors above are reflected to all the engineering disciplines, like requirements engineering, configuration management and safety demonstration.

2.4 System life cycle model

The basic decision in defining the system life cycle model is whether the life cycle stages are purpose-driven categories of activities (see Table 3) or time windows within the life time of the system (see Figure 3). The former allows for iterations between the life cycle stages whereas the latter does not because it is bound to the passage of time.

² The publishing date is not known, but the document was in FDIS state in February 2016.

Table 3. Life cycle stages in a purpose-driven life cycle model [ISO/IEC TR 24748-1 2010].

LIFE CYCLE STAGES	PURPOSE	DECISION GATES
CONCEPT	Identify stakeholders' needs Explore concepts Propose viable solutions	Decision Options: - Execute next stage - Continue this stage - Go to a preceding stage - Hold project activity - Terminate project
DEVELOPMENT	Refine system requirements Create solution description Build system Verify and validate system	
PRODUCTION	Produce systems Inspect and test	
UTILIZATION	Operate system to satisfy users' needs	
SUPPORT	Provide sustained system capability	
RETIREMENT	Store, archive or dispose of system	

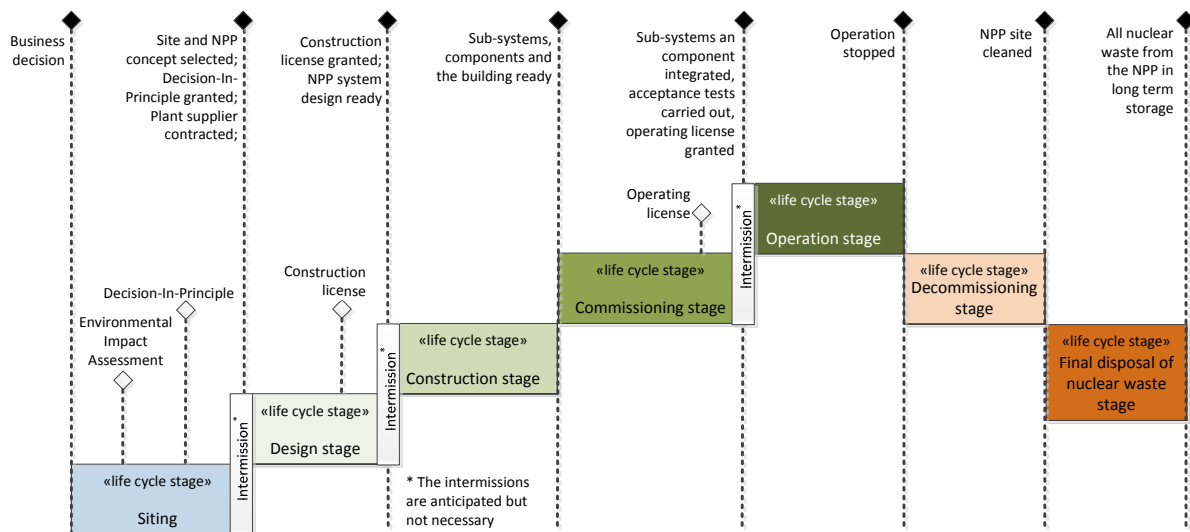


Figure 3. An example of a time window based life cycle model (a NPP life cycle model by the authors of this report).

The definitions for a life cycle and life cycle model can be found in Table 1.

ISO/IEC/IEEE 15288 [2015] does not explicitly define the concept of a life cycle stage.

The authors of this report favour the time window based life cycle model. Hence we define the concept of Life cycle stage as follows:

Life cycle stage: a time window within the life cycle of the system-of-interest. A life cycle stage has only one starting and one ending milestone. A life cycle stage exclusively occupies the time window assigned to it. NOTE: The consequence is that two or more life cycle stages cannot overlap.

In this sense, the concept of a life cycle stage is treated differently from ISO/IEC/IEEE 15288 (and ISO/IEC TR 24748-1) because the life cycle stages cannot be iterated (i.e. it is not

possible to go back in time). Instead, processes (and their activities and tasks) can be iterated. If a life cycle stage is defined such that it can be iterated, it may be a process instead of a life cycle stage.

Note that if the system operation is started, and it is noticed that the system does not work as expected, and re-development is started, it does not mean that the pre-operational life cycle stages are iterated; instead it means that a non-planned life cycle stage is entered. On the other hand, if the re-development after a short operation stage was planned, the particular re-development phase shall be a planned life cycle stage after the (trial) operational stage, or if the operation continues during the re-development, the operational stage simply uses the development phase processes.

If a car model is recalled due to a design defect, the car model is not put back to the development and production stages, but the operational stage is continued, and the development and maintenance processes are applied to fix the defect. If, however, operation of all the sold cars are forbidden before the defect is fixed, a non-planned life cycle stage of the car model is entered.

We claim that in the case of purpose-driven life cycle stages, the categorisation of life cycle stages provides poor added value due to the fact that life cycle stages that can be iterated should be defined as engineering processes instead of life cycle stages, or existing processes should be used. Whereas in the case of time window based life cycle stages, the project(s) can better be synchronised with the life cycle stages of the system-of-interest with clear decision gates and milestones³.

Due to the rationale above, the SEMP template created in this project applies the time window based life cycle model.

STUK defines the following life cycle stages (YVL-A.3-2-202) for a nuclear facility (see also Figure 3):

- siting
- design
- construction
- commissioning
- operation
- decommissioning of a nuclear facility
- final disposal of nuclear waste.

The life cycle stage titles above are not necessarily optimal for the time window based life cycle model but can, nevertheless, be used to define the life cycle stages of a NPP. In this context, however, we need to define the life cycle stages for NPP I&C systems. The resulted life cycle model is presented in Section 6.2.

Another important notion is the fact that in different contexts, there seems to be three different interpretations for the concept of a life cycle:

Case 1: Concept, Development, Production, Utilisation, etc. -life cycle stages

Case 2: Requirements definition, Architecture design, Detailed design, Implementation, etc. -life cycle stages (the so called V-model is a famous presentation of this)

³ Note that the system-of-interest and the project(s) that is (are) used to develop the system-of-interest have different life cycles; for example, the life time of a project is usually much shorter than the life time of its target system (system-of-interest). Project data and system data may thus have different archival requirements. Hence the data repositories for the project artefacts and system-of-interest artefacts should be kept separate where possible. This section deals with the system life cycles, not with project life cycles.

Case 3: System development, Sub-system selection or development, ..., Component selection or development -life cycle stages (this is also sometimes illustrated in the form of a V-model⁴)

It is important to understand how these three models go together. For example, Case 2 stages can be executed in the Case 1 stages Concept (e.g. with virtual models) and Development (real physical products), and they are executed in any of the Case 3 stages (for the system-of-interest, its sub-systems and components development). See Figure 4.

In this work, we consider only the Case 1 a life cycle model. We do not consider Case 2 a life cycle model because its phases are not life cycle stages, but systems engineering processes; we do not consider Case 3 a life cycle model, because its phases are not life cycle stages, but physical structure levels.

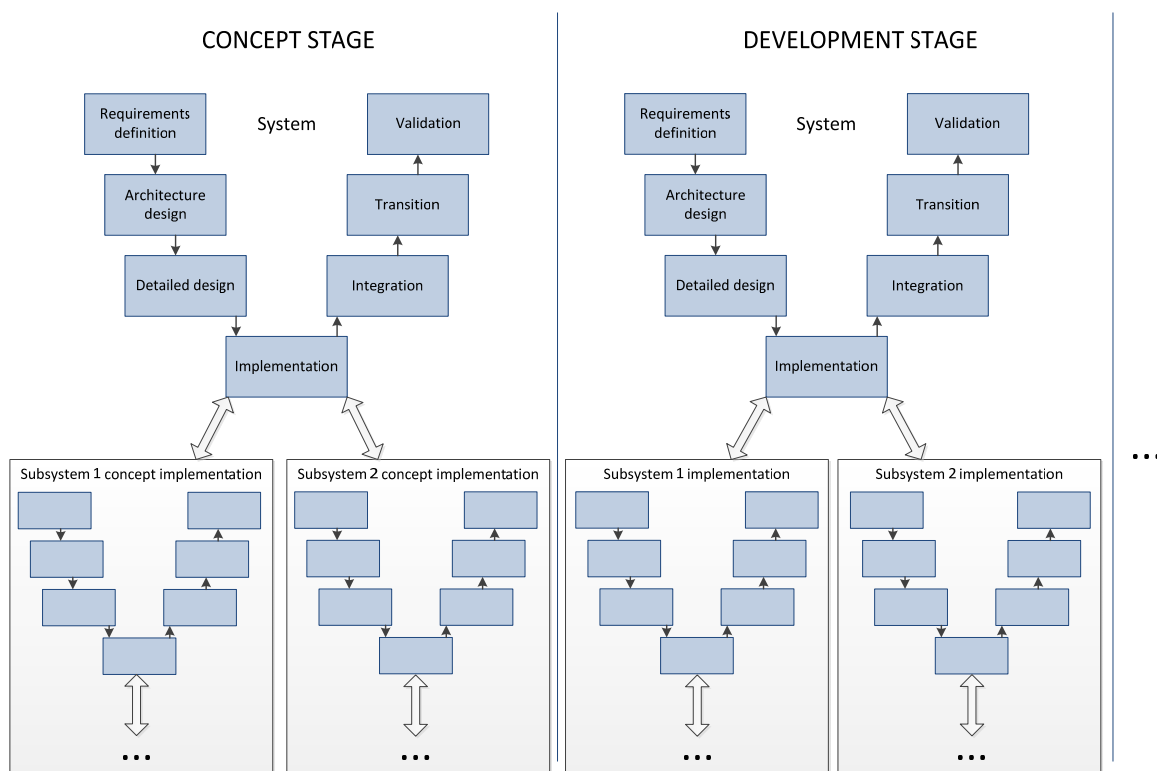


Figure 4. The three dimensional view of the progress of systems engineering work.

Nevertheless, we recognise the need for a 'life cycle model' that defines the order and iteration of the systems engineering processes; ISO/IEC/IEEE 15288 [2015] does not define such explicitly, but implicitly the sequence of execution of the processes, at least to some extent, can be captured from the SE processes; for example, the system requirements definition process cannot start before the stakeholder needs and requirements definition process is executed⁵. As pointed out above, we do not call here V-models and similar models life cycle models, because their phases are not life cycle stages, but processes. In fact, an explicit description of the flow of execution that traverses over several SE processes is a

⁴ In some cases, the two V-model presentations, case 2 and case 3 above, are mixed together. Such should be avoided.

⁵ It is not necessary to capture all the stakeholder requirements before system the requirements definition process starts, but it is necessary that at least a slice of the stakeholder needs are transformed to stakeholder requirements by a complete execution of the stakeholder needs and requirements definition process.

process by its very nature. The process constructs model of ISO/IEC/IEEE 15288 (in its Annex D) allows processes to have sub-processes; in this case we might name the explicit description of the flow of execution of the processes as a master process or a super process, but we call it a *processes execution model*. Nevertheless, whatever we call it, in case of NPP I&C systems, we may have to follow the IEC 61513 [2011] ‘life cycle model’ to be consistent with the standard. Hence the challenge is to map the IEC 61513 ‘life cycle stages’ to ISO/IEC/IEEE 15288 processes. The solution is presented in Section 6.6.

2.5 System life cycle processes

The ISO/IEC/IEEE 15288 [2015] standard defines processes to carry out the systems engineering work. These processes may be utilised during any stage of the system life cycle. The processes are grouped into four process groups: Agreement Processes, Organisational Project-Enabling Processes, Technical Management Processes, and Technical Processes. These process groups and processes are depicted in Figure 5.

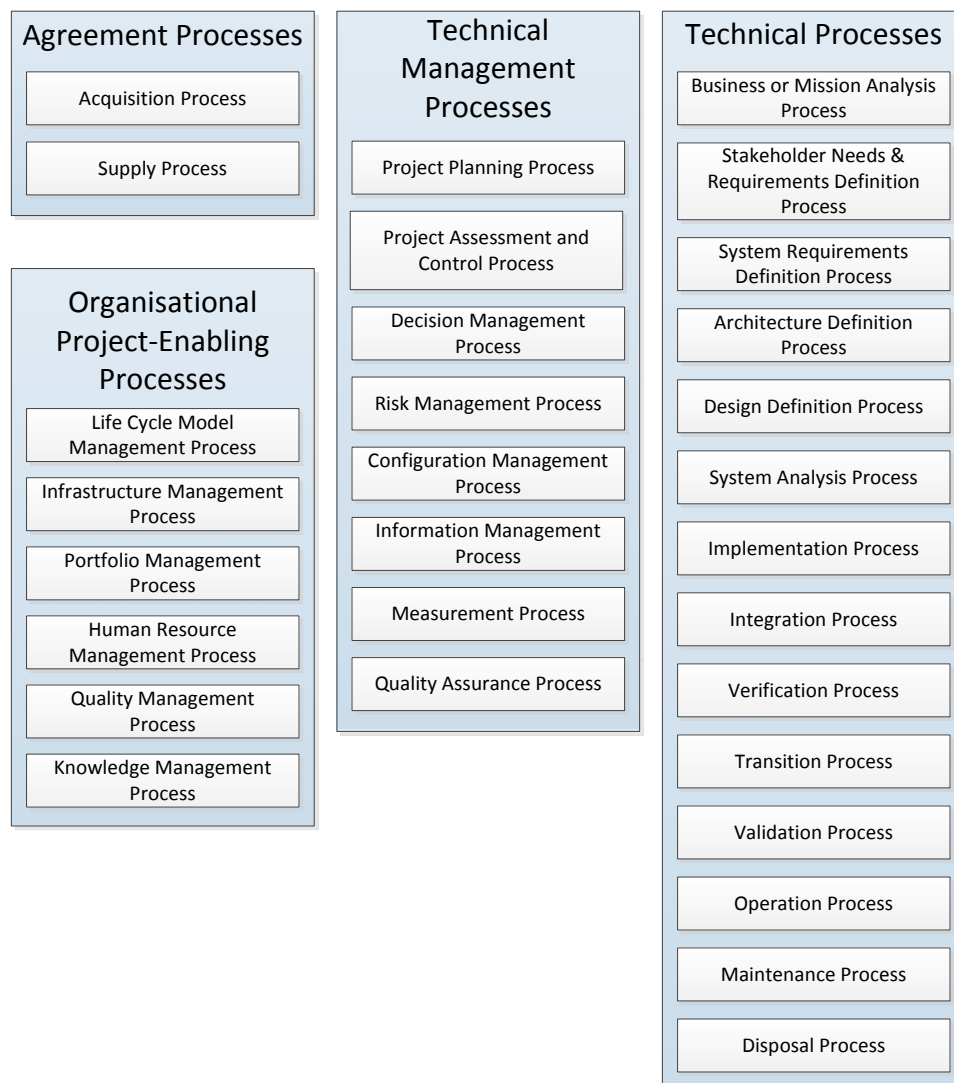


Figure 5. System life cycle processes [ISO/IEC/IEEE 15288 2015].

These processes are tailored according to the organisation and project in question. Tailoring may be needed over the system life cycle. The objective of tailoring is to optimise the performance of the systems engineering work to minimise cost and schedule overruns (see Figure 6).

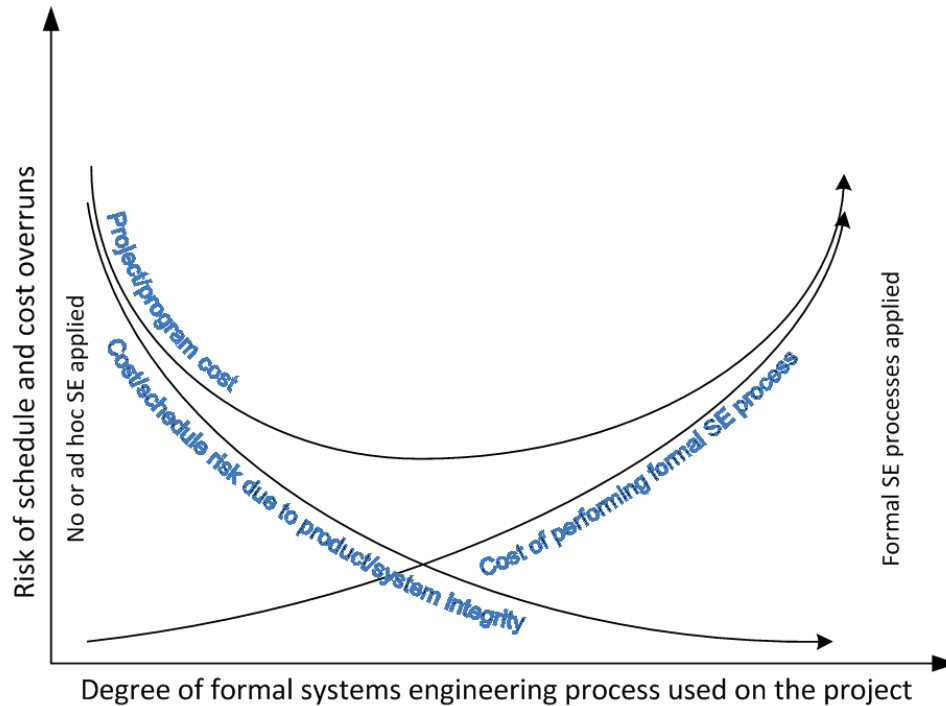


Figure 6. Optimisation of the SE processes tailoring [INCOSE 2015].

The optimum point, i.e. the minimum of the project or program cost, cannot always be achieved; for example, in case of safety critical systems, the degree of required formalism of the engineering processes may exceed the optimal cost point, i.e. the required safety integrity level could possibly be reached without excess formalism.

In this work, tailoring of the processes is not done according to the cost and schedule optimisation (due to lack of data), but to provide a set of SE processes that fits for the NPP I&C domain.

The systems engineering processes consist, according to ISO/IEC/IEEE 15288 [2015], of activities, and activities consist of tasks. The process constructs are depicted in Figure 7.

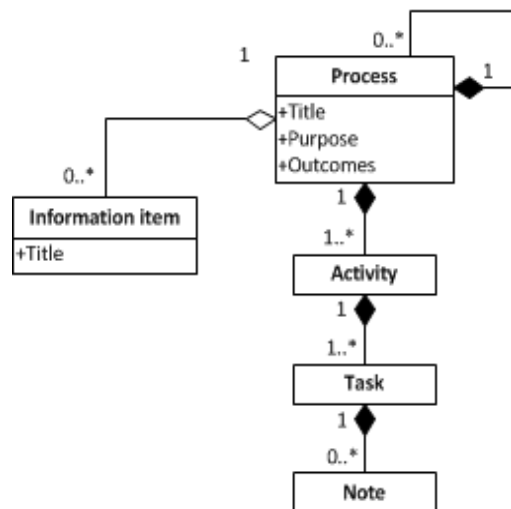


Figure 7. Process constructs (adapted from ISO/IEC/IEEE 15288 [2015] and ISO/IEC/IEEE TR 24774 [2010])⁶.

⁶ The process constructs model is not precisely the same in the two mentioned standards. ISO/IEC/IEEE 15288 uses composite aggregations (black diamonds) between process to process,

ISO/IEC/IEEE 15288 also introduces the concept of process view, which is the vertical view to the horizontal processes and/or their activities and/or their tasks (see the definition of process view in Table 1).

A typical method to model processes is the IDEF0 modelling method (see Figure 8).

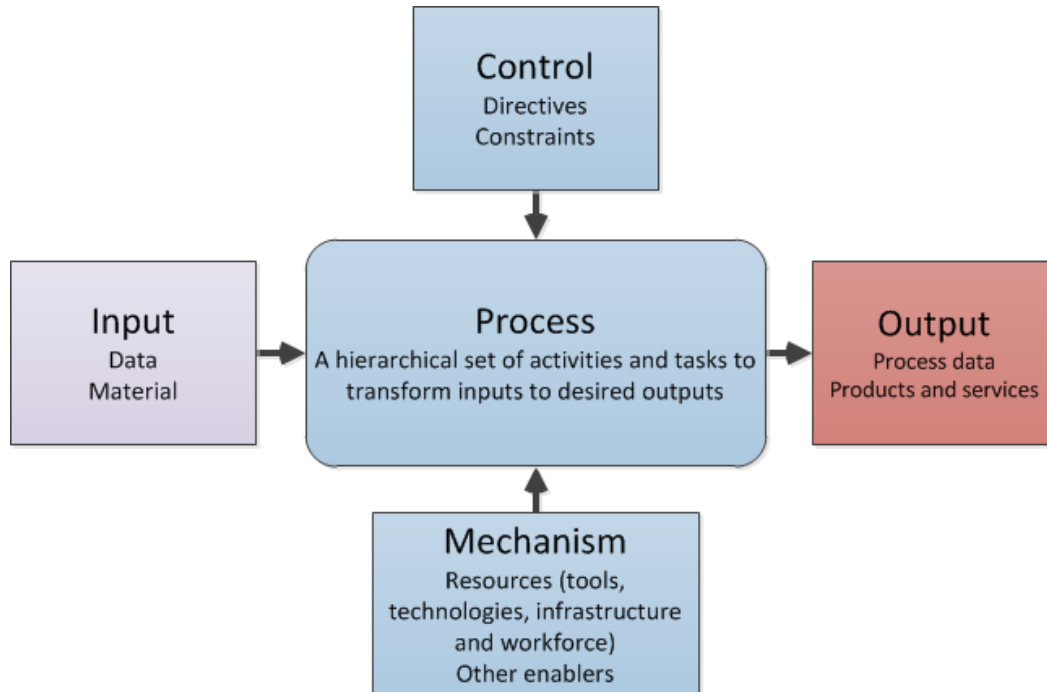


Figure 8. IDEF0 metamodel for processes.

ISO/IEC/IEEE 15288 [2015] does not explicitly define inputs, control and mechanisms for the processes, but the INCOSE handbook [INCOSE 2015] does⁷.

2.6 Systems engineering artefacts model

Another important model for successful engineering is the systems engineering artefacts model, i.e. the data and documents model. There are several models for this purpose, the most famous being ISO 10303-233 [2012]. In this context, however, we suggest using the Systems Engineering Artefacts Model (SEAModel_{NPP}) presented by Tommila & Alanen [2015]. The reason for the selection is that SEAModel_{NPP} is much easier to apply and implement than ISO 10303-233, and it provides thus an easy transition path from document centric systems engineering to model-based systems engineering.

2.7 Systems engineering literature

ISO/IEC 15288 (Systems and software engineering – System life cycle processes) is the main international standard for systems engineering. It “establishes a common framework of process descriptions for describing the life cycle of systems created by humans. It defines a set of processes and associated terminology from an engineering viewpoint”. [ISO/IEC/IEEE 15288 2015]

process to activity and activity to task, whereas ISO/IEC/IEEE TR 24774 uses shared aggregations (empty diamonds); furthermore, ISO/IEC/IEEE TR 24774 does not require that an activity always has at least one task, whereas ISO/IEC/IEEE 15288 requires it.

⁷ INCOSE calls the metamodel IPO (Input-Process-Output) model instead of IDEF0 and rephrase ‘Mechanisms’ as ‘Enablers’.

ISO/IEC/IEEE 12207 (Systems and software engineering – Software life cycle processes) can be called a “daughter standard” of the ISO/IEC/IEEE 15288 standard. ISO/IEC/IEEE 12207 is similar to ISO/IEC/IEEE 15288:2015 but concentrates on the software engineering. [ISO/IEC/IEEE 12207 2008]

The International Council on Systems Engineering (INCOSE) has published a handbook titled “INCOSE Systems Engineering Handbook” It *“defines the discipline and practice of systems engineering (SE) for students and practicing professionals alike and provides an authoritative reference to understand the SE discipline in terms of content and practice.”* [INCOSE 2015]. INCOSE handbook supplies elaborate guidance on the use of ISO/IEC/IEEE 15288.

Another interesting document is the NASA Systems Engineering Handbook. The NASA handbook is an extensive document to give guidance and information of for instance systems engineering processes, tools, technique and best practises. [NASA 2007]

Yet another comprehensive source of information is the SEBoK (Systems Engineering Body of Knowledge) published as a set of wiki pages. [SEBoK 2015]

A book titled “A look into the life-cycle design of complex systems” (published by VTT) presents methods and approaches that could help integrating tools, processes and systems thinking to achieve successful and sustainable products, considering all aspects of the product life cycle. The methodologies presented in the book include Systems Engineering (SE), Product Life Cycle Management (PLM), model-based approaches, virtual prototyping, requirements management and related approaches. [Granholm 2013]

2.8 Requirements engineering

Requirements engineering is one of the core disciplines of systems engineering. It covers the following tasks:

- **requirements capture** (identifying stakeholders, eliciting the customer problem domain, collecting the regulatory requirements)
- **writing requirements** (systematic recording of stakeholder and system requirements, good quality sentences, requirements models and diagrams)
- **verification and validation of requirements** (ensuring that the requirements are proper and reflect perfectly the customer needs)
- **requirements analysis** (assessing the requirements and expressing them in a well-formed and measurable way to engineers that will develop the target system or service)
- **communication of requirements** (to engineers and stakeholders; several presentation formats may be needed)
- **refining and allocation of requirements** (allocation to hardware, software, sub-systems, etc.)
- **requirements management** (identification of requirements, organisation, classification, prioritisation, support for V&V, work flow control, version control, traceability control, and collaboration arrangements).

The STUK YVL guide YVL B.1 [Guide YVL B.1 2013] sets requirements for the NPP requirements engineering process in its Section 3.5. The requirements are as follows:

“336. The requirements concerning systems important to safety of the nuclear facility shall be defined to such a level of detail that a designer independent of the requirement specification

process is able to carry out the re-design required for the in-service maintenance of the system its components as well as their modifications throughout the life cycle of the facility.

337. Requirements that are not considered functional requirements, such as the applicable quality requirements and standards, shall also be specified.

338. The applicability of the referenced standards and guidelines shall be justified. If an exception is made to a specified standard or guideline, such a departure shall be justified and its effect assessed.

339. The requirement specifications shall be unambiguous, consistent and traceable. It shall be possible to verify the fulfilment of the requirements.

340. The accuracy, completeness and consistency of the requirement specification of systems important to safety shall be assessed by experts who are independent of the design and implementation process. The assessment report shall present the observations made as well as a justified conclusion.

341. The traceability of the requirements in the various design stages shall be demonstrable. The traceability of the requirements in the various design stages shall be demonstrated as part of the qualification.”

Especially the traceability requirements (339 and 341 above) prompt to use a dedicated requirements management tool. A common tool in nuclear industry is the IBM Rational DOORS (9.x) tool. However, STUK has decided to use the Polarion software tool to manage STUK requirements. Spreadsheet and text processing tools are not the tools to manage requirements of complex systems. The problem with the spreadsheet and word processing files is in the fact that such files often are distributed as e-mail attachments causing several copies of the requirements set. This always leads to version control problems.

To support traceability of requirements and other engineering artefacts, a traceability information model (TIM) is required. Figure 9 depicts an example TIM for requirements and its relations to other engineering artefacts. It shall be possible to implement such traces with the selected requirements management tools; DOORS and Polarion mentioned above both provide this possibility. Product life cycle management (PLM) tools also provide very sophisticated traceability of virtual engineering artefacts. Sufficient traceability can be arranged even with the MS SharePoint content management tool.

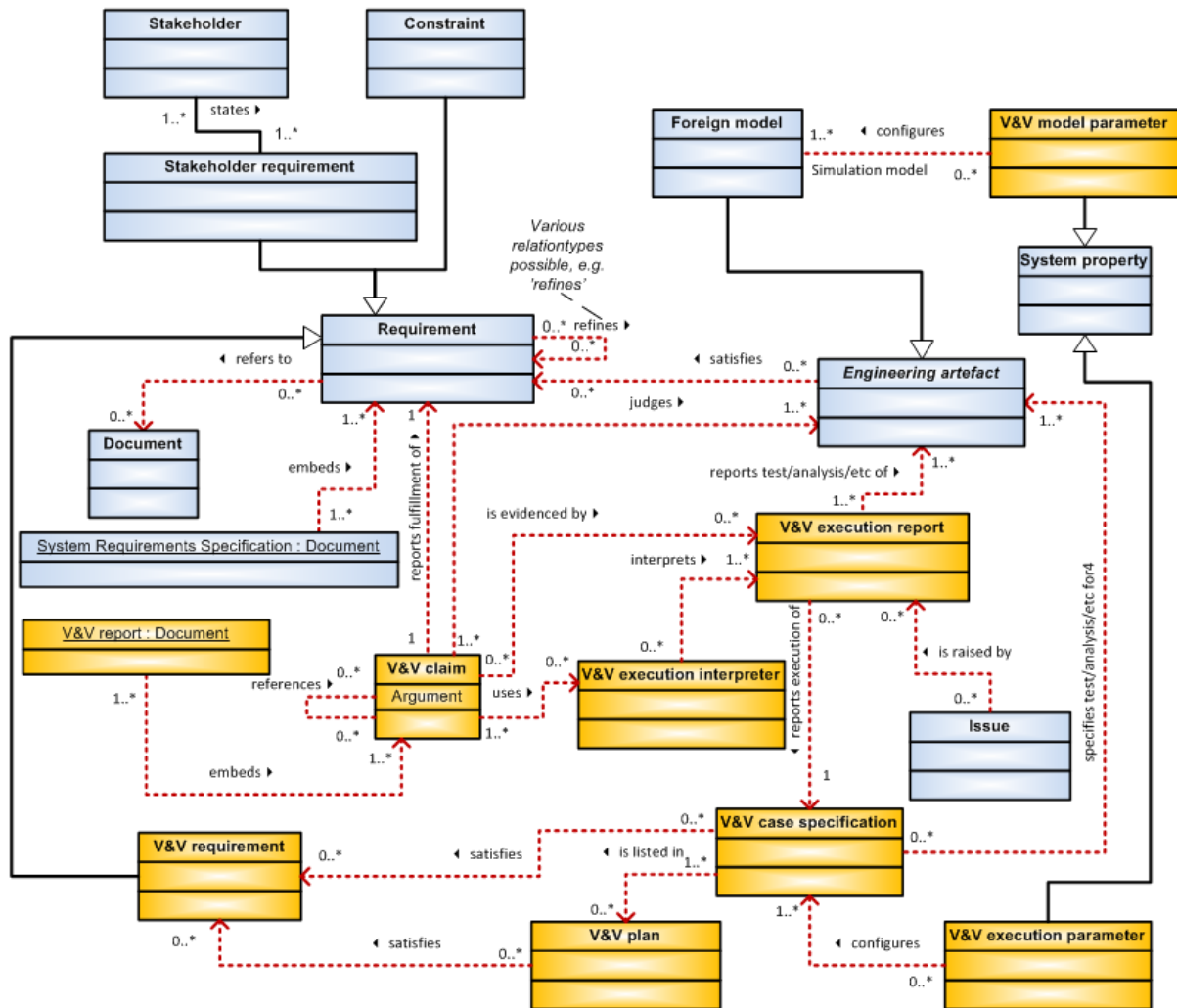


Figure 9. A traceability information model (TIM) for tracing requirements [Tommila & Alanen 2015].

The NPP automation SEMP shall address the systems engineering artefacts model to provide traceability. In this context, it is suggested to apply the systems engineering artefacts model (SEAModel_{NPP}) presented in [Tommila & Alanen 2015].

2.9 Collaboration between organisations

Traceability of requirements, safety demonstration and other engineering artefacts is challenging within an organisation, but it becomes even more challenging in the contractor – subcontractor networks.

Below in Figure 10, the example case of transferring requirements and V&V (verification and validation) through the ISO/IEC/IEEE 15288 system hierarchy is depicted. The flow of requirements goes top down and the flow of verification and validation information bottom up.

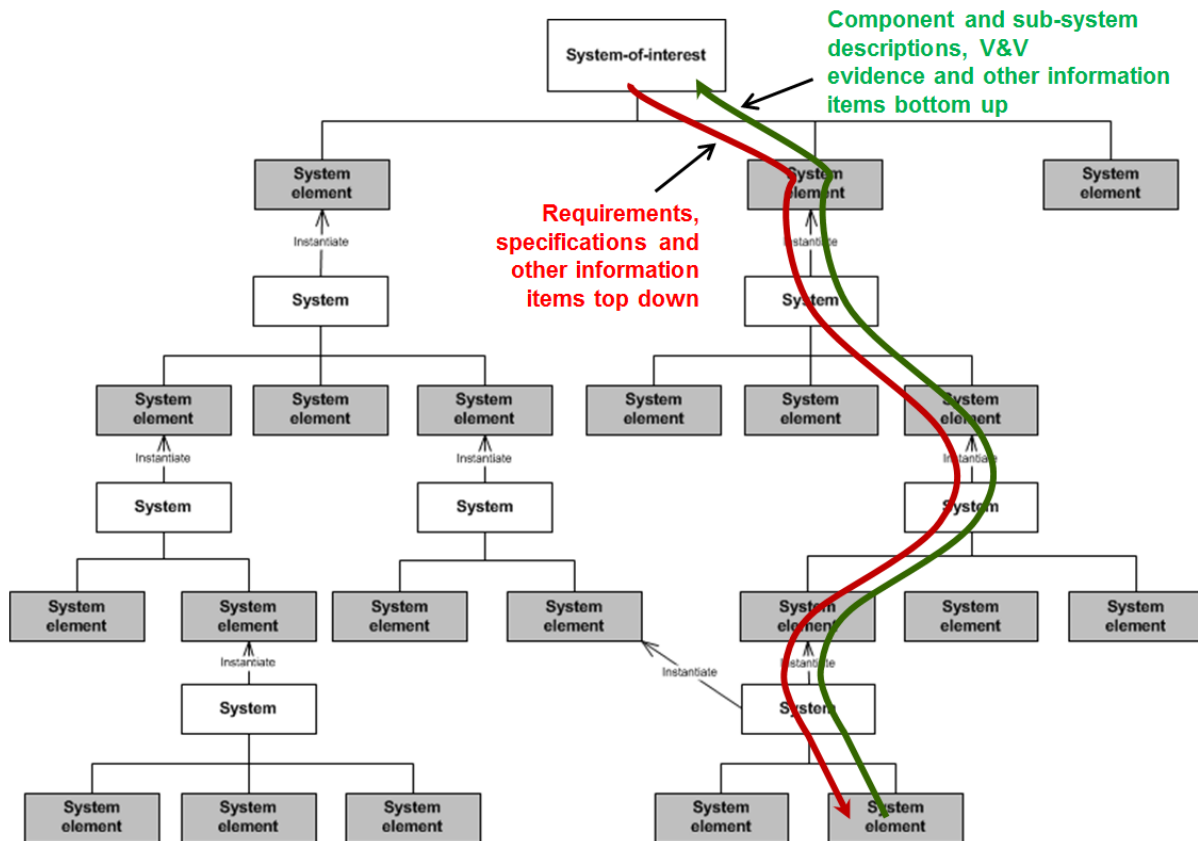


Figure 10. A system structure model by ISO/IEC/IEEE 15288 and the flow of information in the contractor – subcontractor chains.

To facilitate such information chains, the following aspects shall be considered:

1. The organisations involved in the development may have different kinds of tools for requirements management and other activities. Hence an information item transfer procedures need to be specified. For requirements transfer, OMG has specified a file format (ReqIF) to transfer requirements between requirements tools from different vendors. The ReqIF specification is based on the XML specification. For other tools, such as safety demonstration tools, XML file format is suggested, if access to shared project data repository cannot be granted for all the relevant parties.
2. The organisations have different types of roles for the people doing systems and requirements engineering. Hence the roles should be clearly communicated to each participating organisation.
3. The organisations have different work practices and understanding of the concepts. Hence, the contractor should take care of consistent view of concepts and the requirements engineering process.
4. The collaboration model between the organisations should be carefully designed, and the information systems should support well the collaboration model.

A typical artefact created during the systems engineering processes is a requirements specification, e.g. System Requirements Specification (SyRS). It should be noted, however, that in the model-based systems engineering (see Section 2.10), the importance of the traditional requirements specifications documents is lower than in document based engineering. This is due to the fact that engineers work directly with the (requirements) engineering tools (i.e. a single requirement is an individual work item); a requirements specification in that case could be an automatically generated document for the purpose of qualification or archiving. Nevertheless, the change of the mind-set from document based engineering to model-based engineering still takes time until the social media generation

takes place in systems engineering management. Therefore, the main challenge in requirements engineering is to provide tools that make the life of document oriented engineers easier than with word processing and spreadsheet tools.

The future needs in systems engineering considering the NPP automation SEMP are the following:

- Networking of large number of organisations calls for a well-designed collaboration model and information management tools that are easy to use by engineers with different levels of skills.
- The long timescale causes problems in the transfer of tacit information from a generation to another. Hence the rationale of the requirements and the selection criteria of the design solutions shall be recorded in a way that supports easy search of the background information.

2.10 Model-based systems engineering

ISO/IEC/IEEE 42010 [2011] defines a model as follows:

“M is a model of S if M can be used to answer questions about S.”

In that sense, all kinds of typical engineering work products (artefacts) that are created to specify or describe a system are models. This would make all systems engineering to be model-based systems engineering. To make the difference in this context, we use the definition by INCOSE for model-based systems engineering:

“Model-based systems engineering (MBSE) is the formalized application of modeling to support system requirements, design, analysis, verification and validation [activities] beginning in the conceptual design phase and continuing throughout development and later life cycle phases.” [Friedental et al. 2007]

The difference here to the traditional SE is in the use of formalised or semi-formalised, machine readable, models or virtual engineering artefacts instead of word processing documents to specify and describe the system-under-study. This does not mean that documents are not used in MBSE, but it means that MBSE **is not based on** documents but on formalised or semi-formalised or visual models. As a consequence, the role of documents changes: in MBSE, the documents are a means to present information (including models) instead of being containers of information. This fact encourages using automatic or semi-automatic document generation, which is not possible in traditional SE.

Also the structure and relations of the work products should be modelled (see Figure 11). Furthermore, the context of the system, including domain concepts, humans, external systems, environment and the technical processes, can be modelled.

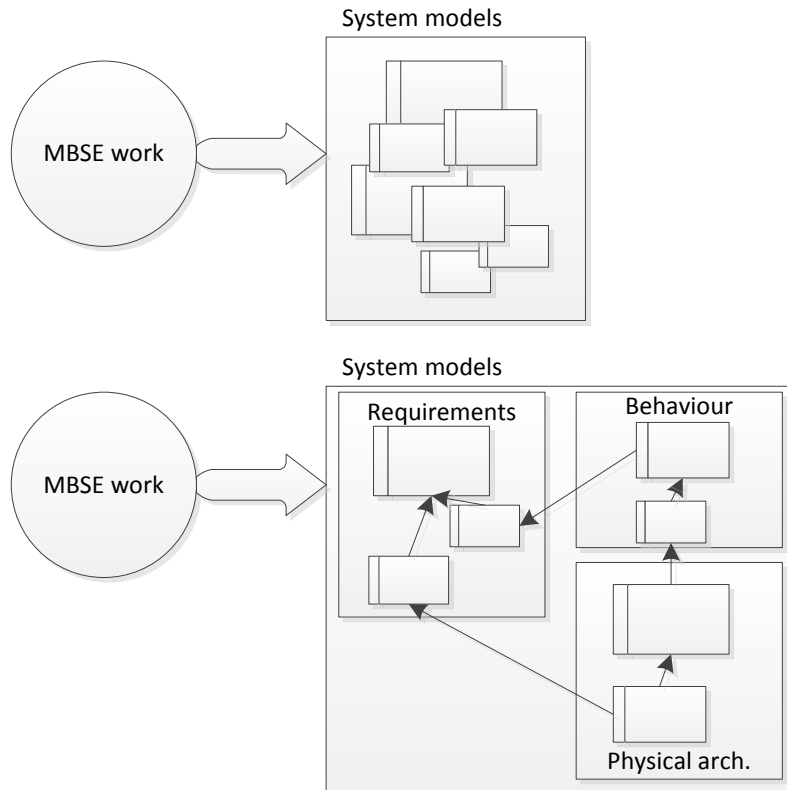


Figure 11. Non-systematic (upper diagram) vs. systematic (lower diagram) organisation of work products (including models).

INCOSE lists the following MBSE benefits [Friedental et al. 2007]:

“MBSE enhances the ability to capture, analyse, share, and manage the information associated with the complete specification of a product, resulting in the following benefits:

- Improved communications among the development stakeholders (e.g. the customer, program management, systems engineers, hardware and software developers, testers, and specialty engineering disciplines).
- Increased ability to manage system complexity by enabling a system model to be viewed from multiple perspectives, and to analyse the impact of changes.
- Improved product quality by providing an unambiguous and precise model of the system that can be evaluated for consistency, correctness, and completeness.
- Enhanced knowledge capture and reuse of the information by capturing information in more standardized ways and leveraging built in abstraction mechanisms inherent in model driven approaches. This in turn can result in reduced cycle time and lower maintenance costs to modify the design.
- Improved ability to teach and learn systems engineering fundamentals by providing a clear and unambiguous representation of the concepts.”

These are vital aspect also in NPP domain. MBSE is not unfamiliar to current NPP and waste management system developments, but the degree of systemic thinking in playing with the models can be increased to exploit the full benefits of MBSE.

The SEMP (template) for NPP I&C systems created in this context follows the principles of MBSE in the sense that storing information in documents is tried to be avoided. Instead, the information is stored in a structured way in a database. This means that the NPP I&C systems SEMP (template) issued in this context is not a word processing document template, but a database oriented application using wiki pages to present the database data. The MS SharePoint application is used for the purpose (see Chapter 6).

3. Current systems engineering practices

In the following five sections, example systems engineering practices are presented. The SE practices of ITER and F4E (ITER European domestic agency) (Sections 3.1 and 3.2 respectively) are selected because the complexity of the ITER project and the reactor itself well reflects the complexity of traditional NPP projects and plants; Rosatom (Section 3.3) was selected due to the fact that Rosatom is the selected plant supplier for the Finland's latest NPP project, Hanhikivi 1 (Fennovoima); U.S. Department of Defence was selected to provide an overview of possible SE processes and an example of the table of contents of a systems engineering plan (Section 3.4 and Appendix 3); and U.S. Department of Transportation Systems Engineering Guidebook was selected to point out that the SEMP itself is an outcome of a process (Section 3.5).

3.1 ITER–SEMP

(With review by Alain Guigon, Systems Engineering Processes Officer, the author of the ITER SEMP, and Ryan Wagner, Industrial Controls Coordinator, both from ITER Organisation, and approved by Daniele Parravicini, Section leader at ITER Organisation.)

The ITER project is an international project to create the first fusion reactor to produce net energy. Due to the complex design and complex procurement scheme of the ITER fusion reactor, ITER Organization (IO) has chosen to apply the systems engineering approach, especially the ISO/IEC/IEEE 15288:2008 and ISO/IEC 26702 [2007] process models.

IO has created an ITER Systems Engineering Management Plan (ITER SEMP) [ITER 2009] to describe the systems engineering processes and management practices to be used by the ITER project. ITER SEMP is a daughter document of the ITER Project Management and Quality Plan.

The ITER SEMP process set is characterised as a *“group of processes which govern the construction and delivery of the ITER Plant with the agreed Quality”*.

ITER SEMP includes the following topics:

- Systems engineering process for ITER
- ITER project's description
- ITER SE participants (including role definitions and responsibilities)
- ITER generic life cycle
- Mapping of ITER SE processes to management processes, technical core processes, and specialty engineering processes and disciplines
- Description of ITER SE processes.

The ITER life cycle model includes construction (includes design), operation, deactivation, and decommissioning main phases. IO has defined six lifecycle stages⁸ with predefined engineering maturity levels. (IO has adapted the life cycle stage model from EN 2900, currently ISO 14300, Space systems – Programme management.) There are six decision gates (Figure 12), which control the continuation of the project from one stage to another (or from one activity to another within a stage). IO applies the life cycle model at the ITER project level and to contracting of the development and realisation of the systems and subsystems.

⁸ IO distinguishes between the phase and stage such that a phase is a period within the project and a stage is a product maturity reached.

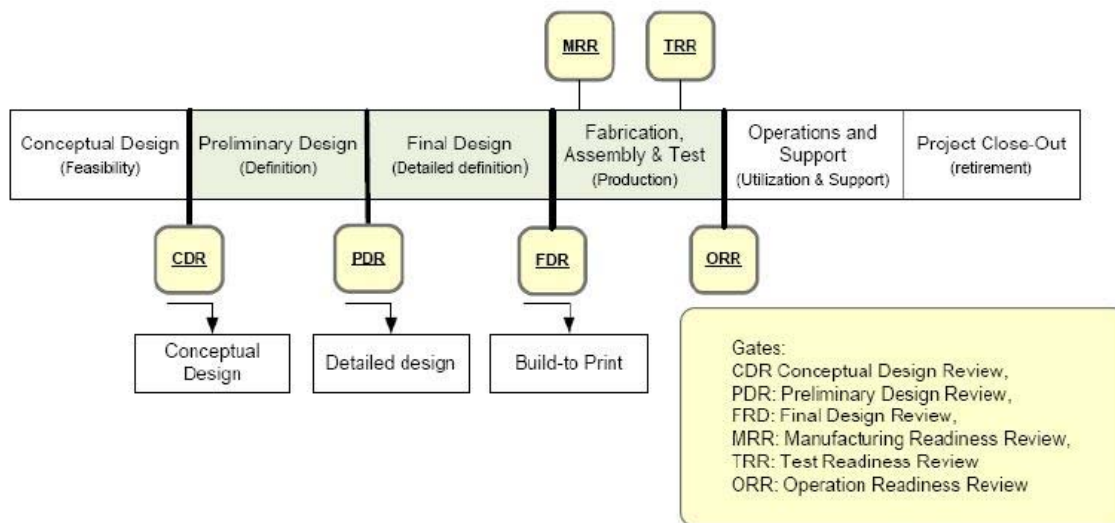


Figure 12. ITER project life cycle and maturity levels of the design [ITER 2009]. (IO is planning to add a construction readiness review CRR.)

The ISO/IEC/IEEE 15288:2008 process model is used as a reference for the ITER SE processes, but the process model has been tailored for ITER. The ITER SE processes are presented in Figure 13.

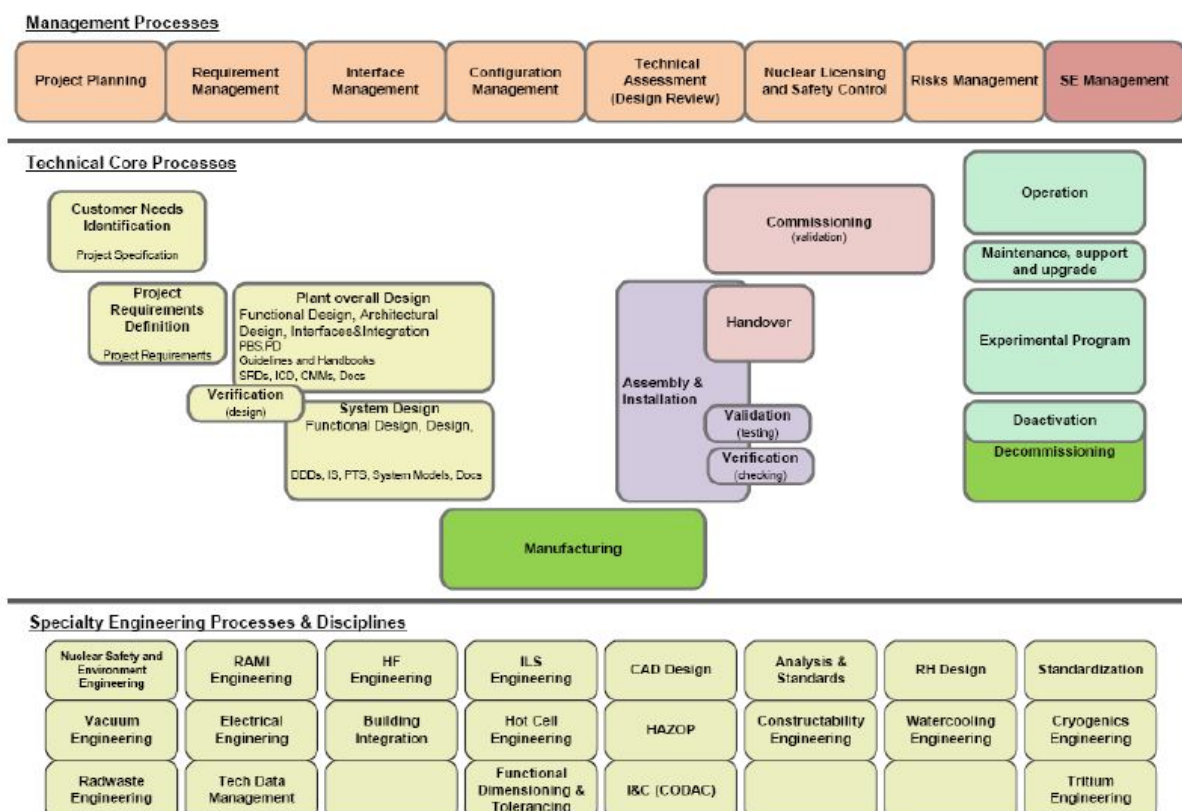


Figure 13. ITER systems engineering processes [ITER 2009].

ITER SEMP supplies a conformity matrix (Table 4) to claim conformity of the tailored set of ITER SE processes with the ISO/IEC/IEEE 15288:2008 processes. The process group⁹ and

⁹ The process groups in the conformity matrix are not the same as in Figure 13; this will be changed in the next SEMP version.

the ID (in the order of appearance in the ITER SEMP) of each of the processes are also provided.

Table 4. Conformity matrix of ITER SE processes [ITER 2009].

ISO 15288:2008 SE process	ITER SE process	ID	Process groups
Project planning process	Project planning process	5	Management
Project assessment	Technical Assessment (Design Review)	10	
Risk management	Risk management	11	
Safety control process	Nuclear Licensing and Safety Control	4	
Configuration Management	Configuration Management	8	
	Requirement Management	6	
Information Management	Technical Data Management	9	
Interface Management	Interface Management	7	
Project Lifecycle Mgt	SE Management	21	
Stakeholder Requirement definition	Customer needs Identification	1	Engineering & Design
Requirements analysis	Technical Requirements Definition	2	
Architectural design	Requirement Management Plant and System Design	3	
Acquisition	Procurement		Procurement
Investment Management	Procurement arrangements		
Implementation	Manufacturing	12	Manufacturing & Installation
Integration	Assembly and Installation	13	
Verification	Verification & Validation	14	
Transition	Handover	16	
Validation	Commissioning (validation)	15	Commissioning
Operation	Operation Experimental Program	17 18	Operation
Maintenance	Maintenance, support and upgrade	19	Maintenance
Disposal	Decommissioning	20	Decommissioning
Specialty Engineering	Nuclear Safety and Env. engineering	21	Support
	RAMI management	22	
	Human factors management	23	
	ILS management	24	
	CAD design management	25	
	Analysis & Standards management	26	
	Standardization management	27	
	Value engineering	28	
	Vacuum engineering	29	
	Electrical engineering	30	
	Building Integration management	31	
	Hot cell engineering	32	
	I & C (CODAC) Engineering	33	
	Constructibility management	34	
	Remote Handling Engineering	35	
	Cooling Water Engineering	36	
	Cryogenics Engineering	37	
	Tritium Engineering	38	
	Radwaste Engineering	39	
	HAZOP	40	

Abbreviations in the table above: CAD = Computer Aided Design; HAZOP = Hazard and Operability Study; I&C (CODAC) = Instrumentation and Control (Control, Data, Access and Communication); ILS = Integrated Logistics Support; SE = Systems Engineering; RAMI = Reliability, Availability, Maintainability and Inspectability

IO describes the SE processes according to the structure shown Table 5.

Table 5. ITER process descriptions template [ITER 2009]. (The pieces of text in brackets by the authors of this report based on the actual ITER SEMP process descriptions.)

<Process name>	
Reference	<i>Programmes and procedures that illustrate the process or output of the process</i>
Purpose	<i>Describes the goals of performing process</i>
Scope	<i>The area covered by the process: product system to be studied; functions, system boundaries...;</i>
Outlines (Activities & Tasks)	<i>Sets of cohesive tasks of the process Derived from ISO 15288 and tailored to IO Project</i>
Owner	<i>Person who has the ultimate responsibility for the performance of a process in realizing its objectives measured by key process indicators, and has the authority and ability to make necessary changes.</i>
Customer	<i>Recipient of the output</i>
Supplier	<i>Provider of the input</i>
User	<i>Person in charge of the application of the process for his own purpose</i>
Support	<i>[The support provided or needed by the participating organisations]</i>
Comment	<i>[Any comments about the responsibilities]</i>
Input	<i>Contents and maturity of the information needed to run the process</i>
Output	<i>Express the observable results expected from the successful performance of the process</i>
Associated data	<i>[Data, e.g. documents, other than input and output data associated with the process]</i>
Comments	<i>[Any comments about the data involved]</i>

The SEMP's of all the participants of the ITER project, including the suppliers, shall be aligned with the ITER overall SEMP. The ITER SE processes are applied by the suppliers of the system elements (subsystems and components) to suitable extent and tailoring depending on the level of maturity and availability of the systems elements under engineering. IO agrees about the tailoring with the particular suppliers.

The table of contents of the ITER SEMP is presented in Appendix 1.

3.2 Fusion for Energy (F4E) SEMP

(With review and permission by Gonalo Serra, F4E, the author of the F4E SEMP.)

Fusion for Energy (F4E) is the European domestic agency for the ITER project. F4E is responsible for the European contribution to the ITER fusion reactor. In various configurations and depending on the components, the domestic agencies are responsible for the design and/or fabrication (procurements) and/or testing, and are thus only involved in the construction phase of the ITER machine. Compared to the regular nuclear power plant projects, ITER Organisation (IO) is the licensee, nuclear operator and also design authority, whereas the domestic agencies are its main suppliers (systems' suppliers), and the companies are the suppliers.

IO requires the domestic agencies to apply SE processes. F4E has thus created a systems engineering management plan [F4E 2011] that is harmonised with the ITER SEMP. F4E requires the suppliers to follow the F4E SEMP when creating system and subsystem specific project plans. The F4E SEMP is presented here because it works as a good example of a practical case in which a contractor organisation has to follow its customer (here: IO) SE practices but on the other hand, requires its subcontractors (here: suppliers) to follow the SE practices of the contractor (here: F4E). This three level hierarchy is well illustrated in Figure 14 by the colouring scheme.

The F4E SEMP follows the ITER life cycle model (construction, operation, deactivation and decommissioning), but divides explicitly the construction phase into two phases,

- Design: conceptual design (output: functional specification), preliminary design (output: detailed design), final design (output: build-to-print)
- Fabrication, Assembly & Test.

The ISO/IEC/IEEE 15288:2008 process model is used as a reference for the F4E SE processes, but the process model has been tailored for F4E based on the ITER process model. The F4E SE processes are presented in Figure 14.

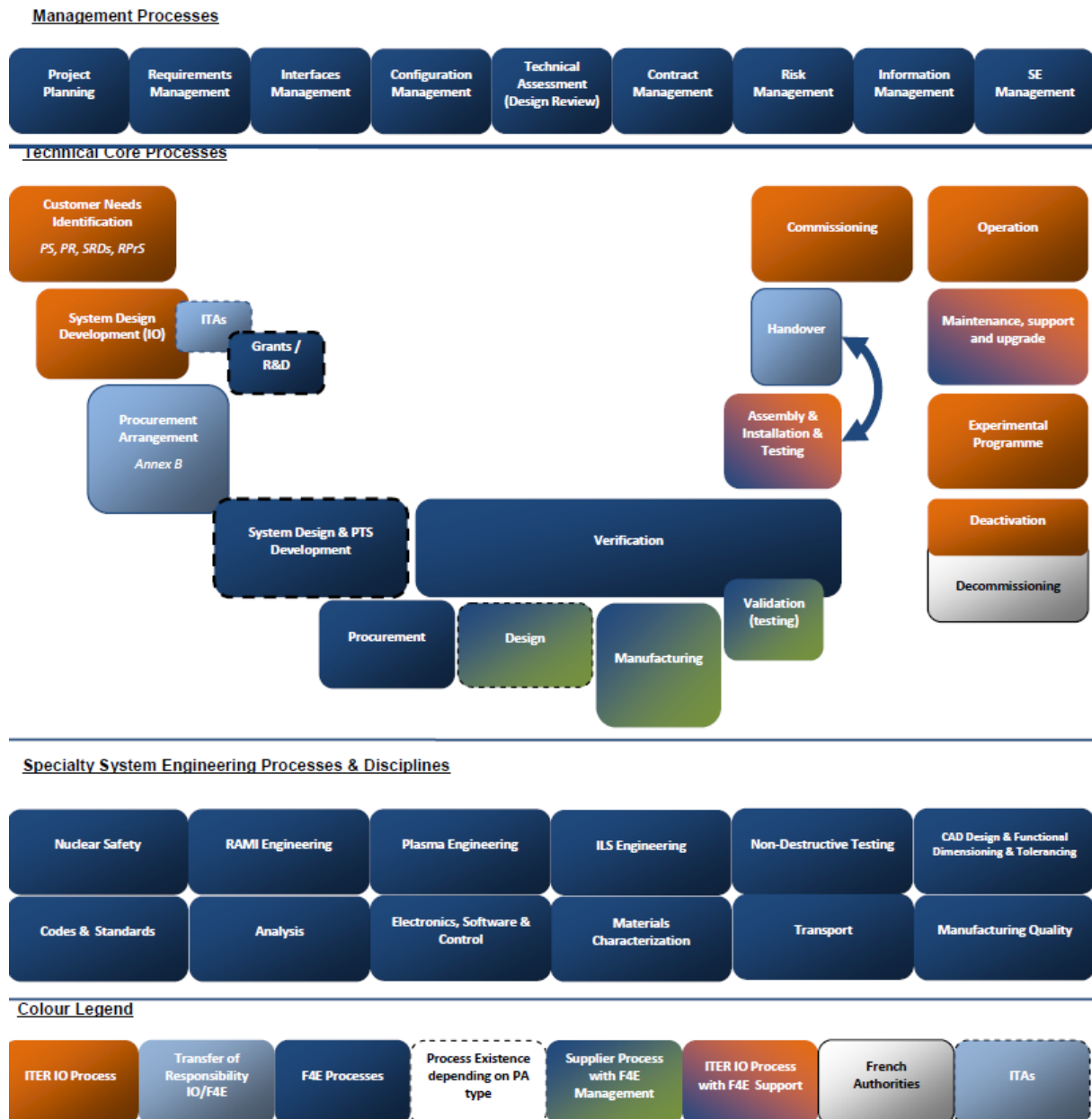


Figure 14. F4E systems engineering processes [F4E 2011].

F4E categorises the SE processes as depicted in Figure 14: Management Processes, Technical core processes and Specialty System Engineering Processes & Disciplines.

F4E formulates the SE process descriptions according to Table 6.

Table 6. F4E process descriptions template [F4E 2011]. (The pieces of text in brackets are by the authors of this report.)

<Process name>	
Reference	<i>Programmes and procedures that illustrate the process or output of the process</i>
Purpose	<i>Describes the goals of performing process</i>
Scope	<i>The area covered by the process: product system to be studied; functions, system boundaries...;</i>
Outlines (Activities & Tasks)	<i>Sets of cohesive tasks of the process Derived from ISO 15288 and tailored to IO Project</i>
Owner	<i>Person who has the ultimate responsibility for the performance of a process in realizing its objectives measured by key process indicators, and has the authority and ability to make necessary changes.</i>
Customer	<i>Recipient of the output</i>
Supplier	<i>Provider of the input</i>
User	<i>Person in charge of the application of the process for his own purpose</i>
Support	<i>[The support provided or needed by the participating organisations]</i>
Comment	<i>[Any comments about the responsibilities]</i>
Input	<i>Contents and maturity of the information needed to run the process</i>
Output	<i>Express the observable results expected from the successful performance of the process</i>
Associated data	<i>[Data, e.g. documents, other than input and output data associated with the process]</i>
Comments	<i>[Any comments about the data involved]</i>

The F4E SEMP supplies a conformity matrix (Table 7) to claim conformity of the tailored set of the F4E SE processes with the ISO/IEC/IEEE 15288:2008 processes. The process group¹⁰ and the ID (in the order of appearance in the F4E SEMP) of each of the processes are also provided; furthermore, the responsible party is identified in the rightmost column.

¹⁰ The process groups in the conformity matrix are not the same as in Figure 14.

Table 7. Conformity matrix of F4E SE processes [F4E 2011].

ISO 15288:2008 SE process	F4E Process name	ID	Process group	F4 / ITER Organisation (IO)
Project planning	Project Planning	1	Management	F4E
Interface Management	Interfaces Management	3		
Configuration Management	Requirements Management	2		
	Configuration Management	4		
Project Assessment	Reviews	5		
Risk Management	Risk Management	7		
Information Management	Data Management	8		
Project Lifecycle Mgmt	Systems Engineering Management	9		
Stakeholder Requirement Definition	Customer needs identification		Engineering & Design	IO
Architectural Design	System Design Development (IO)			F4E
	System Design Development	12		[?] ¹¹
Requirements Analysis	Procurement Technical Specification	13		
Investment Management	Contract & Supplier management & Control	6	Procurement	F4E
Supply	ITAs	10		
Supply	PAs	11		
Acquisition	Procurement	14		
Implementation	Manufacturing	16	Manufacturing & Installation	F4E
Verification	Verification	15		
	Validation	17		
Integration	Assembly, Integration & Testing	18		
Transition	Handover	19		F4E
Validation	Commissioning		Commissioning	IO
Operation	Operation		Operation	IO
	Experimental Program			
Maintenance	Maintenance, support & upgrade	20	Maintenance	F4E
Disposal	Deactivation / Decommissioning		Decommissioning	IO
Specialty Engineering	Nuclear Safety and Environment engineering	21	Support	F4E
	RAMI engineering	22		
	Plasma engineering	23		
	Integrated Logistics Support Engineering	24		
	Non-Destructive testing	25		
	CAD Design and Functional Dimensioning & Tolerancing	26		
	Codes & Standards	27		
	Analysis	28		
	Electronics, Software & Control	29		
	Materials Characterization	30		
	Transport	31		
	Manufacturing Quality	32		

Abbreviations in the table above: CAD = Computer Aided Design; ITA = ITER Task Agreement; PA = Procurement Agreement; SE = Systems Engineering; RAMI = Reliability, Availability, Maintainability and Inspectability

The table of contents of the F4E SEMP is presented in Appendix 2.

¹¹ Not specified in the F4E SEMP.

3.3 Rosatom

Belov et al. [2012] defines a model for the NPP development process and the associated tools, and calls it NPPDS (Nuclear Power Plant Development System) for Rosatom VVER-TOI projects. NPPDS is created using systems architecting methods according to ISO/IEC/IEEE 42010 [2011], and it adopts ISO/IEC/IEEE 15288 [2008] and ISO 15926 [2004]. Belov et al. [2012] do not clearly state, if a systems engineering management plan (SEMP) has been created. Nevertheless, NPPDS answers basically to the same question as a SEMP does.

NPPDS is a systems engineering platform for the design phase of a VVER reactor. One of the main goals in the creation of NPPDS has been to facilitate easy re-use of design artefacts in later NPP designs (see Figure 15).

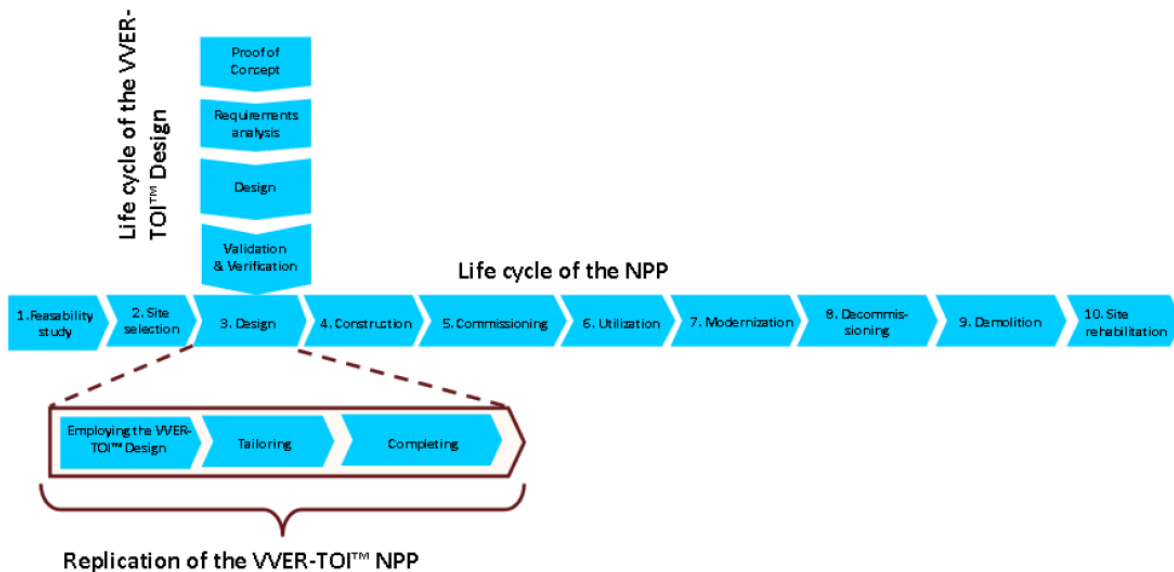


Figure 15. The life cycle models of a VVER-TOI project (two scenarios) and the target NPP; note that the target system of a VVER-TOI project is the NPP design data and documents, not the real NPP, i.e. the real NPP project uses the results of the VVER-TOI project in the design phase. [Belov et al. 2012].

Belov et al. [2012] list the following set of stakeholder requirements for NPPDS¹²:

- “1. Fully automated design in 2D, 3D paradigms;
2. Support for the “building information model” and similar notions;
3. Support for systems engineering and other modern engineering practices, such as parallel engineering and knowledge-based engineering;
4. Support for a data-centric idea and a life cycle management concept, which have become standards in current engineering practice;
5. The idea of ‘creating information once’;
6. The integration of various IT platforms. CAx and PDM systems from different vendors, the requirements management system, the project planning system and other IT platforms are used to design the plant and its subsystems. Widely used engineering approaches require a thorough integration of those IT platforms;

¹² For some reason, the list does not include the requirement for reuse, which is stated to be one of the main goals of NPPDS.

7. Collaboration of geographically scattered groups. Employees from several enterprises participate in the plant development, so the NPPDS should provide for collaboration, not only inside one group in one room, but also among geographically dispersed working groups;
8. Paperless information exchange. Effective work can not be carried out on the basis of paper exchanges; therefore, the NPPDS should support completely paperless technologies;
9. Support for standardized processes (requirements management, configuration management, change management, documents and data management);
10. Design data availability for decades;
11. Simplification of procedures for making changes and making them more cost effective;
12. Industry standards support.”

As Belov et al. [2012] point out, these stakeholder requirements are valid for other industrial fields like oil & gas or petrochemicals. We can well state here that these stakeholder requirements are also valid for NPP I&C system development projects.

The NPPDS architecture is created using the following systems engineering viewpoints:

1. Processes and Functions viewpoint
2. Data viewpoint
3. Organizational Structure viewpoint
4. Information Systems viewpoint

These viewpoints are exactly in-line with our requirements for systematic engineering in Section 2.3 such that our list item 1 relates to Belov et al. list item 1, item 2 to item 2, item 3 to item 3 and item 4 to item 4.

These four Belov et al. viewpoints are discussed briefly in the following:

Process and Functions viewpoint covers three models:

- Life Cycle Model (LCM);
- Life Cycle Function Model (LCFM);
- Process Model (PM).

LCM and PM are easy to understand (see Sections 2.4 and 2.5), but LCFM needs further explanation: LCFM is a coarse-grained process model only to identify (but not to define in detail) the processes or activities (which Belov et al. [2012] call functions) of the involved parties during the NPP development.

Data viewpoint contains the following models [Belov et al. 2012]:

- “Requirements Breakdown Structure Model, containing the hierarchy of the requirements for the NPP, from high level general requirements to very detailed ones, is represented in Rational DOORS format;
- Plant Breakdown Structure Model, containing the hierarchy of the NPP unit functional systems and subsystems, is represented in SmartPlant® Foundation format;
- Documents Breakdown Structure Model, containing the structure of the complete set of documentation created and transferred to the customer, is represented in SmartPlant® Foundation format;

- 3D Breakdown Structure Model, containing the hierarchy of the buildings and their elements, is represented in SmartPlant® 3D format;
- Work Breakdown Structure Model, containing the construction work structure to erect the NPP, is represented in PRIMAVERA format;
- Nuclear Steam Supply System Breakdown Structure Model, containing the hierarchy of the main equipment in subassemblies and details, is represented in TeamCenter format.”

Compared this to our data models (an example of which can be found in Figure 9), it seems that NPPDS data models are more coarse-grained than ours.

Organisational Structure viewpoint “...represents the administrative and role structure of NPP development team entities.” [Belov et al. 2012].

Information Systems viewpoint defines the information system platform used to implement NPPDS. It defines two models [Belov et al. 2012]:

- “Software Systems Model (SSM)
- Requirements for the software platforms implementation and requirements for the platforms integration model (RM).”

The following set of systems engineering tools are listed by Belov et al. [2012] to implement the Information Systems viewpoint:

- “Requirements Management System – Rational DOORS by IBM;
- Plant Data Management – SmartPlant® Foundation by Intergraph;
- Product Data Management – TeamCenter by Siemens PLM Software;
- Project Portfolio Management – Primavera by Oracle;
- Budgeting System – Atomsmeta, custom developed software;
- Procurement System, Work Planning System, ERP – different modules of SAP Business Suite by SAP AG.”

NPPDS is an interesting reference for the SAUNA project. It encourages us to think that there is a strong need in nuclear sector for well-managed systems engineering. In SAUNA project, we do not create a systems engineering system similar to NPPDS, not even a SEMP such that a systems engineering system could be created based on the SEMP, but we create a reference SEMP or a SEMP template to help nuclear organisations create their own SEMP, and then develop systems engineering systems or management systems according to them.

3.4 U.S. Department of Defense

U.S. Department of Defense (DoD) has an office called the Office of the Deputy Assistant Secretary of Defense for Systems Engineering (ODASD [SE]). DoD has published a Defense Acquisition Guidebook (DAG) [DOD 2013]; its Chapter 4 is dedicated to systems engineering guidelines. They have also created an outline or template for a Systems Engineering Plan (SEP), which is the government level document to be followed by the Systems Engineering Management Plans (SEMP) of the contractors. The SEP table of contents is provided in Appendix 3.

DoD’s SE process model is composed of 16 processes, as shown in Figure 16.

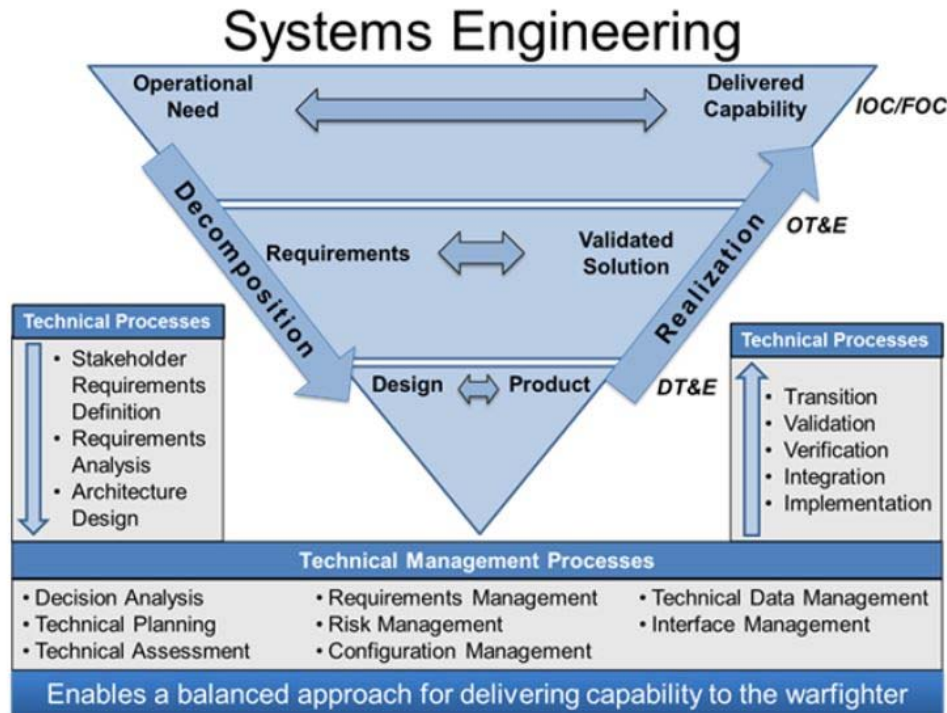


Figure 16. DoD systems engineering processes [DOD].

Defense Acquisition Guidebook [DOD 2013] is an interesting reference in this context providing, for example, a good description of the program manager and systems engineer roles.

3.5 U.S. Department of Transportation Systems Engineering Guidebook

U.S. Department of Transportation defines in its *Systems Engineering Guidebook for ITS* [DOT 2009] the process of Systems Engineering Management Planning. The outcome of the process is a Systems Engineering Management Plan, supporting technical plans (optional) and requests for proposals.

The Systems Engineering Guidebook for ITS is not elaborated here further, however, the Systems Engineering Management Planning process is depicted below in Figure 17 to provide an overview of the activities needed to create a SEMP. Also the whole ITS guidebook is a valuable reference in creating organisation specific SEMP for the nuclear domain.

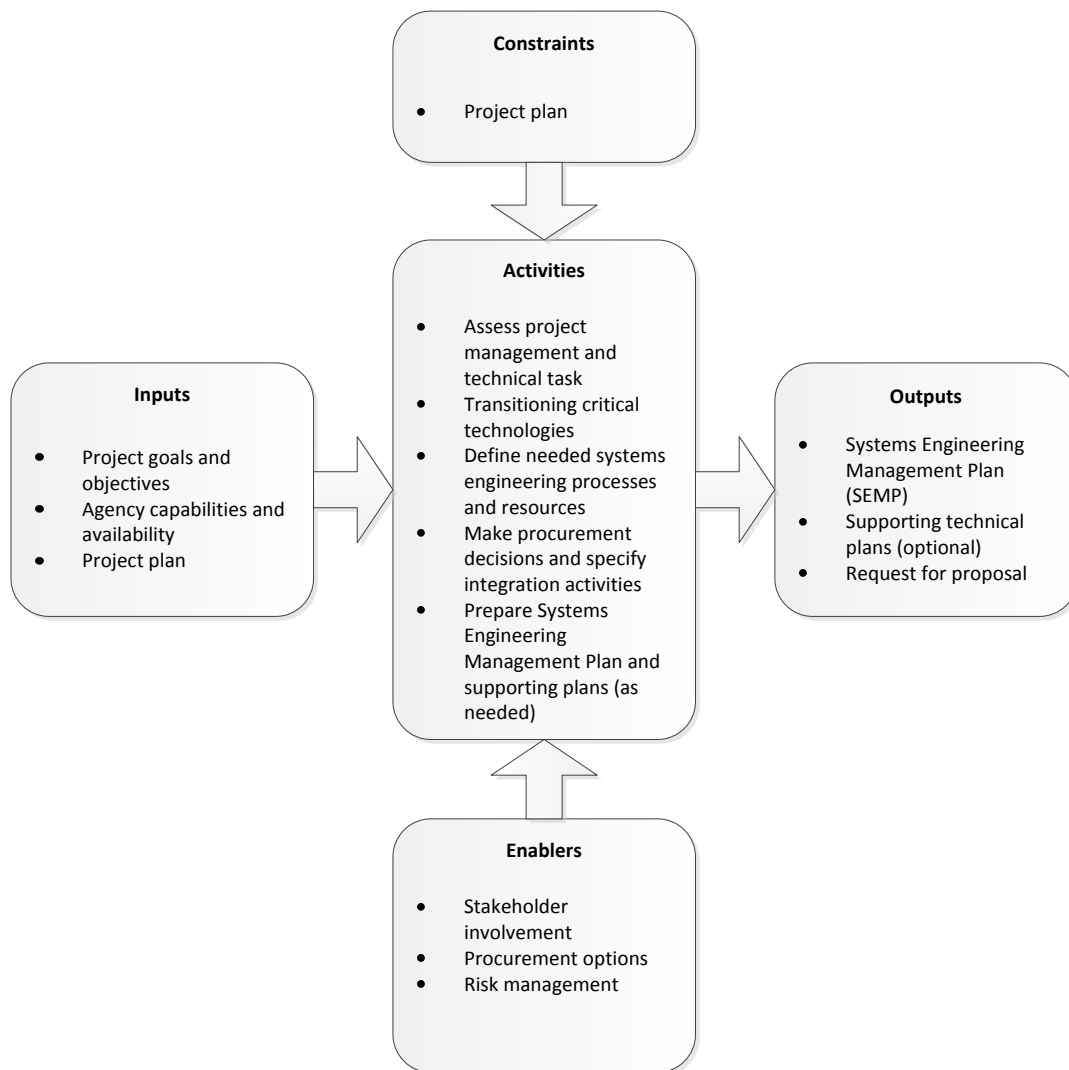


Figure 17. Systems Engineering Management Planning process diagram according to [DOT 2009].

4. SEMP in the context of STUK and IAEA regulations

The IAEA standards and STUK YVL guides do not recognise the Systems Engineering approach. But they recognise and require a **management system** to be used by the organisations “...*applying for a construction or operating licence for a nuclear facility or one constructing or operating a nuclear facility ... [and by]... the plant supplier, suppliers contributing to nuclear fuel fabrication, safety-significant design and expert organisations, testing and inspection organisations, component and material manufacturers, and other safety-significant suppliers.*” (Excerpts from the YVL Guide A.3 [STUK 2014] paragraphs 201 and 203.)

The main contents of a management system are the management system processes. IAEA [2006] and STUK [2014] require that the processes “...*shall be identified, and their development shall be planned, implemented, assessed and continually improved.*” (Citation from IAEA [2006].) Furthermore, IAEA [2006] sets requirements for the development of the processes as follows:

“The development of each process shall ensure that the following are achieved:

- Process requirements, such as applicable regulatory, statutory, legal, safety, health, environmental, security, quality and economic requirements, are specified and addressed.
- Hazards and risks are identified, together with any necessary mitigatory actions.
- Interactions with interfacing processes are identified.
- Process inputs are identified.
- The process flow is described.
- Process outputs (products) are identified.
- Process measurement criteria are established.”

Both IAEA [2006] and STUK [2014] define some obligatory, generic processes to start with; the YVL guide A.3 [STUK 2014] lists the following generic processes: document management, product control, control of records, purchasing, communication, managing organisational changes and project management. Furthermore, YVL B.1 [STUK 2013a] specifies some requirements engineering activities.

Processes are the main contents of a SEMP, too. Because the selected systems engineering standard is the IEC/IEC/IEEE 15288 standard, we compare, in Table 8, the processes identified by the YVL Guide A.3 to the IEC/IEC/IEEE 15288 [2015] processes.

Table 8. Mapping of STUK YVL Guide Y.3 processes to IEC/IEC/IEEE 15288 processes.

YVL Guide Y.3 generic processes	Corresponding IEC/IEC/IEEE 15288 processes
Document management process	Information Management process
Product control process	Several processes from the technical processes group (especially Stakeholder Needs & Requirements Definition process, System Requirements Definition process, Verification process and Validation process) and Configuration Management process
Control of records process	Information Management process and Configuration Management process
Purchasing process	Acquisition process
Communication process	Infrastructure Management process and Information Management process
Managing organisational changes process	<No corresponding process>
Project management process	Project Planning process and Project Assessment and Control process

Due to the fact that the set of IEC/IEC/IEEE 15288 processes is very comprehensive (covering quality planning and assurance, and the like; see Figure 5), nearly all the management system processes can be covered by the systems engineering processes. Hence we state that a management system plan works as a SEMP template for the projects of the organisation in question (i.e. the management system owner), provided that the management system plan defines the technical processes.

What is then the added value gained by introducing the SE approach in the NPP context? The set of ISO/IEC/IEEE 15288 processes provides a ready-made process model, especially to the Product control process required by YVL Guide Y.3. In practice, this involves the IEC/IEC/IEEE 15288 technical processes, but there are other processes in IEC/IEC/IEEE 15288 that can be adopted as hinted in Table 8.

Now that we have noticed the correspondence between a management system and systems engineering, we can capture the requirements for the systems engineering processes from the IAEA and STUK standards and guides by studying their requirements for the management system processes. The YVL A.3 requirements for the management system processes are listed in Appendix 5. Besides the process requirements, we use the management system documentation requirements to amplify the SEMP with the relevant information related to a management system. The YVL A.3 requirements for the management system documentation are as follows (underlining by the authors of this report to elicit the essence of the management system documentation contents):

“The management system shall be documented. The documentation shall include a description of the management system and the organisational structure. Furthermore, the documentation shall include the organisational policies, authorities, and responsibilities, the requirements for individual competences and qualifications, the management and decision-making procedures, the processes and the related guidelines, and communication with the interest groups. The structure of the management system’s documentation and the hierarchy of its parts shall be defined.

Procedures for quality and safety management shall be described and documented in the management system.

The language used in the management system shall be readable and readily understandable to the personnel.” [YVL A.3 2014]

The SEMP template created in this context is based on the above documentation requirements, the management system process requirements in Appendix 5 and Appendix 6, and on the ISO/IEC/IEEE 15288 standard.

To further elaborate the relationship between the concepts of the IAEA and STUK defined management system and the SEMP template, see Figure 18, Figure 19 and Figure 20. Note the following in the particular figures:

- The SEMP template, i.e. the management system plan, resides under the Management System branch whereas the actual SEMP_s reside under projects (see also Figure 1). The reason why the SEMP_s are not under the Systems Engineering program¹³ branch is that the SEMP_s are not system specific but project specific. For example, a single system can be engineered in several projects (parallel and consecutive); the projects (such as a requirements capture project or disposal project) may use only some of the processes defined in the SEMP template. Hence a project specific SEMP is created using an extract of the complete set of processes provided by the SEMP template.
- The SEMP template does not address the projects and systems(-of-interest), because both of them are case specific. But the SEMP template can be system type specific, e.g. for I&C systems only.
- The projects are separated from the systems(-of-interest) that are engineered in the projects. The rationale for this can be found in Footnote 3 in Section 2.4.

¹³ Systems Engineering program is the portfolio of SE management processes, technical processes and specialty engineering discipline processes and the relating information items and the models of the systems (under development or already developed); Project program is the portfolio of project management processes, the project documentation and other project artefacts.

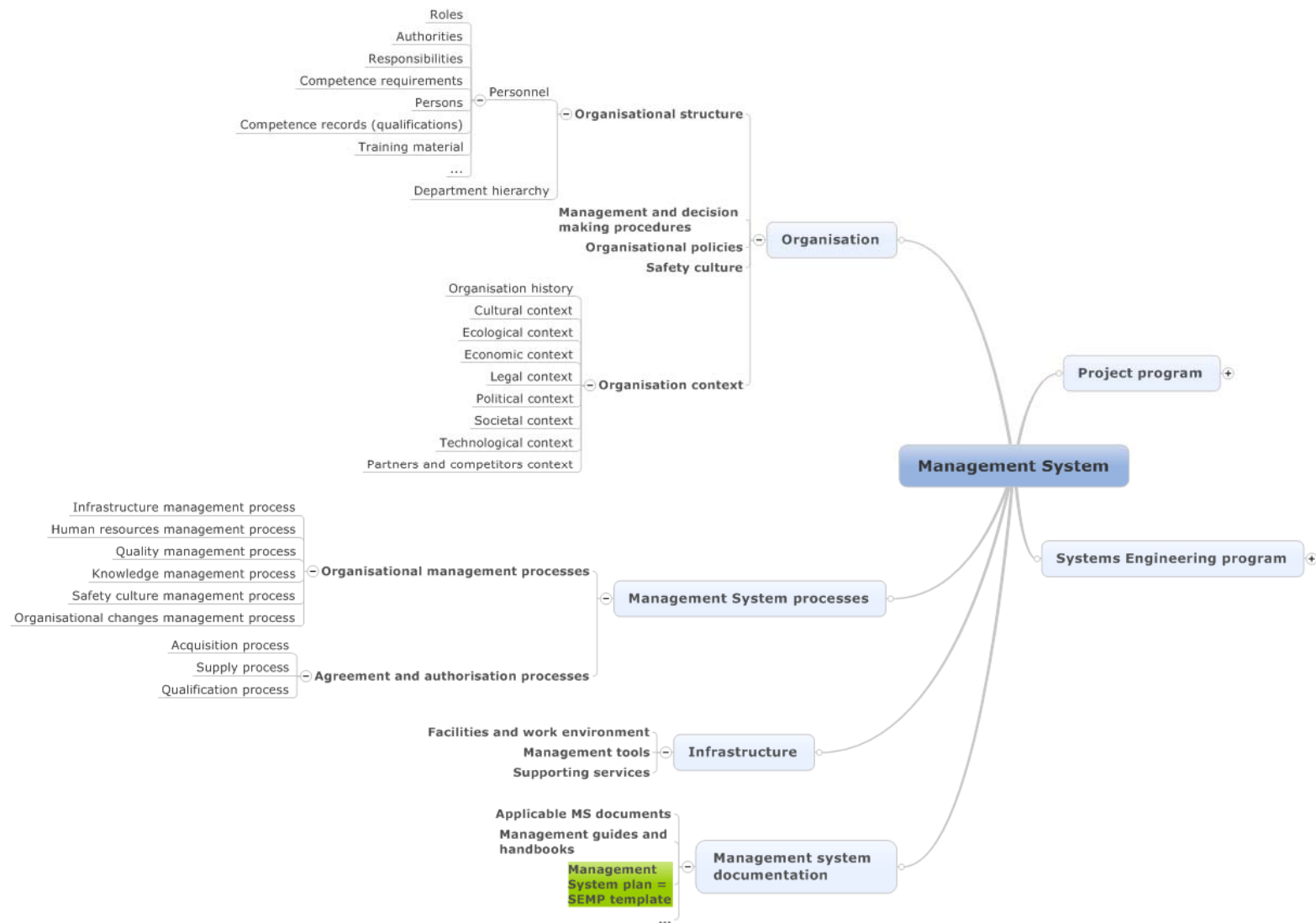


Figure 18. Management System structure, part 1.

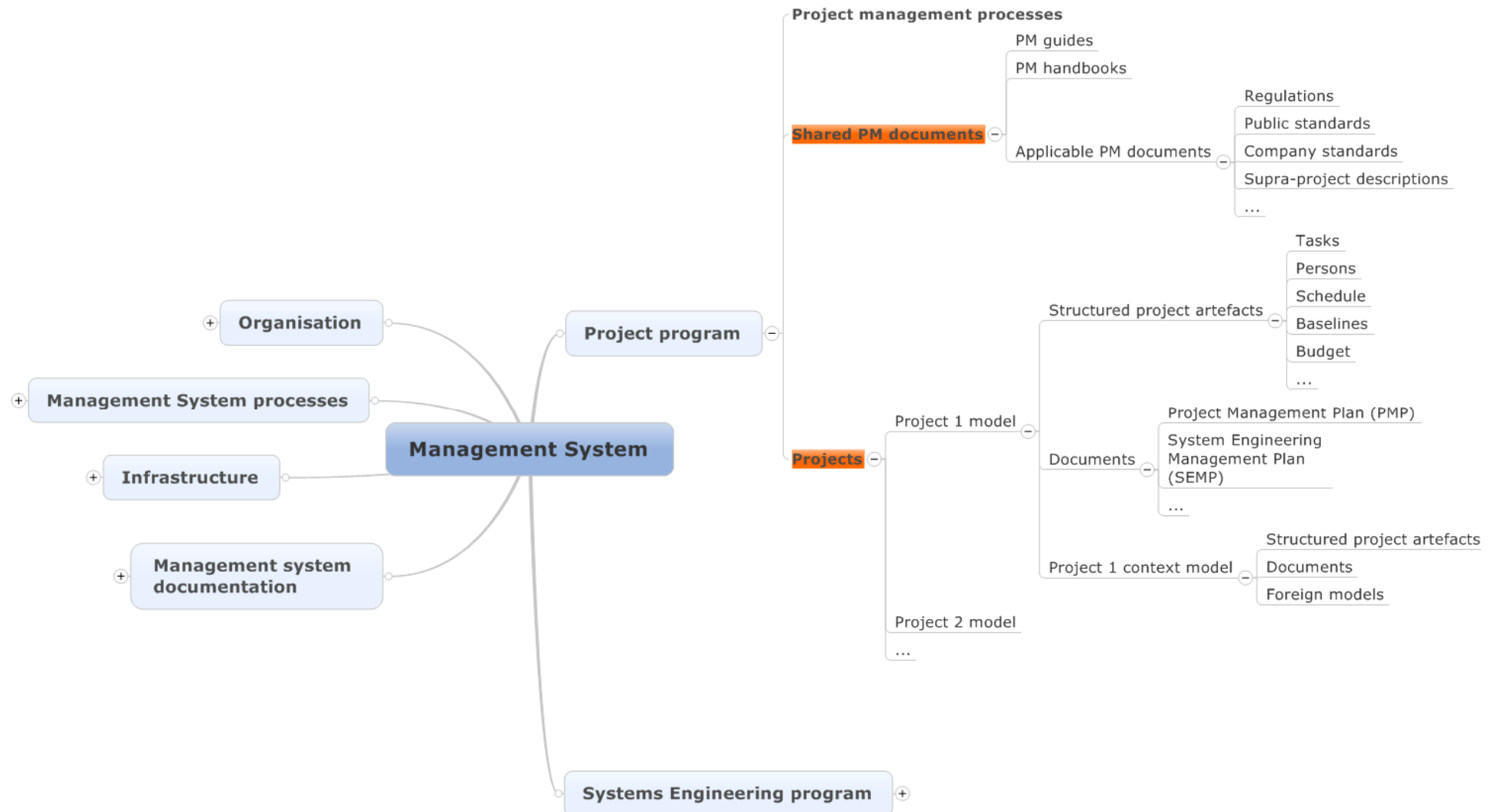


Figure 19. Management System structure, part 2; Project program expanded. The red objects are not addressed by the SEMP template created in this work.

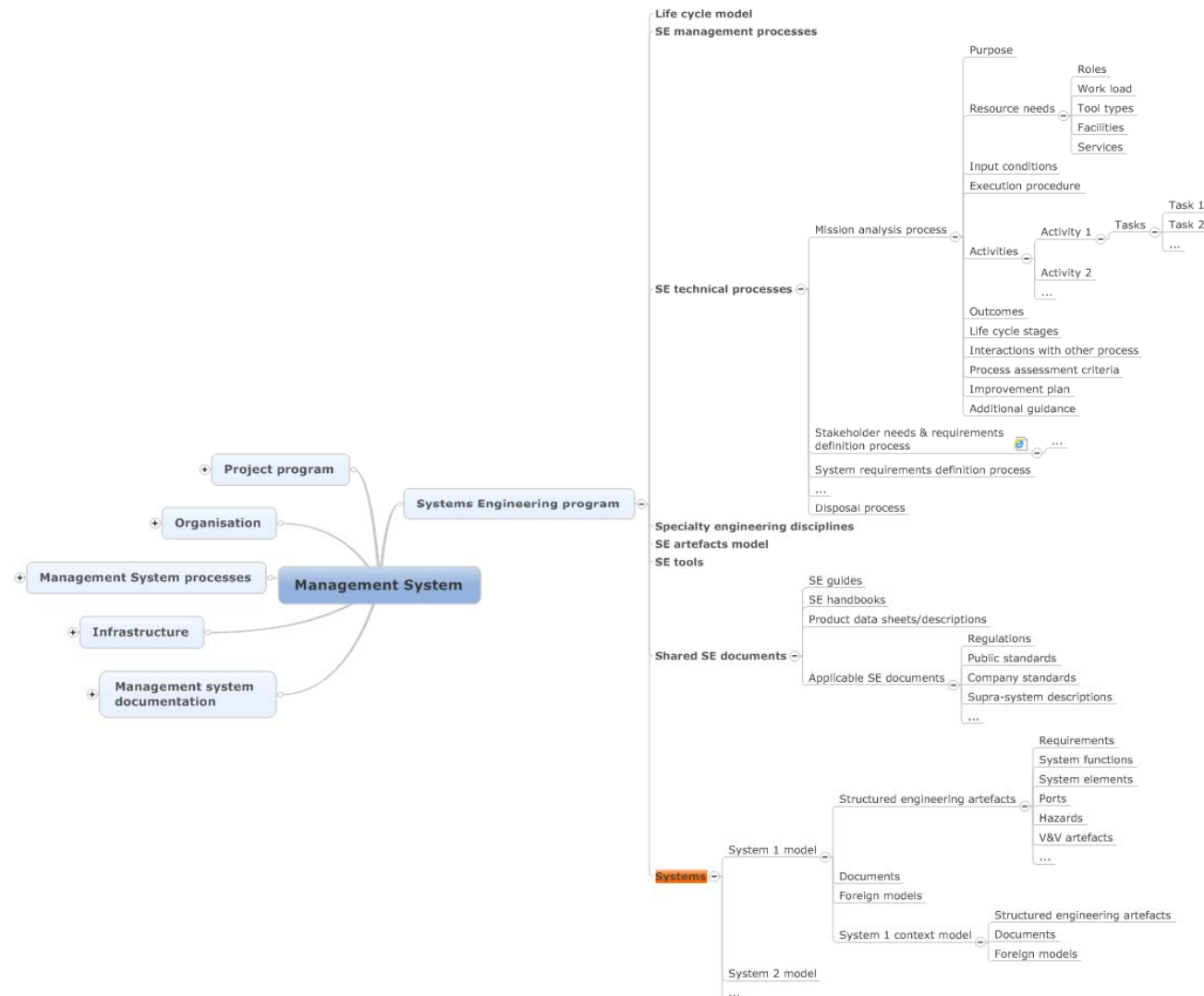


Figure 20. Management System structure, part 3; Systems Engineering program expanded. The red objects are not addressed by the SEMP template created in this work.

5. Foundations for the SEMP template implementation

The decision to use time window based life cycle model (see Section 2.4) and the management system structure depicted in Figure 18, Figure 19 and especially the branch of the Systems Engineering program in Figure 20 are important foundations for the SEMP template. In the following sections, some other important pieces of foundation are laid.

5.1 Document centric vs model-based

When starting creation of the SEMP template, the fundamental decision made was that a typical word processing document template will not be done. Instead, a structured data approach was decided to be used. This decision was made to promote moving from document centric systems engineering towards model-based systems engineering also on management level. **Hence the main added value of this work lies in the structured implementation of the SEMP.**

5.2 Specifications, descriptions, plans and reports

Another decision was to clarify the usage of information item types Specification, Description, Plan and Report. The reason is to make clear distinction between input documents and output documents and a clear distinction between product (system-of-interest) related documents and process related documents.

The rules are the following:

- Specification is an input document that sets requirements or models to be followed for the systems-of-interest.
- Specification specifies a product (system or system element); what the properties of the product shall be.
- Description is an output document that presents the designed solution.
- Description describes a product (system or system element); what the properties of the product are.
- Plan is an input.
- Plan plans (specifies) an activity (process, activity or task); who, what, where, when, why, and how the activity shall be performed.
- Report is an output.
- Report reports (describes) who, what, where, when, why, and how an activity was performed.

Figure 21 depicts these rules.

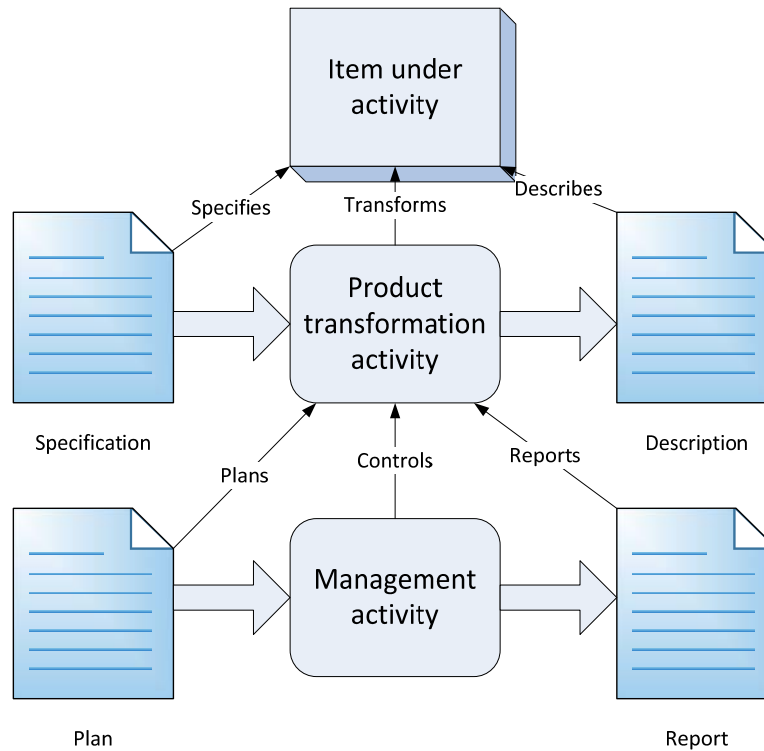


Figure 21. The Scheme for using Specification, Description, Plan and Report information item types.

Note also that Description documents from a product transformation activity are not used directly as inputs to the next product transformation activity, but an analysis phase transforms the Description document to a Specification document (see Figure 22). For example, a schematic diagram (a Description information item) of an electronic device from a schematics designer is not as such the specification for the printed circuit board designer, but other information and parameters, such as the number of board copper layers, are provided in the circuit board specification as the results of the analysis of the schematics diagram.

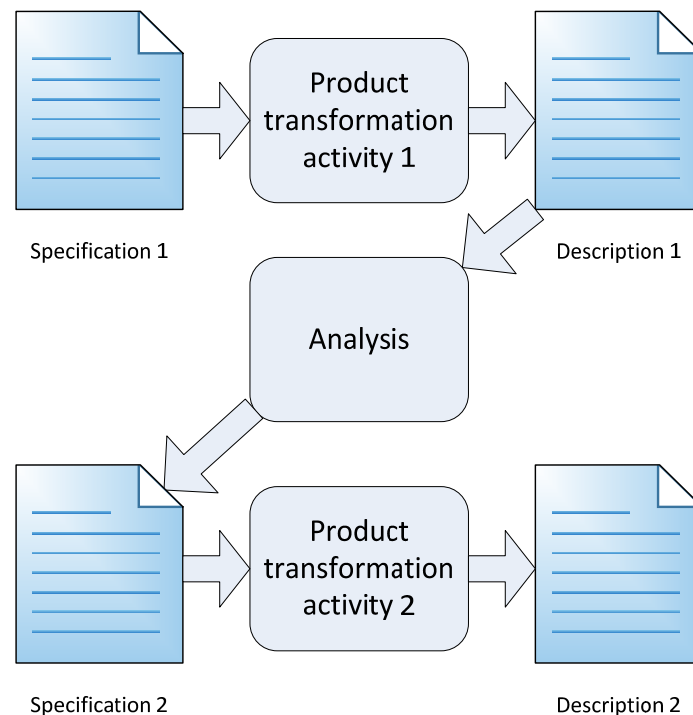


Figure 22. Specification – Description – Specification -chain.

Note also that there are other information types besides Specification, Description, Plan and Report; the information types are depicted in Figure 23.

5.3 Process vs. process views

The definition of process states that a process consists of a set of **interrelated or interacting** activities. In this regard, a set of activities is not considered a process if the activities do not interrelate. E.g. verification activities do not constitute a systems engineering process due to the fact that the verification activities are carried out in different phases of a project, and those activities normally do not interrelate with each other but with the particular design and implementation activities the outcomes of which are verified. For example, the stakeholder needs and requirements definition process shall include an activity that verifies the quality of the compiled set of stakeholder requirements; this activity is an intrinsic member¹⁴ of the stakeholder needs and requirements definition process activities. If the stakeholder needs and requirements definition process is deleted, the particular verification task is useless and shall be deleted as well, and is such proved not to be owned by the verification ‘process’ but by the stakeholder needs and requirements definition process.

The ISO/IEC/IEEE 15288 process construct model presented in Figure 7 does not allow an activity or task to be shared by several processes (due to the composite aggregations), but it allows a process view¹⁵ to refer (with the Concerns relation) to the processes, their activities and tasks.

The fact that the verification activities within the other processes constitute a process view instead of a process does not make it devalued. A process view can have an owner with similar responsibilities than in the case of an actual process.

¹⁴ Task 1) of Activity e) of the ISO/IEC/IEEE 15288 Stakeholder needs and requirements definition process.

¹⁵ See definition of process view in Section 1.2.

If we think about the above verification task which checks the quality of the requirements, the same task is represented in ISO/IEC/IEEE 15288 as task number 2 of activity b of the Verification process, but in a general sense¹⁶. Hence the particular ISO/IEC/IEEE 15288 task is unnecessary, if the verification activities of all the other processes are introduced within the processes (as of course is desirable). Nevertheless, the ISO/IEC/IEEE 15288 Verification process provides a meta model for the verification activities of the actual processes that transform the system-of-interest model. Such an overseer process is also needed to define the way as to how the verification results are stored and what the verification procedure specifications shall include. This moves the Verification process to the Management processes category¹⁷ and can be tagged as a process if it is defined so that its outcomes are guidelines and templates (i.e. the general verification framework) to carry out the actual verification activities, and if the Perform verification -activity would be omitted; the title would also be changed to Verification planning process (or Verification and Validation planning process, if the two processes are very similar in contents). Furthermore, a separate process view called Verification management that concerns the verification activities of the actual processes¹⁸ can be created if needed. The outcomes of the ISO/IEC/IEEE 15288 Verification process are thus separated such that its outcomes a) and b) are Verification planning process outcomes and outcomes c) to g) are Verification management process view outcomes, or all the outcomes of ISO/IEC/IEEE 15288 are allocated to a Verification management process view. Note that the main outcomes of the Verification planning process are the verification guidelines and templates.

The discussion above raises the question that who cares whether a set of activities is tagged a process or process view. The analysis above motivates us to make the careful distinction between these two concepts; it helped us identify the Verification planning process and Verification management process view, which better reflect the real world processes than the original ISO/IEC/IEEE 15288 Verification process. The distinction also helps define well confined processes when modelling the execution sequences of the processes, i.e. the owner or executor of a technical process, such as the Stakeholder needs and requirements definition process, does not have to consult the Verification process when executing the technical process.

The above solution to have two Verification related processes / process views (Verification planning process and Verification management process view) make, however, the outline of the processes complicated, because we need two processes / process views instead of the original one Verification process. Furthermore, we should do the same for example for the Configuration management process. There are two possible solutions to this complexity: 1) We allow hybrid process model such that a process can have its own activities and tasks, but it can also concern, such as a normal process view does, activities and tasks of other processes; 2) We allow all activities and tasks to be shared by all process descriptions, and do not distinguish between processes and process views (i.e. we only have processes or we only have process views). Our solution is the following:

We allow all activities and tasks to be shared, and we do not utilise the concept of process views.

This decision is reflected to the process construct model provided in Figure 7 by changing the composite aggregations (black diamonds) to shared aggregations (empty diamonds)

¹⁶ The task is titled 'Perform verification procedures', which proves our claim that Verification is not a process but a process view; there is no such real task that performs all the verification activities within the particular single task.

¹⁷ In ISO/IEC/IEEE 15288 the category is called Technical management processes; in this work it is called SE management processes.

¹⁸ See a similar ISO/IEC/IEEE 15288 example in its Annex E Section E.5 (Process view for interface management).

from process to process, from process to activity and from activity to task. The solution is presented in Section 5.4.

Nevertheless, both the Verification and Validation processes are moved from the Technical processes category to the SE management processes category due to the fact that the Verification and Validation processes are management oriented (providing the V&V framework and forming thus a set of interrelating activities as required by the process definition), while the actual V&V work is done inside the Technical processes. Both processes are renamed and are called Verification management process and Validation management process. Both management processes include both planning and management¹⁹.

5.4 Enhanced process constructs model

The process constructs diagram provided in Figure 7 is enhanced and presented in Figure 23 to better support a structured process description.

Note that the outcomes of a process (or activity or task) are not presented as an attribute of the SE process construct, but as a separate item type as illustrated in Figure 23. There are two reasons for this: 1) Separate outcome artefacts provide better traceability that is beneficial, for example, during process assessment; 2) relationships with the information items are accurate (otherwise linking would be between the whole process and information items). The input conditions and the outcomes (and the additional artefacts, except Life cycle stage) are linked to the abstract Process construct item type. This means that the input conditions and outcomes (and the additional artefacts, except Life cycle stage) can also be linked to the corresponding activities and tasks. This may be necessary for the process assessment.

Note also that in the process constructs model (Figure 23), there are item types that are not explicitly presented in the ISO/IEC/IEEE 15288 and ISO/IEC/IEEE TR 24774 models; these additional item types are presented in Table 9. The reason why these are not in the ISO/IEC/IEEE 15288 model is that a generic process model cannot define such because they are more or less application or organisation specific.

¹⁹ This is how e.g. the configuration management standard IEEE Std 828-2012 [2012] does, too.

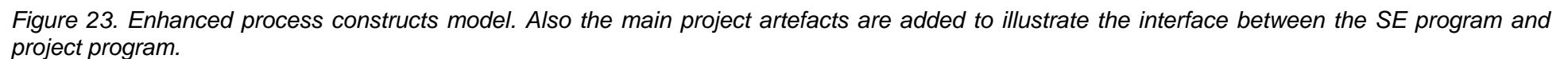


Table 9. Process constructs model additional item types.

Item type	Explanation
Additional guidance	General guidance (documents) for the process. (General in the sense that they are not specific to the particular organisation and application; however, they should relate to the specific process not to all processes. Example entry: 'INCOSE Systems Engineering Handbook, 2015, Section 4.2')
Applicable regulation	A law, directive, regulation, standard etc. that controls planning and execution of the particular process.
Control	Directives and constraints according to the IDEF0 model in Figure 8. In this case, the controls are implemented by the <i>Applicable regulation</i> and <i>Process requirement</i> item types.
Enabler	Resources (tools, technologies, infrastructure and workforce) and other enablers according to the IDEF0 model in Figure 8. In this case, the mechanisms are called enablers and are implemented by the <i>SE resource (need)</i> item types (<i>SE facility</i> , <i>SE role</i> , <i>SE service</i> , <i>SE tool type</i> , <i>SE workload</i>).
Hazard	Any error that may occur during execution of the process, activity or task and that may violate the safety integrity of the process, activity or task outcomes
Information item ref (and two specialisations, one for input and one for output)	A reference to an information item.
Input condition	A sentence with a verb that describes what needs to be ready when execution of the process, activity or task starts, such as 'Stakeholder needs are uttered.'
Life cycle stage	Life cycle stages during which the process is executed
Process requirement	Requirements for the particular process, activity or task (but not generic process requirements). The process requirements are controls of the process. If a whole regulation document is addressed as a control for the particular process, a process requirement can be created as: "Follow the requirements of <regulation reference>", or the document can be presented as an <i>Applicable regulation</i> . (However, it is preferred that process requirements are captured one by one from an applicable regulation instead of introducing the whole applicable regulation.)
SE resource (need)	The resources needed by the process, activity or task. The resource types are listed below. The resources needed are the enablers of the process, activity or task.
	SE facility Facilities and work environment needed to execute the process, activity or task.
	SE role Expected roles needed to execute the process, activity or task
	SE service Services needed to execute the process, activity or task.
	SE tool type Expected tool types needed to execute the process, activity or task.
	SE workload Expected workload needed by the process, activity or task

In this SEMP implementation, there is no special item type for information items, but there is the Information item ref -item type that refers to the actual information item, like a document or part of a document (see Figure 23). If a description document (an output information item) is used as such as an input information item to a process, it is advised here to create another information item reference with type Specification to follow the rule in Figure 22. In this way there can be two Information item ref objects for one document, e.g. Description item reference and Specification item reference for a single document, but not necessarily to the same version of the document. For example, updating of the Description document may start immediately after the document has been approved as a Specification document for the next activity; the Specification information item reference shall then refer to the approved version of the document, while the Description information item reference refers to the current version of the document.

The Information item ref list works as a master information item index for all the information items related to the particular systems engineering program. The information items of the project program, such as the project plan, meeting minutes etc., can be collected to the same index, or a separate index can be created. The idea is that references to information items, like documents, are always done through the Information item ref list. This prohibits usage of hidden and uncontrolled information items within the processes.

Figure 23 does not list the additional attributes of the SE process item type. The list of all the SE process attributes is provided below in Table 10.

Table 10. Attributes of the SE process item type (including the common, Process construct, attributes).

Attribute	Explanation
Code	Process identification code (= Prefix + ID)
Category	Process category: Organisational management, Project management, Systems Engineering management, Technical, Specialty engineering, Agreements and authorisation management
Title	Name of the project; a short description of the process, a noun
Purpose	Overall goal of the process in one sentence
Notes	Additional description about the intent; general overview of the execution; other considerations not covered by the Purpose, ExecutionProcedure and other attributes, and the artefacts depicted in Figure 23.
ExecutionProcedure	Execution procedure in more detail from the organisation point of view (not a general description)
InteractionWithOtherProcesses	Identification and description of the interactions with other processes
ProcessAssessmentCriteria	The criteria for assessment (evaluating and measurement) of the process performance
ImprovementPlan	The improvement plan of the process. Provides process specific improvement guidelines, not generic; the generic ones are described within the Life cycle model management process
PublishingDocument	Link to the wiki page (or other) that publishes the process
AdditionalGuidance	Additional process guidance that is helpful in understanding and executing the process (a link to the guidance)
Order	Process order number relevant only in process listings

The process data model in Figure 23 is implementable with the SharePoint content management software or any other database oriented artefacts management tool.

6. Description of the SEMP template implementation

6.1 Implementation platform

The Microsoft SharePoint content management tool was selected for the SEMP implementation platform due to the fact that SharePoint provides a structured project data repository (SharePoint lists) to implement the process constructs model presented in Section 5.4. Furthermore, SharePoint integrates collaboration features (calendars, issue management, discussions and the like), document libraries and wiki pages. SharePoint wiki pages can embed live data from the SharePoint lists; this enables semi-automatic document generation. Because documents and wiki pages also are list items in SharePoint, it is possible to create trace relations between various engineering artefacts such as process requirements and documents.

6.2 I&C systems life cycle model

The I&C systems life cycle model is depicted in Figure 24. The life cycle model is created based upon YVL B.1 [STUK 2013a], YVL E.7 [STUK 2013b] and YVL D.4 [STUK 2013c] and the life cycle concepts presented in Section 2.4.

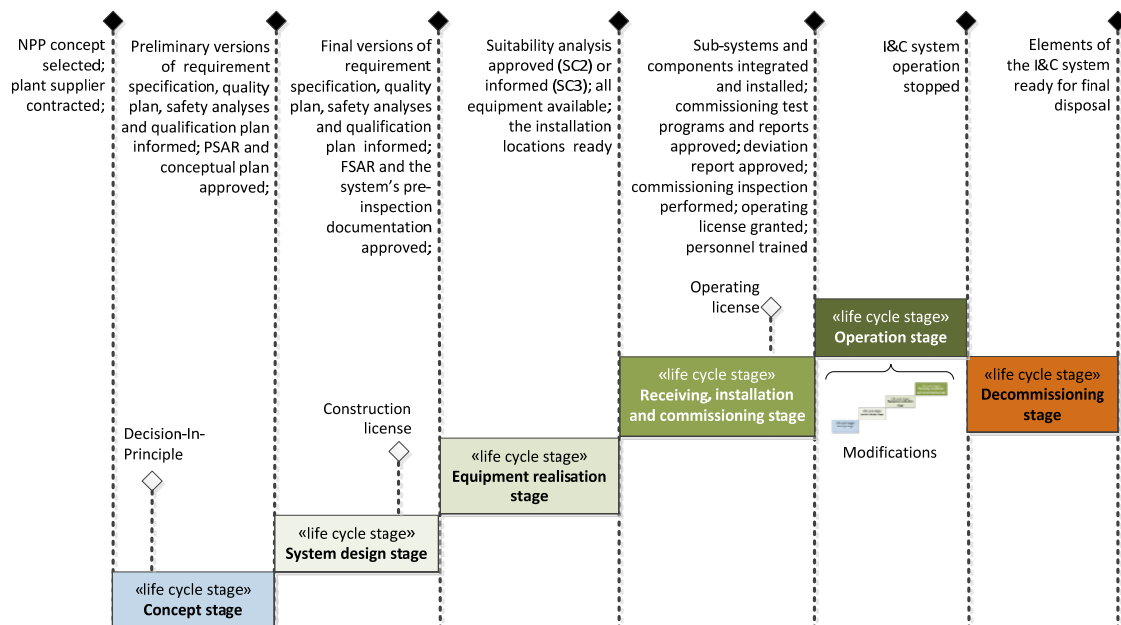


Figure 24. I&C system life cycle model. (The empty diamonds denote the licensing milestones of the whole NPP facility.)

The life cycle stages²⁰ are described in Table 11.

²⁰ See definition in Section 1.2.

Table 11. Life cycle stages of I&C systems.

Life cycle stage	Description	Core SE processes
Concept stage	Preliminary design of the I&C system	Mission analysis process; Stakeholder needs and requirements definition process; System requirements definition process; System analysis process; Architecture definition process; Design definition process; System safety engineering; System security engineering; Qualification process
System design stage	Final design of the I&C system	Stakeholder needs and requirements definition process; System requirements definition process; System analysis process; Architecture definition process; Design definition process; System safety engineering; System security engineering; Qualification process
Equipment realisation stage	Selection and procurement of equipment, and/or manufacturing of equipment	Implementation process; System analysis process; Qualification process
Receiving, installation and commissioning stage	Installation and integration of the received system elements to compose the I&C system; commissioning testing; commissioning inspection	Transition process; Integration process; Qualification process
Operation stage	Nuclear use; modifications of the I&C system; (planning of the I&C system renewal)	Operation process; Maintenance process; Qualification process
Decommissioning stage	Sorting, treatment and packing of waste; Transfer and storage of waste; (installation and commissioning of a new I&C system)	Disposal process; Materials engineering

6.3 Identified systems engineering processes

The systems engineering processes identified in the context of the SAUNA project are listed in Table 12.

Table 12. The systems engineering processes identified in the context of the SAUNA project.

Title	Purpose
Technical processes (Processes that directly manipulate the system-of-interest or its model)	
Mission analysis process	The purpose of the Mission analysis process is to define the mission problem or opportunity, characterise the solution space, and determine the potential solution class(es) that could address a problem or take advantage of an opportunity. (Modified from ISO/IEC/IEEE 15288 [2015])
Stakeholder needs and requirements definition process	The purpose of the Stakeholder needs and requirements definition process is to create the initial concept model of the system-of-interest such that it can provide - in the defined environment - the capabilities needed by the stakeholders. (Modified from ISO/IEC/IEEE 15288 [2015])
System requirements definition process	The purpose of the Systems requirements definition process is to transform the stakeholder (i.e. the problem domain) view of the desired capabilities into solution domain view.
Architecture definition process	The purpose of the Architecture definition process is to define system architecture alternatives, both functional and physical, to select one or more alternative(s) that frame the stakeholders concerns and meet the system requirements, and to express this in a set of consistent views. (Modified from ISO/IEC/IEEE 15288 [2015])
Design definition process	The purpose of the Design definition process is to specify the system elements and to provide sufficient information about the overall system to enable implementation of the system elements consistent with the architectural entities as defined in the models and views of the system architecture. (Modified from ISO/IEC/IEEE 15288 [2015])
System analysis process	"The purpose of the System analysis process is to provide a rigorous basis of data and information for technical understanding to aid decision-making across the life cycle." (ISO/IEC/IEEE 15288 [2015])
Implementation process	The purpose of the Implementation process is to make available the system elements that constitute the system.
Integration process	The purpose of the Integration process is to realise the system-of-interest composing of its system elements according to the system requirements and architecture description.
Transition process	The purpose of the Transition process is to make the system-of-interest and its context (including enabling systems and the personnel) to be ready for operation in its operational environment.
Operation process	The purpose of the Operation process is to use the system-of-interest to deliver its services. (Modified from ISO/IEC/IEEE 15288 [2015])
Maintenance process	"The purpose of the Maintenance process is to sustain the capability of the system to provide the a service." (ISO/IEC/IEEE 15288 [2015])
Disposal process	"The purpose of the Disposal process is to end the existence of a system element or system for a specified intended use, appropriately handle replaced or retired elements, and to properly attend to identified critical disposal needs (e.g. per an agreement, per organisational policy, or environmental, legal, safety, security aspects)." (ISO/IEC/IEEE 15288 [2015])
Systems Engineering management processes (Processes that support and manage the technical processes)	
Life cycle model management process²¹	The purpose of the Life Cycle Model Management process is to define, maintain, and assure availability of policies, life cycle processes, life cycle models, and procedures for use by the organisation with respect to the ISO/IEC/IEEE 15288 [2015] (Modified from ISO/IEC/IEEE 15288 [2015])

²¹ The work done in this report, and in SEMP creation in general, is one of the activities (Establish the processes) of the Life cycle model management process.

Title	Purpose
Systems Engineering artefacts model management process	The purpose of the Systems Engineering artefacts model management process is to provide a model of information items that supports structured storage and traceability of engineering artefacts.
Systems Engineering tools and tools integration management process	The purpose of the Systems Engineering tools and tools integration management process is to provide a list of planned SE tools to be used and an integration plan of the SE tools.
Configuration management process	The purpose of the Configuration management (CM) process is to manage and control model and system elements and configurations over the life cycle. CM also manages consistency between a product and its associated configuration definition. (Modified from ISO/IEC/IEEE 15288 [2015])
Verification management process	The purpose of the Verification management is to provide the framework for the verification activities.
Validation management process	The purpose of the Validation management is to provide the framework for the validation activities.
Virtual engineering management process	The purpose of the Virtual engineering management process is to provide the framework for the virtual engineering activities.
Electrical engineering management process	The purpose of the Electrical engineering management process is to provide the framework for the electrical engineering activities.
Electronics engineering management process	The purpose of the Electronic engineering management process is to provide the framework for the electronic engineering activities.
Software engineering management process	The purpose of the Software engineering management process is to provide the framework for the software engineering activities.
Specialty engineering disciplines (Vertical processes ('process views' as called by ISO/IEC/IEEE 15288) that focus on special concerns)	
System safety engineering discipline	The purpose of the System safety engineering discipline is to help ensure that the system achieves the required safety integrity level.
System security engineering discipline	The purpose of the System safety engineering discipline is to help ensure that the system achieves the required security characteristics.
Dependability and inspectability engineering discipline	The purpose of the Dependability and inspectability engineering discipline is to help ensure that the system achieves the required dependability (availability, reliability, maintainability and maintenance support performance) and inspectability characteristics.
Resilience engineering discipline	The purpose of the Resilience engineering discipline is to help ensure that the system achieves the required resilience characteristics.
Human factors engineering discipline	The purpose of the Human factors engineering discipline is to help ensure that the system achieves the required usability and other human factors characteristics.
EMC engineering discipline	The purpose of the EMC engineering discipline is to help ensure that the system achieves the required EMC characteristics.
Materials engineering discipline	The purpose of the Materials engineering discipline is to help ensure that the system achieves the required materials characteristics.
Project management processes (Processes that plan and manage the project model and the project work that engineer the system-of-interest)	
Project planning process	"The purpose of the Project planning process is to produce and coordinate effective and workable plans." (ISO/IEC/IEEE 15288 [2015])
Project assessment and control process	"The purpose of the Project assessment and control process is to assess if the plans are aligned and feasible, determine the status of the project, technical and process performance; and direct execution to help ensure that the performance is according to plans and schedules, within projected budgets, to satisfy technical objectives." (ISO/IEC/IEEE 15288 [2015])

Title	Purpose
Decision management process	“The purpose of Decision management process is to provide a structured, analytical framework for objectively identifying, characterising and evaluating a set of alternatives for a decision at any point in the life cycle and select the most beneficial course of action.” (ISO/IEC/IEEE 15288 [2015])
Risk management process	“The purpose of the Risk management process is to identify, analyse, treat and monitor the risks continuously.” (ISO/IEC/IEEE 15288 [2015])
Measurement process	“The purpose of the Measurement process is to collect, analyse, and report objective data and information to support effective management and demonstrate the quality of the product, services, and processes.” (ISO/IEC/IEEE 15288 [2015])
Collaboration management process	The purpose of the Collaboration management process is to provide the collaboration framework for the project(s) parties.
Quality assurance process	“The purpose of the Quality assurance process is to help ensure the effective application of the organisation’s Quality management process to the project.” See ISO/IEC/IEEE 15288 [2015]
Organisational management processes (Processes that manipulate the organisation that engineers the system-of-interest)	
Infrastructure management process	“The purpose of the Infrastructure management process is to provide the infrastructure and services to projects to support organisation and project objectives throughout the life cycle.” (ISO/IEC/IEEE 15288 [2015])
Human resources management process	“The purpose of the Human resources management process is to provide the organisation with necessary human resources and to maintain their competencies, consistent with the business needs.” (ISO/IEC/IEEE 15288 [2015])
Quality management process	The purpose of the Quality management process is to assure that products, services and implementations of the (other) processes meet organisational and project quality objectives and achieve customer satisfaction. (Modified from ISO/IEC/IEEE 15288 [2015])
Knowledge management process	See ISO/IEC/IEEE 15288 [2015]
Safety culture management process	The purpose of the Safety culture management process is to help ensure that the safety culture of the organisation achieves the acceptable level.
Organisational changes management process	The purpose of the Organisational changes management process is to ensure that the organisational changes implemented support the achievement of safety goals and that the implementation of the organisational changes is controlled. (Modified from YVL A.3, STUK [2014])
Agreements and authorisation management processes (Processes that deal with agreements and approvals between the organisation in question and external organisations)	
Acquisition process	“The purpose of the Acquisition process is to obtain a product or service in accordance with the acquirer’s requirements.” (ISO/IEC/IEEE 15288 [2015])
Supply process	“The purpose of the Supply Process is to provide an acquirer with a product or service that meets agreed requirements.” (ISO/IEC/IEEE 15288 [2015])
Qualification process	The purpose of the Qualification process is to demonstrate to the regulator that the I&C systems of a nuclear facility and their components and cables are suitable for the intended use and satisfy the relevant safety requirements.

6.4 SEMP table of contents

As stated in Section 5.1, our SEMP implementation is not a typical word processing document template, but a repository of structured data. Hence the entrance to the SEMP contents can be arranged with different ways using graphical and textual user interfaces. Nevertheless, we also provide the traditional table-of-contents entrance to the SEMP contents to make SEMP printouts possible. Such a SEMP table of contents is listed below in Table 13.

Each SEMP chapter or section is a self-contained wiki page, and is considered as a document fragment with an identification code and version control. The document fragments together make the whole document, i.e. the SEMP (template). Each document fragment embeds information items from the SharePoint list, i.e. the actual data is recorded into the SharePoint lists (not into the document fragments), and the document fragments aggregate the necessary information items from the SharePoint lists. The main information items are presented in Section 6.5.

Table 13. SEMP table of contents.

Chapter and section headings	Description of the contents
1. Introduction to the SEMP	Purpose, scope and structure of the SEMP
2. System and system context identification	Identification and overview of the system-of-interest; description of its objectives; initial system concept model (minimum: 'black box' with title and one functional requirement); system context identification and overview; initial system context model
3. Description of the Management system	Introduction to management system concept; definitions; relevant standards; requirements and recommendations for the management system; short identification and overview of the management system; the owner of the management system; management system architecture: the selected systems engineering approach
3.1. Policy statements	Purpose of the policy statements; list of policy statements
3.2. Organisations, roles, responsibilities and competences	List and descriptions (incl. diagrams) of organisations and roles involved in the management system, project and SE processes; responsibilities of the roles; competence requirements of the roles
3.3. Safety management and safety culture	Purpose of the safety management; description as to how the safety management is carried out; description of the safety culture (mind-set; knowledge and understanding; organisational systems and structures), safety culture training and how the safety culture is maintained
3.4. Quality management and culture of quality	Purpose of the quality management; description as to how the quality management is carried out (refer to Quality management and Quality assurance processes); description of the culture of quality, culture of quality training and how the culture of quality is maintained
3.5. Training	Description of the training policy and program
3.6. Infrastructure	Identification and overview of the infrastructure
3.6.1. Facilities, buildings, workspaces and associated utilities	List and descriptions of the facilities, buildings, workspaces and associated utilities
3.6.2. Process tools and equipment	List and descriptions of the expected or provided process tools and equipment
3.6.3. Supporting services	List and descriptions of the expected or provided supporting services

3.6.4. Work environment	Description of the work environment conditions (such as noise, temperature, humidity, lightning, etc.) needed to carry out the processes
4. Management system context	Short introduction the management system context; purpose of the chapter
4.1. Organisation's history context	Description of such history that may have effect on the safety and quality culture, especially incident history
4.2. Cultural context	Description of the cultural context of the organisation, i.e. the context in which the processes are carried out
4.3. Ecological context	Description of the ecological context of the organisation, i.e. the context in which the processes are carried out
4.4. Economic context	Description of the economic context of the organisation, i.e. the context in which the processes are carried out
4.5. Legal context	Description of the legal context of the organisation, i.e. the context in which the processes are carried out
4.6. Political context	Description of the political context of the organisation, i.e. the context in which the processes are carried out
4.7. Societal context	Description of the societal context of the organisation, i.e. the context in which the processes are carried out
4.8. Technological context	Description of the technological context of the organisation, i.e. the context in which the processes are carried out
4.9. Partner context	Description of the partners and their organisations that are involved in the processes; initial or overall collaboration model (refer to Collaboration management processes)
5. Project context	Description of the project the daughter document of which this SEMP is; short overview of schedule, budget, baselines, etc.
6. Stakeholders and their needs, applicable documents	Short introduction to the chapter; purpose of the chapter
6.1. Stakeholders	List of stakeholders with description and categorisation
6.2. Main stakeholder needs	Main characteristics, features and functions needed by the stakeholders
6.3. Applicable documents	List of applicable documents that control the processes and set requirements for the system-of-interest
7. Life cycle model	Description of the life cycle model; a reference and comparison to the parent system life cycle model
8. Systems Engineering processes	Introduction (definitions, overview, process constructs model); list of SE processes; relation with the project management; recording of the outcomes; assessment of the SE processes; improvement of the SE processes
8.1. Detailed descriptions of the Systems Engineering processes	void
8.1.1. Technical	void
8.1.1.1. Mission analysis process	Process identification; definitions; process requirements and recommendations; applicable regulations; purpose; notes; input conditions and corresponding information items; roles and responsibilities; estimated workloads; needed tool types; needed facilities; needed services; execution procedure; activities; tasks; outcomes and corresponding information items; interactions with other processes; identified process hazards; process assessment criteria; improvement plan; additional guidance

8.1.1.2. Stakeholder needs and requirements definition process	- “ -
8.1.1.3. System requirements definition process	- “ -
8.1.1.4. Architecture definition process	- “ -
8.1.1.5. Design definition process	- “ -
8.1.1.6. System analysis process	- “ -
8.1.1.7. Implementation process	- “ -
8.1.1.8. Integration process	- “ -
8.1.1.9. Transition process	- “ -
8.1.1.10. Operation process	- “ -
8.1.1.11. Maintenance process	- “ -
8.1.1.12. Disposal process	- “ -
8.1.2. Systems Engineering management	void
8.1.2.1. Life cycle model management process	Process identification; definitions; process requirements and recommendations; applicable regulations; purpose; notes; input conditions and corresponding information items; roles and responsibilities; estimated workloads; needed tool types; needed facilities; needed services; execution procedure; activities; tasks; outcomes and corresponding information items; interactions with other processes; identified process hazards; process assessment criteria; improvement plan; additional guidance
8.1.2.2. Systems Engineering artefacts model management process	- “ -
8.1.2.3. Systems Engineering tools and tools integration management process	- “ -
8.1.2.4. Configuration management process	- “ -
8.1.2.5. Verification management process	- “ -
8.1.2.6. Validation management process	- “ -
8.1.2.7. Virtual engineering management process	- “ -
8.1.2.8. Electrical engineering management process	- “ -
8.1.2.9. Electronics engineering management process	- “ -
8.1.2.10. Software engineering management process	- “ -
8.1.3. Specialty engineering	void

8.1.3.1. System safety engineering discipline	Process identification; definitions; process requirements and recommendations; applicable regulations; purpose; notes; input conditions and corresponding information items; roles and responsibilities; estimated workloads; needed tool types; needed facilities; needed services; execution procedure; activities; tasks; outcomes and corresponding information items; interactions with other processes; identified process hazards; process assessment criteria; improvement plan; additional guidance
8.1.3.2. System security engineering discipline	- “ -
8.1.3.3. Dependability and inspectability engineering discipline	- “ -
8.1.3.4. Resilience engineering discipline	- “ -
8.1.3.5. Human factors engineering discipline	- “ -
8.1.3.6. EMC engineering discipline	- “ -
8.1.3.7. Materials engineering discipline	- “ -
8.1.4. Project management	void
8.1.4.1. Project planning process	Process identification; definitions; process requirements and recommendations; applicable regulations; purpose; notes; input conditions and corresponding information items; roles and responsibilities; estimated workloads; needed tool types; needed facilities; needed services; execution procedure; activities; tasks; outcomes and corresponding information items; interactions with other processes; identified process hazards; process assessment criteria; improvement plan; additional guidance
8.1.4.2. Project assessment and control process	- “ -
8.1.4.3. Decision management process	- “ -
8.1.4.4. Risk management process	- “ -
8.1.4.5. Measurement process	- “ -
8.1.4.6. Collaboration management process	- “ -
8.1.4.7. Quality assurance process	- “ -
8.1.5. Organisational management	void
8.1.5.1. Infrastructure management process	Process identification; definitions; process requirements and recommendations; applicable regulations; purpose; notes; input conditions and corresponding information items; roles and responsibilities; estimated workloads; needed tool types; needed facilities; needed services; execution procedure; activities; tasks; outcomes and corresponding information items; interactions with other processes; identified process hazards; process assessment criteria; improvement plan; additional guidance
8.1.5.2. Human resources management process	- “ -
8.1.5.3. Quality management	- “ -

process	
8.1.5.4. Knowledge management process	- “ -
8.1.5.5. Safety culture management process	- “ -
8.1.5.6. Organisational changes management process	- “ -
8.1.6. Agreements and authorisation management	void
8.1.6.1. Acquisition process	Process identification; definitions; process requirements and recommendations; applicable regulations; purpose; notes; input conditions and corresponding information items; roles and responsibilities; estimated workloads; needed tool types; needed facilities; needed services; execution procedure; activities; tasks; outcomes and corresponding information items; interactions with other processes; identified process hazards; process assessment criteria; improvement plan; additional guidance
8.1.6.2. Supply process	- “ -
8.1.6.3. Qualification process	- “ -
9. References	A list of such references referred to by the process descriptions that are not applicable regulations or additional guidance (i.e. that are not information items)
Appendix A: Glossary	List of definitions and abbreviations
Appendix B: Master document index of the SE program	List of all information items presented by the processes structured by the information type

6.5 Main information items

The information items according to the process construct model (presented in Section 5.4) are stored in the SharePoint lists. The main information items are listed in Table 14.

Table 14. Main information items of the SharePoint implementation of the SEMP.

Content	Description	Implemented as
Systems	List of the systems under the SE program	SharePoint list
Life cycle stages	List of the life cycle stages	SharePoint list
Process requirements	List of the process requirements	SharePoint list
Input conditions	List of the input conditions that need to be met to execute the processes	SharePoint list
SE processes	List of the processes	SharePoint list
SE activities	List of the activities of the processes	SharePoint list
SE tasks	List of the tasks of the activities	SharePoint list
SE roles	List of the human roles that are involved in the processes	SharePoint list
SE workloads	List of the estimated workloads needed to execute the processes	SharePoint list
SE tool types	List of the tool types (software and hardware tools) needed to execute the processes	SharePoint list
SE facilities	List of the buildings, rooms, and other workspaces and associated utilities needed to execute the processes	SharePoint list
SE services	List of the services (such as transport, communication or information systems and services) needed to execute the processes	SharePoint list
Outcomes	List of the outcomes of all processes	SharePoint list
Process hazards	List of the hazards (typically human errors) that are identified from the processes	SharePoint list
Corrective actions	Suggestions of the corrective actions for the process hazards	SharePoint list
Risk evaluations	Evaluations of the risks of the identified hazards (includes the actual corrective actions and assessment of the remaining risk)	SharePoint list
Wiki documents and document fragments	Library of all the SE program wiki pages; some of them are independent documents; some are document fragments.	SP wiki library
Process models	Library of process model files such as UML and SysML activity models (with diagrams)	SP document library
Images and diagrams	Library of any image or diagram that is not a process model	SP document library
SE program guides	Library of wiki pages that provide additional guidance for the SE processes (Note: additional guidance document can be external documents; not all guidance documents are stored in this library)	SP wiki library
Information items references	List of references to any kind of information items. This list also works as a documents master index. There can be several references to the same information item (possibly to different versions though) with different type attributes, e.g. <i>Specification</i> and <i>Description</i>	SharePoint list
Reference to reference trace list	This list can be used to create reference trees in case where an information item, such as a standard, references to another information item, such as another standard.	SharePoint list
Shared SE documents	Library for documents that are shared by all the systems-of-interest, such as standards, datasheets and templates	SP document library

6.6 IEC 61513 requirements for activities

As discussed in Section 2.4, we do not actually consider presentations such as the V-model or any other similar model (including the IEC 61513 ‘life cycle model’) as a life cycle model, but we call them processes execution models. IEC 61513 defines such models on two levels, the overall I&C safety life cycle and system safety life cycle. Compared to the three different interpretations for the concept of a life cycle presented in Section 2.4, progression from the overall I&C level to the system level corresponds to the Case 3, whereas the phases and their execution order within the two levels correspond to the Case 2, but not in the form of a V-model, but in the form of a straight waterfall model²² (recognising, however, that the activities “*may be in reality partially executed in parallel, or include iterations*”. [IEC 61513 2011]). Nevertheless, IEC 61513 is not a process standard, but a safety requirements standard; it specifies the general requirements for the safety engineering activities of the I&C systems of nuclear power plants. Hence the trinity of IEC 61513, ISO/IEC/IEEE 15288 and YVL A.3 (or the corresponding IAEA management systems standards such as IAEA GS-R-3 and IAEA GS-G-3.1) can be presented as illustrated in Figure 25.

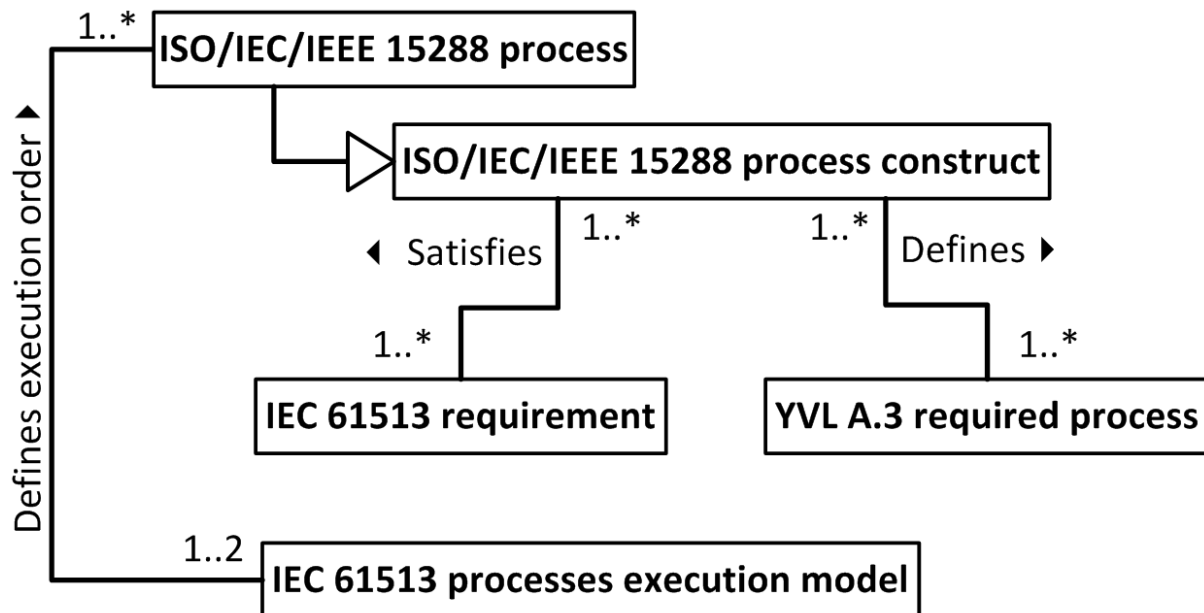


Figure 25. IEC 61513 – ISO/IEC/IEEE 15288 – YVL A.3 trinity.

(Note that IEC 61513 is not the only source of process requirements, not even the safety engineering process requirements.)

As concluded in Section 2.4, our challenge is to map the IEC 61513 ‘life cycle phases’²³ to the systems engineering processes in order to implement the Satisfies relations of Figure 25. We do that in Table 15 and Table 16.

²² V-model is in principle also a waterfall model, but illustrated in the shape of the letter V.

²³ Note that IEC 61513 uses the term ‘life cycle phase’, but also calls them ‘activities’. This validates our claim that the IEC 61513 life cycle phases are actually not life cycle stages but systems engineering processes (or their activities or tasks).

Table 15. Overall I&C life cycle phases and their mappings to the systems engineering processes defined in this report (in Section 6.2).

IEC 61513 phase	Corresponding systems engineering processes and activities
Deriving the I&C requirements from the plant safety design base <ul style="list-style-type: none"> Review of the functional, performance and independence requirements Review of the categorisation requirements Review of plant constraints Output documentation [creation of the Overall I&C requirements specification] 	System requirements definition process
Design of the overall I&C architecture and assignment of the I&C functions <ul style="list-style-type: none"> Design of the I&C architecture Functional assignment Required analysis 	Activities included in these processes: <ul style="list-style-type: none"> Architecture definition process; Design definition process Architecture definition process; Design definition process Architecture definition process; Design definition process; Verification management process; System analysis process; System safety engineering; Human factors engineering
Overall planning <ul style="list-style-type: none"> [Planning of the] overall quality assurance programs Overall security plan Overall I&C integration plan Overall commissioning plan Overall operation plan Overall maintenance plan Planning of training 	Activities included in these processes: <ul style="list-style-type: none"> Quality management process; Quality assurance process System security engineering Integration process; Validation management process Transition process; Validation management process Operation process Maintenance process A task within the Prepare for operation –activity within the Operation process
System safety life cycle	Implementation process; and see Table 16
Overall integration and commissioning	Integration process; Transition process; Qualification process
Overall operation and maintenance	Operation process; Maintenance process; Qualification process

Table 16. System life cycle phases and their mappings to the systems engineering processes defined in this report (in Section 6.2).

IEC 61513 phase	Corresponding systems engineering processes and activities
System requirements specification	System requirements definition process
System specification	Architecture definition process; Design definition process
System detailed design and implementation	Design definition process; Implementation
System integration	Integration process
System validation	Validation management process; Qualification process
System installation	Transition process; Validation management process; Qualification process
System design modifications	Configuration management process
System planning <ul style="list-style-type: none"> System verification plan System configuration management plan Fault resolution procedures [plan] System security plan System integration plan System validation plan System installation plan System operation plan System maintenance plan 	Activities included in these processes: <ul style="list-style-type: none"> Verification management process Configuration management process Verification management process; Validation management process; Configuration management process; Dependability and Inspectability engineering System security engineering Integration process; Validation management process Transition process; Validation management process Transition process; Validation management process Operation process Maintenance process
System qualification	Qualification process

The clauses of IEC 61513 corresponding paragraphs (in Chapters 5, 7 and 8 in case of Table 15, and Chapter 6 in case of Table 16) are copied to the Requirements list, and are then traced with the Is satisfied –link (see Figure 23) to the corresponding process constructs (processes, activities or tasks) according to Table 15 and Table 16.

The mappings in Table 15 and Table 16 may not be accurate due to the fact that the systems engineering process activities and tasks are not defined in detail in this context; the final definition of activities and tasks may cause changes to the mappings.

As hinted above in the first paragraph and in Figure 25, IEC 61513 defines the execution order of the processes (although not detailing the iteration of the activities), but it is assumed here that the internal execution order of activities and tasks are defined inside the systems engineering process descriptions. An example execution procedure can be found in Section 6.7.

6.7 Example process

In the following, an example process description (Stakeholder needs and requirements definition process) is presented. The sections of the process description follow the process constructs model presented in in Section 5.4 (see Figure 23 and Table 10).

Note that the substance of the process description is aggregated from the relevant SharePoint lists as presented in Section 6.5. Note also that the process description is not complete; it is provided only as an example to help creating organisation specific process descriptions.


Stakeholder needs and requirements definition process

Document fragment info

Document fragment identification

☐ Title

Stakeholder needs and requirements definition process

DocumentID	<input type="checkbox"/> Modified By	Modified	Version	Issuing organisation
DOCW-00059	Alanen Jarmo 	29/01/2016 14:13	0.114	VTT

Change log


Version	Date	Status (draft /proposal /approved)	Author(s) / Reviewer(s) / Approver, Organisation	Remarks of changes
0.114	29.01.2016	Draft	Jarmo Alanen, VTT	Created

Introduction

Process identification

The process is identified as follows:

▼ □

Code	Title	Category	Modified	<input type="checkbox"/> Modified By
Code	PRCSS-1			
Title	Stakeholder needs and requirements definition process			
Category	Technical			
Modified	11/01/2016 15:56			
Modified By	Alanen Jarmo 			

Definitions

Stakeholder is defined here as follows:

[system] individual, team, organization, or classes thereof, having an interest in a system
ISO/IEC/IEEE 42010:2011

Requirement is defined here as follows:

A condition or capability that must be met or possessed by a system, system component, product, or service to satisfy an agreement, standard, specification, or other formally imposed documents.

[ISO/IEC/IEEE 24765:2010](#) (definition 2)

Requirement shall refer to a need or expectation of which a special mention is made, or one which is generally implied or obligatory. (ISO 9000)


STUK YVL glossary

Controls

Process requirements and recommendations

The following table (Table DOCW-00059-1) lists the requirements and recommendations for this particular process.

Table DOCW-00059-1. Requirements and recommendations for this process.

<input type="checkbox"/>		Code	Title	Requirement	Source	SourceDetails
		REQ-1	Requirements in the level of detail understandable throughout the whole life cycle	The requirements concerning systems important to safety of the nuclear facility shall be defined to such a level of detail that a designer independent of the requirement specification process is able to carry out the re-design required for the in-service maintenance of the system its components as well as their modifications throughout the life cycle of the facility	Guide YVL B.1 2013	336
		REQ-2	Specify also non-functional requirements	Requirements that are not considered functional requirements, such as the applicable quality requirements and standards, shall also be specified.	Guide YVL B.1 2013	337
		REQ-3	Applicability of referenced standards	The applicability of the referenced standards and guidelines shall be justified. If an exception is made to a specified standard or guideline, such a departure shall be justified and its effect assessed.	Guide YVL B.1 2013	338
		REQ-4	Unambiguous, consistent, traceable and verifiable requirements	The requirement specifications shall be unambiguous, consistent and traceable. It shall be possible to verify the fulfilment of the requirements.	Guide YVL B.1 2013	339
		REQ-5	Requirements specification assessed by independent experts	The accuracy, completeness and consistency of the requirement specification of systems important to safety shall be assessed by experts who are independent of the design and implementation process. The assessment report shall present the observations made as well as a justified conclusion.	Guide YVL B.1 2013	340
		REQ-6	Traceability	The traceability of the requirements in the various design stages shall be demonstrable. The traceability of the requirements in the various design stages shall be demonstrated as part of the qualification	Guide YVL B.1 2013	341
		REQ-7	...			

Applicable regulations

The following laws, regulations, standards and agreements control this particular process.

ApplicableRegulations

REF-81: Requirements Writing Guidelines; REF-83: ...

Purpose

The purpose of the Stakeholder needs and requirements definition process is to create the initial concept model of the system-of-interest such that it can provide - in the defined environment - the capabilities needed by the stakeholders.

Notes

NOTE 1: The main contents of initial concept model of the system-of-interest is the list of the stakeholder requirements (with possible requirements modelling diagrams), but also a system model, no matter how coarse the model becomes, is created. Also the (initial) system context model is established.


NOTE 2: The Stakeholder needs and requirements definition process listens to the stakeholder requirements, analyse them and record the needs as well-defined stakeholder requirements. Furthermore, stakeholder requirements are captured from directives, standards, and other legally or otherwise binding documents.

NOTE 3: In general, the outcome of this process can be attached to a project agreement.

Input conditions and corresponding information items

The input conditions that need to be ready for this process to be started are listed in Table DOCW-00059-2.

Table DOCW-00059-2. Input conditions of this process.

<input type="checkbox"/>		Code	Title	Description	Related information
		INCND-1	Stakeholder needs are available	E.g. customers can be interviewed, or stakeholder documents, such as binding safety standards are available.	
		INCND-2	System is identified and described	The system-of-interest is identified (at least a descriptive name is provided) and a short description of its intended use is available. E.g. Reactor control system for the XXX nuclear power plant that ...	
		INCND-3	Descriptions of previous generations of the system or similar systems is available	System descriptions of the previous generations or similar systems. The source of history information shall be pointed out (it is not necessary to compile the information, because that will be the outcome of this process).	
		INCND-4	Experience of use (of previous models or similar system) has been captured	Experience of use shall especially include damage to health (long term effects, such as noise), accident, incident or malfunction history of the actual or similar system.	
		INCND-5	Domain knowledge is available	Domain knowledge can in minimum be tacit information and as best a structured domain knowledge model	
		INCND-6	Project constraints are known	The project plan may state constraint on execution of this process. Such constraints include work time and other resource constraints.	REF-79: Plan - Project plan

Enablers

The enablers that make this process possible to execute are listed below.

Roles and responsibilities

The roles that are needed to execute this process are listed in Table DOCW-00059-3.

Table DOCW-00059-3. Roles and responsibilities for this process.

<input type="checkbox"/>	Code	Title	Description	DescriptionOfResponsibility
	SEROLE-1	Project Manager		
	SEROLE-2	Stakeholder		
	SEROLE-3	Systems Engineer		
	SEROLE-4	Requirements Engineer		
	SEROLE-5	Safety engineer		
	SEROLE-6	Dependability Engineer		

Estimated workloads

The workload estimates are listed in Table DOCW-00059-4.

Table DOCW-00059-4. Estimated workloads for this process.

<input type="checkbox"/>	Code	Title	Description
	SEWORK-1	Stakeholder requirements definition process work load estimation - whole process	<p>To execute the Stakeholder requirements definition process requires approximately the following amount of man months:</p> <ul style="list-style-type: none"> • M1 man months if the number of requirements is expected to be less than N1. • M2 man months if the number of requirements is expected to be less than N2. • M3 man months if the number of requirements is expected to be less than N3. • M4 man months if the number of requirements is expected to be less than N4.

Needed tool types

The tool types that are needed to facilitate the execution of this process possible are listed in Table DOCW-00059-5.

Table DOCW-00059-5. Tool types needed by this process.

<input type="checkbox"/>	Code	Title	Description
	SETOOL-1	Requirements management tool	The tool has to support traceability and impact analysis.

Needed facilities

The facilities that are needed to execute this process are listed in Table DOCW-00059-6.

Table DOCW-00059-6. Facilities needed for this process.

<input type="checkbox"/>	Code	Title	Description
	SEFCLTY-1	Typical office premises	Typical indoor comfortable office premises with chair, desk and electricity and lightning.

Needed services

The services that are needed to execute this process are listed in Table DOCW-00059-7.

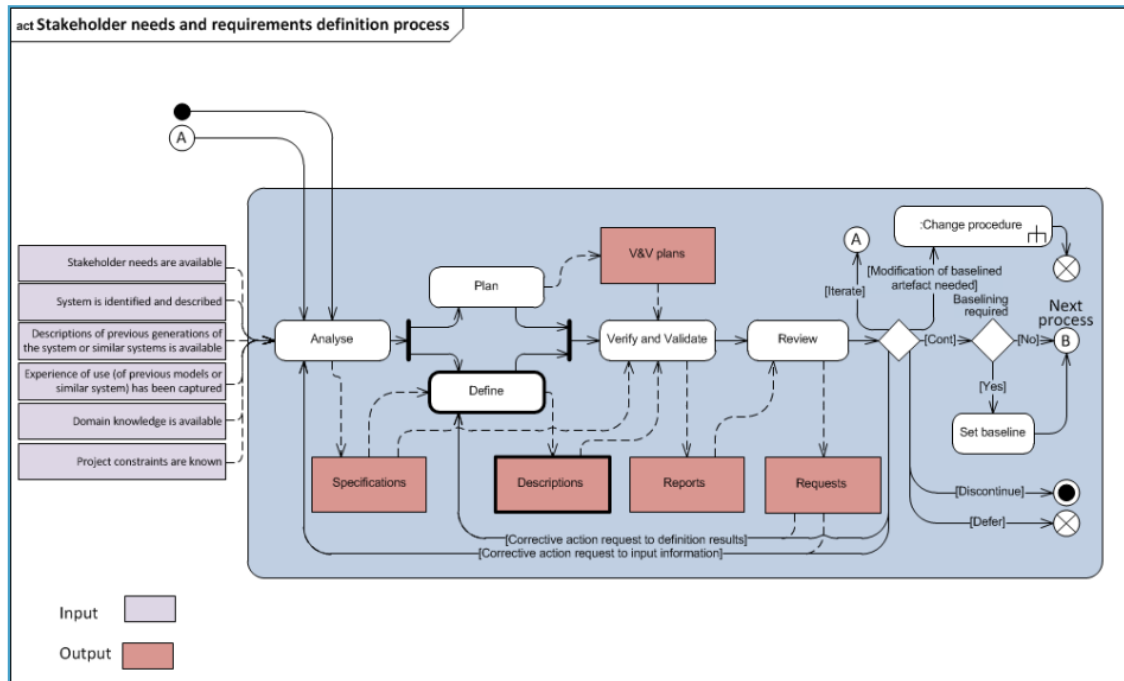
Table DOCW-00059-7. Services needed by this process.

<input type="checkbox"/>	Code	Title	Description
	SESERV-1	Internet connection	A fast internet connection that ...

Execution procedure

The activity diagram of the Stakeholder needs and requirements definition process is depicted below.

The core activity is the Define activity. Other activities relate to analysis, planning, V&V, review and configuration management. The activities are described in detail in the task descriptions.



Activities

The activities of this process are listed below in Table DOCW-00059-8.

Table DOCW-00059-8. Activities of this process.

<input type="checkbox"/> Title	ExecutionProcedure	Notes
Analyse stakeholder needs	The stakeholder needs and expectations are analysed to create a structured set of input artefacts to the stakeholder requirements definition activity. This activity involves identifying the stakeholders, interviews of stakeholders and capture of regulations, standards, guidelines and other applicable documents as well as the concepts and terminology of the system and its context.	NOTE 1: This activity can be executed either during the Systems Engineering Management process or Stakeholder Requirements Definition process.
Define stakeholder requirements and initial concepts	The purpose of this activity is to define an approved set of stakeholder requirements. Compared to the initial freely-formed stakeholder needs, the stakeholder requirements are well-formed. To determine the scope of the requirements, the system-of-interest is identified by providing a concept model of the system and its context. Finally, the platform independent behaviour is modelled (i.e. the behaviour from the problem domain point of view).	
Plan V&V of the output artefacts of this process	The purpose of this activity is to plan the verification and validation tasks executed during the stakeholder requirements definition process. Planning involves specification of the V&V cases to verify the stakeholder requirements (i.e. to check the quality of the requirements), to validate the stakeholder requirements (i.e. to check that defined set of stakeholder requirements is complete and completely covers the stakeholder needs) and to carry out the preliminary safety analysis of the system concept. It also involves initial planning of the system validation plan. Besides specifying the V&V cases, the V&V case specification are scheduled and assigned to persons (or roles). (V&V case specification specifies a test, analysis, inspection, calculation, design document review, demonstration, calculation, simulation, comparison, sampling, measurement etc. to verify or validate that the artefacts under V&V complies with the expectations. A V&V case specification includes, among others, description of the V&V case and its detailed steps, a list of proposed or obliged tools, a description of the expected environment and infrastructure for the V&V case, e.g. required space and temperature, vibration etc. parameters. It also includes a description of the expected results. Issues such as the schedule and persons or roles whom this V&V case is assigned to are not included; this is because the V&V case may be re-used in different phases of the project. Such issues are defined in the V&V plans.)	
Verify and validate the output artefacts of this process	The purpose of this task is to carry out the verification and validation tasks of the stakeholder requirements definition process to assess compliance to the expectations. Execution of the V&V cases is done according to the defined V&V plans. Such tasks include verification of the stakeholder requirements (i.e. to check the quality of the requirements), validation of the stakeholder requirements (i.e. to check that the defined set of stakeholder requirements is complete and completely cover the stakeholder needs), and carrying out the preliminary safety analysis of the system concept. These tasks also cover reporting of the execution of the V&V cases.	
Review stakeholder requirements definition process V&V results	The purpose of this activity is to draw the conclusions from the reports from the <i>Verify and validate the output artefacts of this process</i> -activity. The basic decision is to decide whether to continue to the next process or to iterate back to the beginning of this process (or even to earlier processes or only to the main activity of this process). Iteration back may be planned, or iteration may be commanded due to discrepancies between the expected and actual V&V results. It is also possible that the review results lead to suggestion to hold or discontinue the project. Note that the <i>Verify and validate the output artefacts of this process</i> -activity may also include reviews, i.e. to review is one of the many V&V work types, others being such as testing, analysis, demonstration etc. A typical such V&V case is 'Design document review'. The activity described here defines the reviewing of the results of the tests, analyses, demonstrations, reviews etc. This activity also defines the decision procedure. During the <i>Verify and validate the output artefacts of this process</i> -activity, decisions are not done, but the V&V results are reported; Compare to a case of a doctor and the laboratory personnel; the doctor makes the decisions while the laboratory personnel provide the test results.	
Set stakeholder requirements baseline	Baseline is set if commanded by the project manager (in the project plan). ...	

Tasks

The tasks of the activities of this process are listed below in Table DOCW-00059-8.

Table DOCW-00059-8. The tasks of this process grouped by Activity.

Task title	ExecutionProcedure
Activity : a) Analyse stakeholder needs (5)	
Task title	Create glossary
ExecutionProcedure	Collect and record the terms and abbreviations relating to the system and its context. Define the terms and abbreviations that are not defined or are poorly defined. Record also the relevant general terms and abbreviations. Record the terms and abbreviations to the system specific Glossary list [the link directs to the Management System glossary; you shall update the link after creating the system specific list; you might start by copying the Management System glossary].
Task title	Identify stakeholders
ExecutionProcedure	Identify organisations and persons (or roles) that have an interest in the system under development. Potential stakeholders include but are not limited to: authorities; customers; operators; developer engineers; policy-makers; producers; maintainers; implementing agencies; scientific experts; consultants; potential host communities. Record the list of stakeholder into Stakeholders list [the link directs to the Management System stakeholder list; you shall update the link after creating the system specific list; you might start by copying the Management System stakeholder list].
Task title	Record initial system concept and system context descriptions
ExecutionProcedure	Identify and record the system concept and its context from the description as uttered or published by the stakeholders. Simple text and illustration can be used here.
Task title	Capture stakeholder needs
ExecutionProcedure	Interview the stakeholders and/or read the documents (like regulations and standards) issued by the stakeholders. Record the stakeholder needs systematically into the requirement management tool by tagging them 'Stakeholder need' (not 'Stakeholder requirement'). In case of regulations and standards, the relevant (either mandatory or supporting) documents shall be introduced in the Information items reference list and linked to the outcome: Stakeholder needs are defined .
Task title	Prepare the requirements management tool <small>NEW</small>
ExecutionProcedure	Prepare the requirements management tool and other enabling systems for the requirements capture and recording. This involves setting the priority levels and requirement categories to be used.

Activity : b) Define stakeholder requirements and initial concepts (4)

Task title	Define system concept model
ExecutionProcedure	Define the initial concept model of the system according to the available documentation or oral descriptions by the stakeholders. The initial concept model is documented into the Initial system concept model document.
Task title	Define system context model
ExecutionProcedure	Describe the context (text, diagrams etc.); Define the life cycle model of the system; Capture past incidents; Define the constraints by the system context and to the system context; List external system elements; List the human actors that will interact with the machine (including bystanders); Define the flows between the system and system context objects; Define the system ports (i.e the interaction points to system context objects, like external system elements and human actors) that provide or exploit the flow; Define the operational environment including spatial environment, seismological environment, climatic environment, magnetic environment, electromagnetic environment, mechanical environment, hydraulic environment, pneumatic environment, chemical environment, optical environment, particle environment, terrain, flora and fauna; Define which of the terms in the glossary are domain terms (and optionally create a domain model, e.g. a SysML block definition diagrams, to model the relationships between the objects defined as domain terms in the glossary); Include the list of stakeholders in the system context model.
Task title	Formulate and record stakeholder requirements
ExecutionProcedure	Formulate the stakeholder requirements such that they match the stakeholder needs; and trace the stakeholder requirements to stakeholder needs and stakeholders using the Requirements management tool . Analyse the related regulations and standards and capture the relevant requirements from them (copy as it is or create a surrogate object of the original requirement to the requirement database; or restructure and reformulate the original requirements and create traces to the original requirements). The requirements shall be of good quality (see Requirements writing guidelines). Define constraints on the system and by the system. The constraints can be introduced as requirements with a flag 'constraint'.
Task title	Define physical architecture independent behaviour
ExecutionProcedure	Define the behaviour, i.e. the functionality of the system dependless of the anticipated physical architecture of the system. Methods such as Use Case Description or ConOps (Concept of Operations) can be used. SysML diagrams like Activity Diagram, Sequence Diagram, State Machine Diagram, Use Case Diagram and Block Definition Diagram can be used to illustrate the functionality.

Activity : c) Plan V&V of the output artefacts of this process (3)

Task title	Plan V&V of the stakeholder requirements
ExecutionProcedure	Plan verification, i.e. quality checking of the stakeholder requirements in accordance with the Requirements writing guidelines . Plan validation of the stakeholder requirements to ensure that the captured set of stakeholder requirements reflects exactly the stakeholder needs.
Task title	Create initial system validation plan
ExecutionProcedure	Create initial system validation plan, i.e. the plan by which it is assessed whether the developed system fulfils the stakeholder requirements.
Task title	Plan preliminary safety analysis for the system concept
ExecutionProcedure	Plan the preliminary safety analysis. The analysis can be made e.g. by using the Preliminary Hazard Analysis method. Provide the template for the safety analysis.

Activity : d) Verify and validate the output artefacts of this process (3)

Task title	Check quality of requirements
ExecutionProcedure	Check that the requirements fulfil the selected quality criteria according the the stakeholder requirements V&V plan. Report the results with the corrective actions recommendations according to the framework provided by the <i>Verification management process</i> .
Task title	Check that the stakeholder requirements are what the stakeholders expect
ExecutionProcedure	The stakeholder requirements are assessed together with the stakeholders or their representatives according the stakeholder requirements V&V plan. Report the results with the corrective actions recommendations according to the framework provided by the <i>management processmanagement process</i> .
Task title	Do preliminary safety analysis for the system concept
ExecutionProcedure	The system concept is analysed according to the preliminary safety analysis plan. Report the safety analysis with the corrective actions recommendations according to the instructions and/or templates provided by the according to the framework provided by the <i>Verification management process</i> .

Activity : e) Review stakeholder requirements definition process V&V results (4)

Task title	Review the stakeholder requirements verification results
ExecutionProcedure	Review the stakeholder requirement verification results to decide whether to continue the process with this set of stakeholder requirements or to resolve requirements problems. ...
Task title	Review the stakeholder requirements validation results
ExecutionProcedure	Review the stakeholder requirement validation results together with the stakeholders or their representatives to decide whether to continue the process with this set of stakeholder requirements or to resolve requirements problems. ...
Task title	Evaluate the preliminary safety analysis results
ExecutionProcedure	The risk assessment continues by risk evaluation to decide upon new or updated risk reduction methods based upon the corrective actions recommendations from the preliminary safety analysis. The results of this task are issued as corrective actions requests.
Task title	Decide about the continuation
ExecutionProcedure	If corrective action requests from the review tasks involve updating of the baselined artefacts, the modification procedure according to the <i>Configuration management process</i> is executed. Otherwise, corrective actions can be incorporated immediately. Corrective actions include e.g. updating or creating a new safety requirement, re-analysis of the stakeholder needs, re-definition of the stakeholder requirements. If there are no corrective actions requests, continuation to the next process is enabled or planned iteration can be carried out. If there are severe corrective actions (or project management reasons), discontinuation or deferring of the development work is possible.


Activity : f) Set stakeholder requirements baseline (4)

Task title	Check if requirements baseline is needed
ExecutionProcedure	Check the project plan to see if a requirements baseline is needed.
Task title	Identify the requirements baseline set
ExecutionProcedure	Identify the requirements to be baselined. ... Several baseline sets can be selected at a time.
Task title	Get approval for the stakeholder requirements set <small>new</small>
ExecutionProcedure	Obtain approval for the stakeholder requirements set according to the <i>Configuration management process</i> .
Task title	Create the requirements baseline
ExecutionProcedure	Create the requirements baseline with the baselining facility of the <i>requirement management tool</i> . Provide a comment to memorise the reason and to summarise the main updates.

Outcomes and corresponding information items

The outcomes from this process are listed below in Table DOCW-00059-9.

Table DOCW-00059-9. Outcomes from this process.

<input type="checkbox"/>		Code	Title	Description	RelatedInfoItem	RelatedActivity	RelatedTask
		OTCM-1	Stakeholders of the system are identified		REF-77: List of stakeholders	SEACT-1: Analyse stakeholder needs	SETASK-1: Identify stakeholders
		OTCM-2	Required characteristics and context of use of capabilities and concept in the life cycle stages, including operational concepts, are defined			SEACT-2: Define stakeholder requirements and initial concepts	SETASK-5: Define physical architecture independent behaviour
		OTCM-3	Constraints on a system are defined			SEACT-2: Define stakeholder requirements and initial concepts	SETASK-8: Formulate and record stakeholder requirements
		OTCM-4	Stakeholder needs are defined			SEACT-1: Analyse stakeholder needs	SETASK-2: Capture stakeholder needs
		OTCM-5	Stakeholder needs are prioritised and transformed into clearly defined stakeholder requirements			SEACT-2: Define stakeholder requirements and initial concepts	SETASK-8: Formulate and record stakeholder requirements
		OTCM-6	Critical performance measures are defined				
		OTCM-7	Stakeholder agreement that their needs and expectations are reflected adequately in the requirements is achieved			SEACT-4: Verify and validate the output artefacts of this process	SETASK-16: Check that the stakeholder requirements are what the stakeholders expect
		OTCM-8	Any enabling systems or services needed for stakeholder needs and requirements are available			SEACT-1: Analyse stakeholder needs	SETASK-66: Prepare the requirements management tool
		OTCM-9	Traceability of stakeholder requirements to stakeholders and their needs is established			SEACT-2: Define stakeholder requirements and initial concepts	SETASK-8: Formulate and record stakeholder requirements

The Stakeholder needs and requirements definition process possibly interacts with the System analysis process (and consequently Decision Management process) ...

Table DOCW-00059-10. Identified process hazards.

Stakeholder requirements definition guide

6.8 SEMP implementation in the context of a Management system implementation

To put the SEMP template into the management system context according to Chapter 4 (especially, Figure 18, Figure 19 and Figure 20), we decided to create a prototype management system SharePoint site for a fictitious NPP I&C organisation. In the prototype, however, we concentrate on the Systems Engineering management and Technical processes (i.e., the processes under Systems Engineering program in Figure 20). The user interface of the SharePoint management system prototype implementation is depicted in Figure 26.

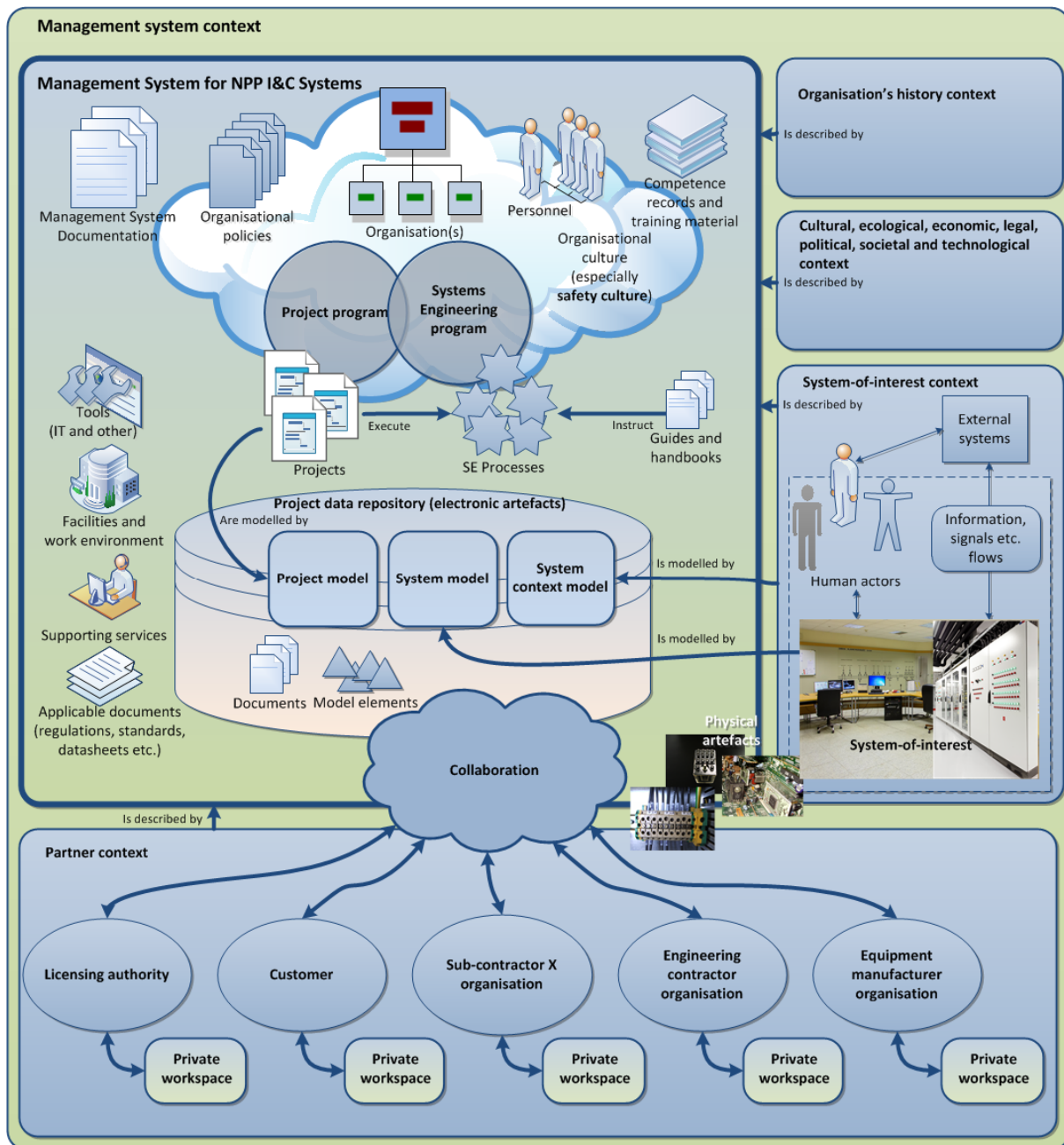


Figure 26. The management system prototype user interface.

The idea is that the objects in the figure are links to the corresponding information, in most cases to wiki pages that aggregate data from the structured data repository of SharePoint (i.e. from the SharePoint lists). The SEMP (template) is accessed by clicking the 'Management System Documentation' object.

7. Summary and conclusions

Systems engineering is not mentioned as a term in the IAEA standards or in the YVL guides. Instead, STUK and IAEA have issued 'Management systems' guides and standards that are relevant to systems engineering planning. The road from the particular guides and standards, however, does not explicitly lead to the systems engineering standards and methodologies, but to the ISO 9000 –series of standards. This means that SE is not the de facto methodology dictated by STUK and IAEA for NPP developments. Despite of this, it is clear for all the stakeholders that the nuclear power plants are complex systems, the developments of which call for systematic and comprehensive life cycle management starting from the very early concept stages to the decommissioning, closure and disposal stages of the NPP systems, even to the post-closure time in case of nuclear waste management systems. Hence the need for SE with advanced requirements engineering is nowadays well recognised among the Finnish nuclear power.

To make SE attractive, its power in managing development of complex systems, such as NPPs, the Systems Engineering approach needs to be highlighted and demonstrated. Requirements engineering is a good starting point to enter the SE world. This is particularly true in the cases, such as in Finland, where the authorities require traceability of requirements; traceability is impossible to implement without also considering the engineering artefacts of all the processes.

This work has shown that the management system process requirements can be well satisfied with the Systems Engineering approach, and that the systems engineering processes, and hence the Systems Engineering Management Plan (SEMP), can be implemented in a structured, model-based, way. The report provides an enhanced set of life cycle processes, an enhanced process construct model and an example SharePoint implementation of the process construct model. The report also describes the relation between a management system and the systems engineering processes such that the SE program can be implemented within the management system of an organisation; in this case a SharePoint implementation of a management system is presented. Furthermore, it is shown that the IEC 61513 I&C systems requirements can be satisfied with the SE processes.

Very important success factors in advocating SE are a well planned information model for information items (and other engineering artefacts) and provision of sophisticated tools to carry out the engineering processes and to manage, according to the defined information model, the artefacts consumed and produced within the processes. Without good tools, SE becomes a bureaucratic burden to engineers, not a framework to do elegant engineering.

References

- Belov, M., Kroshilin, A. & Repin, V. 2012. ROSATOM™s NPP Development System Architecting: Systems Engineering to Improve Plant Development. In: O. HAMMAMI, D. KROB and J. VOIRIN, eds, Springer Berlin Heidelberg, pp. 255–268.
- DOD (U.S. Department of Defense). 2013. Defense Acquisition Guidebook, Production Date: 16 September 2013. 1248 p.
- DOT (U.S. Department of Transportation). 2009. Systems Engineering Guidebook for Intelligent Transportation System. Version 3.0. U.S. Department of Transportation, Federal Highway Administration, California Division. November 2009. 313 p.
- Friedental, S., Griego, R. & Simpson, M. 2007. INCOSE Model Based Systems Engineering (MBSE) Initiative. INCOSE2007, San Diego, June 24-29 2007. A presentation. 29 p.
- Granholm, G. (Editor). 2013. Katsaus kompleksisten järjestelmien elinkaaren suunnitteluun. Espoo: VTT. VTT Technology: 121. 220 p + app. 9 p.
- IAEA. 2006. The Management System for Facilities and Activities. GS-R-3. Vienna: International Atomic Energy Agency (IAEA). 27 p.
- IEEE Std 828-2012. 2012. IEEE Standard for Configuration Management of Systems and Software Engineering. New York: Institute of Electrical and Electronics Engineers (IEEE). 58 p.
- IEC 61513. 2011. Nuclear power plants - Instrumentation and control important to safety - General requirements for systems. Geneva: International Electrotechnical Commission (IEC). 205 p.
- INCOSE. 2015. Systems Engineering Handbook – A guide for system life cycle processes and activities. Fourth edition. San Diego: International Council on Systems Engineering (INCOSE). 290 p.
- ISO 10303-233. 2012. Industrial automation systems and integration – Product data representation and exchange – Part 233: Application protocol: Systems engineering. Geneva: International Organization for Standardization (ISO). 800 p.
- ISO 15926. 2004. Industrial automation systems and integration – Integration of life-cycle data for process plants including oil and gas production facilities (Several parts, Part 1 published 2004). Geneva: International Organization for Standardization (ISO).
- ISO/IEC 15026-1. 2013. Systems and Software Engineering – Systems and Software Assurance – Part 1: Concepts and Vocabulary. Geneva: International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC). 24 p.
- ISO/IEC TR 24774-2010 Systems and Software Engineering – Life Cycle Management – Guidelines for Process Description. Geneva: International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC). 15 p.
- ISO/IEC TR 24748-1. 2010 Systems and Software Engineering – Life Cycle Management – Part 1: Guide for Life Cycle Management. Geneva: International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC). 76 p.
- ISO/IEC 12207. 2008. Systems and software engineering – Software life cycle processes. Geneva: International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC). 123 p.

- ISO/IEC/IEEE 15288. 2015. Systems and software engineering – System life cycle processes. Geneva: International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) and New York: Institute of Electrical and Electronics Engineers (IEEE). 108 p.
- ISO/IEC/IEEE 15289. 2015. Systems and software engineering – Content of life-cycle information products (documentation). Geneva: International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) and New York: Institute of Electrical and Electronics Engineers (IEEE). 84 p.
- ISO/IEC 26702 2007. Systems engineering -- Application and management of the systems engineering process. Geneva: International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC). 87 p.
- ISO/IEC/IEEE 42010. 2011. Systems and software engineering – Architecture description. Geneva: International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) and New York: Institute of Electrical and Electronics Engineers (IEEE). 37 p.
- ITER. 2009. Systems Engineering Management Plan (SEMP). Saint-Paul-lès-Durance: ITER Organisation. Document 2F68EX_v2_2. 84 p.
- NASA. 2007. Systems Engineering Handbook, Washington D.C.: National Aeronautics and Space Administration, NASA Headquarters. 340 p.
- STUK. 2013a. Safety design of a nuclear power plant. Guide YVL B.1. 2013. Helsinki: Radiation and Nuclear Safety Authority (STUK) in Finland. 46 p.
- STUK. 2013b. Electrical and I&C equipment of a nuclear facility. Guide YVL E.7. 2013. Helsinki: Radiation and Nuclear Safety Authority (STUK) in Finland. 34 p.
- STUK. 2013c. Safety design of a nuclear power plant. Guide YVL D.4. 2013. Helsinki: Radiation and Nuclear Safety Authority (STUK) in Finland. 22 p.
- STUK. 2014. Management system for a nuclear facility. Guide YVL A.3. Helsinki: Radiation and Nuclear Safety Authority (STUK) in Finland. 20 p.
- Tommila, T. & Alanen, J. 2015. Conceptual model for safety requirements specification and management in nuclear power plants. Espoo: VTT. VTT Technology: 238. 120 p. + app. 26 p.

Appendix 1. ITER SEMP Table of Contents

1. INTRODUCTION
2. PURPOSE
3. REFERENCES
4. SCOPE OF THE SEMP
5. SYSTEMS ENGINEERING PROCESS FOR ITER
 - 5.1. SYSTEMS ENGINEERING APPROACH
 - 5.2. INTRODUCTION TO PROCESS CONCEPT
 - 5.3. INTRODUCTION TO A STANDARDIZED SE PROCESS
6. ITER PROJECT'S DESCRIPTION
 - 6.1. ITER PROJECT
 - 6.2. MASTER SCHEDULE OF ITER PROJECT
 - 6.3. MASTER COST OF ITER PROJECT
7. ITER SE PARTICIPANTS
 - 7.1. PRINCIPAL DEPUTY DIRECTOR GENERAL (PDDG)
 - 7.2. SENIOR SCIENTIFIC ADVISER FOR TECHNICAL INTEGRATION (SSATI)
 - 7.3. SENIOR ADVISER FOR INDUSTRIAL MATTERS (SAIM)
 - 7.4. LICENSING & QUALITY
 - 7.5. PROJECT OFFICE
 - 7.6. OFFICE FOR CENTRAL INTEGRATION AND ENGINEERING
 - 7.6.1. Technical Integration Division
 - 7.6.2. CAD& Design Coordination Division
 - 7.6.3. Nuclear Safety & Env. Division (NSE)
 - 7.6.4. Assembly & Operations
 - 7.7. DOMESTIC AGENCIES
 - 7.7.1. Integrated Product Teams
 - 7.8. TECHNICAL DEPARTMENTS
8. ITER GENERIC LIFE CYCLE
 - 8.1. CONCEPTUAL DESIGN
 - 8.2. PRELIMINARY DESIGN PHASE
 - 8.3. FINAL DESIGN PHASE
 - 8.4. FABRICATION, ASSEMBLY AND TESTS
 - 8.5. OPERATIONS AND SUPPORT PHASE
 - 8.6. PROJECT CLOSE-OUT
 - 8.6.1. Deactivation
 - 8.6.2. Decommissioning
 - 8.7. DECISION GATES
9. MAPPING OF ITER SE PROCESSES
10. CUSTOMER NEEDS IDENTIFICATION
 - 10.1. TECHNICAL REQUIREMENT DEFINITION
 - 10.1.1. Functional requirement
 - 10.1.2. Requirements analysis
 - 10.2. DESIGN SOLUTION DEFINITION
 - 10.2.1. Design Input
 - 10.2.2. Design Output
 - 10.2.3. Responsibility during the design
 - 10.2.4. Design activities
 - 10.3. NUCLEAR LICENSING & SAFETY CONTROL
 - 10.4. PROJECT PLANNING
 - 10.4.1. Technical Planning of Systems
 - 10.4.2. Plant Breakdown Structures-PBS
 - 10.4.3. Work Breakdown Structure-WBS
 - 10.5. REQUIREMENTS MANAGEMENT
 - 10.6. INTERFACE MANAGEMENT
 - 10.7. CONFIGURATION MANAGEMENT
 - 10.7.1. Project baselines
 - 10.7.2. Baseline development:
 - 10.8. TECHNICAL DATA MANAGEMENT
 - 10.9. TECHNICAL PROGRESS ASSESSMENT (DESIGN REVIEWS)
 - 10.9.1. Conceptual Design Review (CDR) Meeting

- 10.9.2. Preliminary (Development) Design Review (PDR) Meeting
- 10.9.3. Final Design Review (FDR) Meeting
- 10.9.4. Reviews during Fabrication, Assembly, Installation and Test (FAIT) phase
- 10.9.5. Operational Readiness Review (ORR) Meeting
- 10.9.6. Design Reviews and Procurement Arrangements
- 10.10. RISK MANAGEMENT (CONSTRUCTION PHASE ONLY)
- 10.11. MANUFACTURING
- 10.12. ASSEMBLY AND INSTALLATION
- 10.13. VERIFICATION AND VALIDATION
 - 10.13.1. Design verification
 - 10.13.2. Product verification
- 10.14. COMMISSIONING
- 10.15. HANDOVER
- 10.16. OPERATION
- 10.17. EXPERIMENTAL PROGRAMME
- 10.18. MAINTENANCE, SUPPORT AND UPGRADE
- 10.19. DECOMMISSIONING (DEACTIVATION PHASE)
- 10.20. SE PROCESS MANAGEMENT
- 10.21. SPECIALTY ENGINEERING PROCESSES
 - 10.21.1. Nuclear Safety and Environment Engineering
 - 10.21.2. RAMI Management
 - 10.21.3. Human Factor Management
 - 10.21.4. ILS Management
- 10.22. OTHER DISCIPLINES
 - 10.22.1. CAD Design Management
 - 10.22.2. Analysis and Standards management
 - 10.22.3. Parts and Material Standardization Management
 - 10.22.4. Value Engineering Management
 - 10.22.5. Vacuum Engineering
 - 10.22.6. Electrical Engineering
 - 10.22.7. Building Integration Management
 - 10.22.8. Hot Cell Engineering
 - 10.22.9. I&C (CODAC) Management
 - 10.22.10. Constructability Management
 - 10.22.11. Remote Handling Management
 - 10.22.12. Water Cooling Engineering
 - 10.22.13. Cryogenics Engineering
 - 10.22.14. Tritium Engineering
 - 10.22.15. Radwaste Engineering
 - 10.22.16. HAZOP Engineering
- 11. CONCLUSION

Appendix 2. F4E SEMP Table of Contents

- 1 Introduction
- 2 ITER Project description
 - 2.1 ITER project
 - 2.2 Master Schedule of ITER
 - 2.3 Master Cost of ITER Project
- 3 EU-ITER Department Organisation
 - 3.1 EU ITER Department
 - 3.2 Project Office
 - 3.3 Technical Support Services
 - 3.4 IC and EC Antenna & Plasma Engineering
 - 3.5 Diagnostics
 - 3.6 Cryoplat and Fuel Cycle
 - 3.7 Magnets and Vacuum Vessel
 - 3.8 In Vessel
 - 3.9 Neutral Beam and Gyrotron Power Supplies
 - 3.10 TBM and Materials Development
 - 3.11 Remote
 - 3.12 Site and Buildings and Power Supplies
- 4 ITER Life Cycle
 - 4.1 Conceptual Design
 - 4.2 Preliminary Design Phase
 - 4.3 Final Design Phase
 - 4.4 Fabrication, Assembly and
 - 4.5 Operations and Support Phase
 - 4.6 Project Close-Out
 - 4.7 Decision Gates
- 5 System Engineering Process Approach
 - 5.1 Introduction to process concept
 - 5.2 System Engineering Processes According to ISO 15288
 - 5.3 Mapping Of ITER System Engineering Processes
- 6 External Technical Core Processes
 - 6.1 Customer Needs Identification
 - 6.2 System Design Development
 - 6.3 Commissioning
 - 6.4 Operation
 - 6.5 Experimental Programme
 - 6.6 Deactivation / Decommissioning
- 7 F4E System Engineering Management Processes
 - 7.1 Project Planning
 - 7.2 Requirements Management
 - 7.3 Interfaces Management
 - 7.4 Configuration Management
 - 7.5 Reviews (project assessment process)
 - 7.6 Contract & Supplier Management & Control
 - 7.7 Risk Management
 - 7.8 Information (and data) Management
 - 7.9 System Engineering Management
- 8 F4E System Engineering Technical Core Processes
 - 8.1 ITAs
 - 8.2 Procurement Arrangements
 - 8.3 Procurement Technical Specification development
 - 8.4 Procurement
 - 8.5 Design (suppliers)
 - 8.6 Manufacturing
 - 8.7 Verification &
 - 8.8 Assembly, Installation & System Testing
 - 8.9 Handover
 - 8.10 Maintenance, Support & Upgrade

9 F4E Specialty Engineering Processes & Disciplines

- 9.1 Nuclear Safety
- 9.2 RAMI Engineering
- 9.3 Plasma Engineering
- 9.4 Integrated Logistics Support Engineering
- 9.5 Non-Destructive Testing
- 9.6 CAD Design and Functional Dimensioning & Tolerancing
- 9.7 Codes & Standards
- 9.8 Analysis
- 9.9 Electronics, Software and Control
- 9.10 Materials Characterization
- 9.11 Transport
- 9.12 Manufacturing Quality

10 Other disciplines

11 Management Tools

12 Conformity Matrix w.r.t ISO 15288

Appendix 3. DoD Systems Engineering Plan (SEP) Table of Contents

1. Program Technical Requirements
 - 1.1. Architectures and Interface Control
 - 1.2. Technical Certifications
2. Engineering Resources and Management
 - 2.1. Technical Schedule and Schedule Risk Assessment
 - 2.2. Engineering Resources and Cost/Schedule Reporting
 - 2.3. Engineering and Integration Risk Management
 - 2.4. Technical Organization
 - 2.5. Relationships with External Technical Organizations
 - 2.6. Technical Performance Measures and Metrics
3. Technical Activities and Products
 - 3.1. Results of Previous Phase SE Activities
 - 3.2. Planned SE Activities for the Next Phase
 - 3.3. Requirements Development and Change Process
 - 3.4. Technical Reviews
 - 3.5. Configuration and Change Management Process
 - 3.6. Design Considerations
 - 3.7. Engineering Tools

Annex A – Acronyms

Appendix 4. ISO/IEC 26702 / IEEE Std 1220 example SEMP table of contents

- 1.0 Scope
- 2.0 Applicable Documents
- 3.0 Systems Engineering Process (SEP) Application
 - 3.1 Systems Engineering Process Planning
 - 3.1.1 Major Deliverables and Results
 - 3.1.1.1 Integrated Repository
 - 3.1.1.2 Specifications and Baselines
 - 3.1.2 Process Inputs
 - 3.1.3 Technical Objectives
 - 3.1.4 System Breakdown Structure (SBS)
 - 3.1.5 Training
 - 3.1.6 Standards and Procedures
 - 3.1.7 Resource Allocation
 - 3.1.8 Constraints
 - 3.1.9 Work Authorization
 - 3.2 Requirements Analysis
 - 3.3 Requirements Baseline Validation
 - 3.4 Functional Analysis
 - 3.5 Functional Verification
 - 3.6 Synthesis
 - 3.7 Design Verification
 - 3.8 Systems Analysis
 - 3.8.1 Trade-Off Analyses
 - 3.8.2 System/Cost-Effectiveness Analyses
 - 3.8.3 Risk Management
 - 3.9 Control
 - 3.9.1 Design Capture
 - 3.9.2 Interface Management
 - 3.9.3 Data Management
 - 3.9.4 Systems Engineering Master Schedule (SEMS)
 - 3.9.5 Technical Performance Measurement
 - 3.9.6 Technical Reviews
 - 3.9.7 Supplier Control
 - 3.9.8 Requirements Traceability
- 4.0 Transitioning Critical Technologies
- 5.0 Integration of the Systems Engineering Effort
 - 5.1 Organizational Structure
 - 5.2 Required Systems Engineering Integration Tasks
- 6.0 Additional Systems Engineering Activities
 - 6.1 Long-Lead Items
 - 6.2 Engineering Tools
 - 6.3 Design to Cost
 - 6.4 Value Engineering
 - 6.5 Systems Integration Plan
 - 6.6 Interface with Other Life Cycle Support Functions
 - 6.7 Safety Plan
 - 6.8 Other Plans and Controls
- 7.0 Notes
 - 7.1 General Background Information
 - 7.2 Acronyms and Abbreviations
 - 7.3 Glossary

FIGURES

TABLES

APPENDICES

Appendix 5. YVL A.3 requirements for management system processes (including project and systems engineering processes)

601. The processes of the management system shall be planned and implemented in a controlled manner. The development of each process shall ensure that the requirements, interfaces, interaction with other processes, and the risks relating to the activities have been identified and taken into consideration. The process flow and phases as well as the measurement and assessment procedures necessary for continuous improvement shall be specified and described.

602. The responsibilities and procedures for process implementation, evaluation, and development shall be specified process by process.

603. Written instructions shall be provided for process-related procedures and the manner of carrying out the activities. The possibility of human error in work performances shall be taken into account when defining the processes and the activities contained in them. The processes shall be planned so as to identify and disclose potential errors as early in the process as possible.

604. For each process, the necessary inspection, testing, verification, and validation phases, the acceptance criteria for each phase, and the responsibilities for the performance of the activities shall be specified. It shall also be specified if these activities are to be performed by individuals other than those responsible for the process.

605. The work performances shall be planned. Work shall be carried out under controlled conditions using only the approved instructions and procedures as well as the appropriate equipment. Each individual shall be responsible for the quality of his or her work. The personnel shall be given adequate training and instructions prior to starting work.

606. The management system shall have established procedures for the control of outsourced processes and activities.

607. Process implementation and effectiveness shall be continuously followed and periodically assessed. The processes and guidelines shall be continuously improved.

608. The management system processes shall be specified, and they shall be suitable for the relevant stage in the life cycle of the nuclear facility. They shall take into account radiation and nuclear safety as well as the co-ordination of security and emergency preparedness arrangements.

609. In defining and establishing the processes, the requirements specific to each stage shall be observed as regards, e.g., documentation, instructions, management of interfaces, transfer of responsibilities, research and analysis, and training.

610. The requirements and guidelines in the IAEA publications [6–15] shall be taken into account in defining and establishing processes for the different stages in the life cycle of the nuclear facility.

611. Throughout the life cycle of the facility, the management system shall include the generic processes described in 6.2.1–6.2.7 to support safety and quality management.

612. The documents shall be managed by systematic procedures. Document management shall cover documents needed in the operation of the facility and organisations, such as documentation for the nuclear facility as well as the documents for design, construction, commissioning, operation, decommissioning, and final disposal. In addition, procedures and requirements shall be defined for the documentation of activities and events and for storing and archiving the resulting documents. With regard to the documents pertaining to final disposal, additional attention shall be paid to maintaining the readability of the documents and their availability to different organisations even after a very long period of time.

613. The document management procedures shall be described. They include, among other things, the identification, preparation, drawing up, review, approval, implementation, revision, distribution, archival, and disposal of documents. The documents to be kept permanently or temporarily and their storage periods shall be defined. The materials and recording methods used shall meet the requirements for long-time storage and availability, if necessary. The document management system shall also take into account the information security requirements.

614. In drawing up, reviewing, and approving a document, the independence principle shall be applied. The drawing up, revision, review, and approval of a document shall be based on a defined authorisation. The management system shall guide the personnel towards the use of appropriate documents.

615. The documents to be updated and the updating procedures shall be specified, taking into account the documents' safety significance and regulatory requirements.

616. The requirement specifications of products shall conform with the applicable regulations, guides, and standards.

617. Prior to a product's approval, realisation, or commissioning, its conformity shall be assured by the necessary inspection, testing, verification, validation, and qualification. The methods and tools used shall be suitable for their purpose. Approval of the product documentation shall be attached to a product approval document.

618. Products must be identifiable to ensure their correct use. Where traceability is a requirement, a control procedure to identify products shall be arranged and documented.

619. Products shall be handled, transported, stored, maintained, and used according to instructions in order to avoid their damaging, loss, deterioration, or inadvertent misuse.

620. The records generated during activities and the procedures pertaining to their management shall be defined. The records shall be specified, identifiable, readable, and easily traceable.

621. The retention times of records, associated test pieces, and testing materials shall be defined. The recording media, the manner of recording, and the storage conditions shall ensure readability for the duration of the retention period specified for each record. In specifying the retention period, the nuclear facility's life cycle and the long duration of nuclear waste management shall be considered.

622. Systematic procedures shall be in place for the purchasing of the nuclear facility and its systems, structures, components, supplies, and services so as to ensure the conformity and validity of the purchased products.

623. Systematic procedures shall be in place for defining the requirements for purchased products.

624. Adequate quality requirements shall be established for products and compliance with the quality requirements and achievement of the required quality level shall be ensured. There shall be adequately qualified personnel to specify the quality requirements and to control the products and suppliers.

625. Systematic procedures shall be in place for resolving and reporting deviations from the purchasing requirements.

626. The requirements for the selection of suppliers and the selection procedures shall be defined. These shall include the requirements pertaining to the supplier's management system and its quality management.

627. Appropriate procedures shall be in place for supplier assessment and selection. Records shall be kept of the assessments. Prior to ordering a product, the supplier's ability to deliver the product and the related documentation in compliance with the requirements shall be evaluated. Where necessary, a follow-up audit shall be used to ensure the supplier's capability to deliver a product compliant with the requirements prior to the commencement of manufacturing.

628. A list shall be kept of suppliers approved on the basis of assessment. The approval of suppliers of products important to safety shall be for a fixed duration only. The periods of validity shall be defined in the purchasing procedures.

629. Suppliers of safety-significant products shall have in place a management system that is appropriately certified or independently evaluated by a third party. In addition, the suppliers of products in safety class 1 and 2 shall comply with the management system requirements set forth in this guide. As necessary, the licensee may apply the procedure described in 630 with regard to suppliers that supply products related to structures or components in the safety class 2. The application of the procedure shall be justified.

630. The selection procedures shall define when a supplier referred to in 629 shall present a quality plan for the delivery, including the quality assurance procedures to complement its management system. The quality plan (see the annex) shall present the quality management procedures used for ensuring that the quality management requirements specified in the YVL guides and those set by the licensee are realised in the purchasing process.

631. The meeting of requirements set for products shall be ensured prior to commissioning. Product conformity shall be systematically monitored. The experiences of the product shall be evaluated for possible further actions and the supplier shall be given feedback on the product, where necessary.

632. The purchasing procedures shall define the conditions for the supplier's use of subcontractors and for the communication and relaying of requirements within the supply chain.

633. The management system shall define procedures for the licensee to ensure that, when purchasing sets of equipment involving several fields of technology, the contractual relationships and responsibilities within the entire supply chain are unambiguously defined.

634. The licensee is responsible for supervising all the suppliers in the supply chain. The licensee shall also incorporate the oversight rights of authorities into the supervision procedures.

635. For all purchases, the documentation to be attached to a product and control during product manufacture and implementation shall be defined. The control procedures shall be presented in supplier-specific delivery control plans.

636. The purchasing procedures shall contain procedures for the purchasing of type-approved, serial products for safety-significant components. The procedures shall define the validation of the suitability and conformity of the products as well as the documentation to be attached to the product.

637. Suppliers shall draw up a delivery-specific quality plan for the supply of safety-significant products. Through the use of a quality plan, it can be ensured that a product supplier has correctly understood the requirements of quality management applicable to the delivery and demonstrates that the supplier has in place procedures to fulfil the requirements.

638. A single quality plan may be used for all products that have the same quality management requirements and the same implementing organisations guided by the quality plan. In case of minor differences between the quality management objectives of different products, the differences may be specified in a shared quality plan.

639. The contents of a quality plan for deliveries is described in an Annex to this Guide. Field of technology-specific YVL guides set forth detailed requirements for the contents of quality plans and their submission to the Radiation and Nuclear Safety Authority. The standard ISO 10005, for example, can be applied to the drawing up of a quality plan.

640. The licensee shall have in place procedures to reliably prevent the purchasing of counterfeit and fraudulent products.

641. The management system shall include procedures and means for communicating matters related to nuclear and radiation safety, quality, and security and emergency preparedness arrangements within the organisation and to interest groups.

642. The life cycle stage of the nuclear facility shall be taken into account when planning and implementing communications.

643. In developing the organisation's structure or ways of working, it shall be ensured that the changes implemented support the achievement of safety goals and that the implementation process is controlled.

644. Objectives shall be set for organisational changes. The safety implications of the changes shall be assessed. The planning and implementation of changes shall be proportioned to the outcome of the assessment. The different phases of a change shall be documented.

645. Organisational changes that significantly affect the organisation's operation shall also be subject to an independent evaluation.

646. The implementation of changes shall be planned and supervised. The management shall ensure adequate communication during the different phases of organisational change. The justifications for and method of implementing the changes shall be documented.

647. Safety-significant organisational changes shall also be evaluated after implementation. The evaluation verifies if the safety objectives set for the change are met.

648. The management system shall have documented procedures for project leadership, management, and progress assessment. There shall be a set of instructions for drawing up the project plan as well as the risk management, resource, and quality plan for the project.

649. A project shall be set up for the construction of new nuclear facilities, operating licence renewals, periodic safety assessments and, if considered necessary, plant modifications or other modification projects. The projects shall be described in a project plan and complemented, where necessary, with a project-specific resource, risk-management, and quality plan.

650. The project plans for modification projects important to safety, the associated human resource and quality plans, and the safety and quality-related risk management plans shall be submitted to STUK for information.

651. Project management shall comply with the applicable standards.

Appendix 6. YVL B.1 selected requirements for management system processes (including project and systems engineering processes)

The requirements below are from sections 3.2 (Design processes) and 3.4 (Quality plans) of YVL B.1. There are other management system related requirements in YVL B.1, but the selected requirements below are considered to be the most important when planning the systems engineering processes.

311. A nuclear power plant and the systems important to safety shall be designed by using design processes and methods appropriate for the required level of quality, and by applying the relevant safety regulations, guidelines and standards. The selection of the standards applied in design shall be justified in terms of suitability and coverage.

312. The design of systems important to safety shall be based on a life-cycle model where design and implementation are divided into stages. The life-cycle model shall comprise all successive stages from the determination of the applicable requirements to the operation stage. In particular, the life-cycle model shall include a separate requirement specification stage that precedes the actual design stages.

313. Each design and implementation stage shall be verified. The verification activities and methods shall be duly planned.

314. Each design and implementation stage shall be reviewed before the stage is declared as complete.

315. The licence applicant/licensee shall reserve the opportunity to participate in the review of any of the stages. The licence applicant/licensee shall participate in any reviews that are important in terms of safety. The licence applicant/licensee shall reserve the right to abort the stage if it is obvious that the safety requirements are not fulfilled.

316. The organisations involved in the design shall have capable processes in place for managing requirements.

317. In design tasks involving several fields of technology, a communication process shall be provided to ensure due exchange of information across the organisational interfaces.

318. The participation of competent personnel in every aspect of design that is relevant to safety shall be ensured through stage reviews covering several fields of technology.

331. For the purpose of designing and implementing systems important to safety and any modifications to such systems, a quality plan specific to each individual system shall be prepared and adopted. However, the same quality plan may be utilised for several systems if the quality objectives, the methods for attaining the quality objectives and the organisation implementing the plan are the same for all the systems concerned.

332. The quality plan shall present

1. the organisation designing the system, complete with responsibilities and interfaces to other organisations involved in design;
2. the standards and guidelines, including the YVL Guides, to be applied in the design and implementation;
3. the stages of the design and implementation process;
4. the documents, records and other stage inputs serving as input data for each design stage;
5. the documents, records and other stage outputs created as an outcome of each design stage;
6. the stage reviews upon completion of individual stages including the timing, content and performer of the stage review, acceptance criteria, and the applicable decision-making procedures and responsibilities;
7. the procedures used in the supervision of subcontractors;
8. configuration and change management and procedures for product identification;
9. the management of conformity, design changes, and management of non-conformities;
10. the support processes utilised concurrently with design and implementation, complete with the associated management and quality procedures;
11. the division of responsibilities for the processes and decision-making procedures, including the procedures for modifying the quality plan.

333. The system-specific quality plan shall be prepared and implemented in compliance with the requirements set out in this YVL Guide and an applicable standard.

334. When standards-compliant processes and the quality manual of the design organisation are used, a detailed description of the application of the processes and guidelines shall be provided in the quality plan.

335. The requirements for the quality plan that complements the supplier's management system included in the delivery are set out in Guide YVL A.3.