



**RESEARCH REPORT**

VTT-R-00478-16



# **A reference model for the NPP I&C qualification process and safety demonstration data**

Authors: Jarmo Alanen & Teemu Tommila

Confidentiality: Public

<b>Report's title</b>		
A reference model for the NPP I&C qualification process and safety demonstration data		
<b>Customer, contact person, address</b>		<b>Order reference</b>
SAFIR2018 programme		
<b>Project name</b>		<b>Project number/Short name</b>
Integrated safety assessment and justification of nuclear power plant automation		102392 / SAUNA
<b>Author(s)</b>		<b>Pages</b>
Jarmo Alanen & Teemu Tommila		43, 21 appendix pages
<b>Keywords</b>		<b>Report identification code</b>
Nuclear, Instrumentation and control, Systems Engineering, Qualification, Safety demonstration		VTT-R-00478-16
<b>Summary</b>		
<p>This report presents a qualification process example and safety demonstration data metamodel we suggest to be used in qualification of I&amp;C systems, equipment and components of nuclear power plants. By utilising such model-based systems engineering approach in assuring the safety of complex I&amp;C systems, the engineering and conformity assessment effort can be managed more rigorously, yet with better agility due to possibility of automatic generation of documents. The systematic process and data models help identify gaps in fulfilling the process and product safety requirement. Applicability of the safety demonstration data metamodel is demonstrated by a simple case example.</p>		
<b>Confidentiality</b>	Public	
Tampere 15.11.2016		
<b>Written by</b>	<b>Reviewed by</b>	<b>Accepted by</b>
Jarmo Alanen Senior Scientist	Janne Valkonen Senior Scientist	Johannes Hyrynen, Head of research area
<b>VTT's contact address</b>		
Jarmo Alanen, PL 1300, FI-33101 Tampere; jarmo.alanen@vtt.fi, +358 40 501 5813		
<b>Distribution (customer and VTT)</b>		
SAFIR2018 program VTT / archive, original		
<p><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></p>		

## 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 2016 consisted of several tasks of which this report relates to Task 1.1 (Planning and management of qualification process and safety demonstration data) of Work package 1 (Safety Systems Engineering). The members of Task 1.1 were Jarmo Alanen (VTT), Teemu Tommila (VTT) and Janne Valkonen. The goal of Task 1.1 was “...to create a reference model for the qualification process and safety demonstration data.” (An excerpt of the SAUNA 2016 project plan.)

The goal of this report is to document the created reference model and to provide the rationale for the design decisions.

Task 1.1 as well as the whole SAUNA project was steered by the Reference Group 1 (Automation, organisation and human factors). The authors thank the RG1, and especially Mika Johansson (STUK), Janne Peltonen (Fennovoima), Mauri Viitasalo (TVO) and Ville Lestinen and his colleagues (Fortum) for guiding the work. We also thank Kirsi Hassinen (TVO) and Aarno Keskinen (TVO) for providing us with valuable background information and documentation examples. We also thank Joonas Linnosmaa (VTT) for the support in creating the qualification process activity diagrams and Janne Valkonen (VTT) for reviewing the report.

Tampere 15.11.2016

Authors

## Contents

---

Preface.....	2
Contents.....	3
1. Introduction, goal and scope .....	4
1.1 Scope .....	4
1.2 Definitions and abbreviations .....	5
2. Basis of the work.....	9
2.1 Applicable documents.....	9
2.2 Conformity assessment constructs .....	10
2.3 Basic statements .....	12
3. Qualification process model .....	16
3.1 Description of the process under study .....	16
3.2 The resulted qualification process model .....	17
3.3 Method for describing the qualification process model .....	27
4. Safety demonstration data model.....	29
4.1 IEC/IEC 15026-2 C-A-E structure .....	29
4.2 SACM 2.0 C-A-E structure .....	30
4.3 Suggested data model.....	33
4.4 A case example using the suggested data model .....	36
4.5 Automatic generation of claim and argument sentences.....	39
5. Summary and conclusions .....	41
References.....	42
Appendix 1. Quality process template (draft) .....	44

## 1. Introduction, goal and scope

One of the goals of the SAUNA project (a SAFIR2018 programme project) in year 2016 was to create a reference model for the qualification process and safety demonstration for the NPP automation sector. The aim of this report is to help the licensees of nuclear facilities, their automation suppliers and the authorities to assess NPP I&C systems according to the systems engineering principles. The ultimate goals of this work are assured safety, quality and shorter qualification times of NPP I&C systems, subsystem and components.

The goal is, as stated above, twofold:

- to create a qualification process model
- to create a safety demonstration data model.

Note that we consider ‘qualification’ an activity (or a set of activities) and ‘safety demonstration’ an artefact (or a set of artefacts). In both cases, we apply Model Based Systems Engineering<sup>1</sup> to define the reference model.

In terms of the IDEF0 metamodel for systems engineering processes, we define thus the model for the parts of the metamodel as depicted in Figure 1.

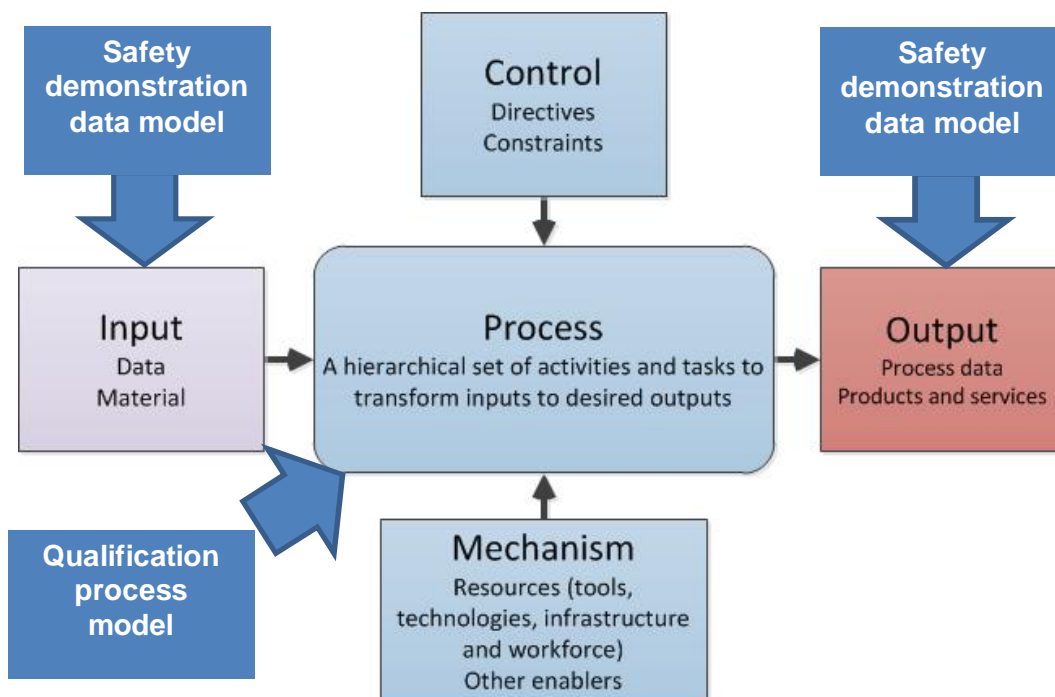


Figure 1. IDEF0 metamodel for systems engineering processes with the indication of the scope of this report (the IDEF0 model is modified from [INCOSE 2007]).

In fact, the qualification and safety demonstration data reference model means that we create a qualification process example and safety demonstration data metamodel.

### 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

<sup>1</sup> See definition of Model Based Systems Engineering in Table 2.

*Systems Engineering Management Plan (SEMP) template.*” In this work, we concentrate on I&C systems but we also consider the equipment and component level. Hence the organisations-of-interest are authorities, licensees, (plant suppliers,) I&C system suppliers, equipment suppliers and component suppliers. We try to make the process model and the data model generic enough to be utilised and applied on such organisations. Nevertheless, our focus is in the licensee point of view concerning qualification of I&C systems, equipment and components. Furthermore, the collaboration between the licensee and the supplier (of system, sub-system or component) is taken into account.

## 1.2 Definitions and abbreviations

The abbreviations used in the report are listed in Table 1.

*Table 1. Abbreviations.*

Abbreviation	Description
<b>ARG</b>	Argumentation Metamodel
<b>C-A-E</b>	Claim-Argument-Evidence
<b>EU</b>	European Union
<b>IAEA</b>	International Atomic Energy Association
<b>I&amp;C</b>	Instrumentation and Control
<b>INCOSE</b>	International Council on Systems Engineering
<b>MBSE</b>	Model Based Systems Engineering
<b>NDI</b>	Non-Developmental-Item
<b>NPP</b>	Nuclear Power Plant
<b>OMG</b>	Object Management Group
<b>PLM</b>	Product Life cycle Management
<b>SACM</b>	Structured Assurance Case Metamodel
<b>SEAM</b>	Structured Assurance Evidence Metamodel
<b>SE</b>	Systems Engineering
<b>SEMP</b>	Systems Engineering Management Plan
<b>STUK</b>	Säteilyturvakeskus (Radiation and Nuclear Safety Authority)
<b>TVO</b>	Teollisuuden voima Oyj
<b>V&amp;V</b>	Verification and Validation
<b>XML</b>	eXtensible Markup Language

Some key concepts used in this report are defined in Table 2.

*Table 2. Key concepts.*

Definition	Description
<b>Artefact</b>	A synonym to <i>Work product</i>
<b>Attestation</b>	Issue of a statement, based on a decision following review, that fulfilment of specified requirements has been demonstrated [source: ISO 17000:2004]  NOTE: In this report, attestation is considered to include the review activity (which we call assessment), although in case of certification at component level, the attestation may be independent of the review. Furthermore, the activities to prepare for the approval are included in the set of attestation activities.

Definition	Description
<b>Assurance case</b>	<p>1. Reasoned, auditable artefact created that supports the contention that its top-level claim (or set of claims), is satisfied, including systematic argumentation and its underlying evidence and explicit assumptions that support the claims(s)</p> <p>NOTE 1: An assurance case contains the following and their relationships:</p> <ul style="list-style-type: none"> <li>• one or more claims about properties</li> <li>• arguments that logically link the evidence and any assumptions to the claims(s)</li> <li>• a body of evidence and possibly assumptions supporting these arguments for the claim(s)</li> <li>• justification of the choice of top-level claim and the method of reasoning.</li> </ul> <p>[source: ISO/IEC 15026-1 2013]</p> <p>2. A collection of auditable claims, arguments, and evidence created to support the contention that a defined system/service will satisfy its assurance requirements.</p> <p>[source: Structured Assurance Case Metamodel (SACM) Version 2.0 (December 2015 draft)]</p>
<b>Certification</b>	<p>Third-party attestation related to products, processes, systems or persons [source: ISO 17000:2004]</p>
<b>Configuration item</b>	<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 information item or a collection of information items, or any other engineering artefact, 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>
<b>Conformity assessment</b>	<p>Demonstration that specified requirements relating to a product, process, system, person or body are fulfilled</p> <p>[source: IEC Glossary]</p>
<b>Determination</b>	<p>Activity to find out one or more characteristics and their characteristic values</p> <p>[source: ISO 9000:2015]</p>
<b>Information item</b>	<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 configuration item, 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>
<b>Management system</b>	<p>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]</p>
<b>Model based systems engineering</b>	<p>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. [Source: INCOSE Systems Engineering Vision 2020, INCOSE-TP-2004-004-02, September, 2007]</p>
<b>Process</b>	<p>Set of interrelated or interacting activities that transforms inputs into outputs.</p> <p>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.</p> <p>[source: ISO/IEC/IEEE 15288 2015, except the note, which is by the authors of this report]</p>

Definition	Description
<b>Process view</b>	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]
<b>Qualification</b>	<ol style="list-style-type: none"> <li>1) Qualification shall refer to a process to demonstrate the ability to fulfil specified requirements (corresponds to the qualification process of the ISO 9000 standard). [Source YVL Glossary by STUK] [ISO 9000:2015 does not define the term qualification (process) any more]</li> <li>2) Process of determining whether a system or component is suitable for operational use.               <ul style="list-style-type: none"> <li>• Qualification is generally performed in the context of a specific set of qualification requirements for the specific facility and class of system and for the specific application.</li> <li>• Qualification may be accomplished in stages: e.g., first, by the qualification of pre-existing equipment (usually early in the system realization process), then, in a second step, by the qualification of the integrated system (i.e. in the final realized design).</li> <li>• Qualification may rely on activities performed outside the framework of a specific facility design (this is called 'generic qualification' or 'prequalification').</li> <li>• Prequalification may significantly reduce the necessary effort in facility specific qualification; however, the application specific qualification requirements must still be met and be shown to be met.</li> </ul> </li> </ol> <p><b>Equipment qualification.</b> Generation and maintenance of evidence to ensure that equipment will operate on demand, under specified service conditions, to meet system performance requirements.</p> <p>See IAEA GSR Part 4 (Rev. 1).</p> <ul style="list-style-type: none"> <li>• More specific terms are used for particular equipment or particular conditions; for example, seismic qualification is a form of equipment qualification that relates to conditions that could be encountered in the event of earthquakes.</li> <li>• The proof that an item of equipment can perform its function, which is an important part of equipment qualification, is sometimes termed substantiation.</li> </ul> <p>[Source IAEA Safety glossary]</p> <p>NOTE 1: In this report, we consider that <i>qualification</i> is an <i>attestation</i> activity required by an authority (internal or external), and we emphasise the distinction between <i>validation</i> and <i>qualification</i> by considering that the qualification process is assumed to only consist of the additional activities after the V&amp;V activities in high rigour projects to attest the V&amp;V results. We see this distinction important and commendable to provide for well capsulated qualification and V&amp;V processes.</p> <p>NOTE 2: In some contexts, <i>licensing</i> is used as a synonym for <i>qualification</i>; in other cases, the term licensing is only used for plant level authorisation. Due to the vague usage of the term licensing, we do not define nor use the term licensing in this report.</p>
<b>Safety demonstration</b>	<p>The set of arguments and evidence elements which support a selected set of claims on the safety of the operation of a system important to safety used in a given plant environment. [source: Common position 2014]</p> <p>NOTE 1: When safety demonstration is presented in a structured fashion it can be called a safety related <i>assurance case</i> [source: Valkonen et al. 2016]</p> <p>NOTE 2: In some contexts, <i>safety demonstration</i> is treated as an activity; here we treat it as an artefact according to Common position (2014); <i>qualification</i> is the activity that assembles the safety demonstration.</p>
<b>System</b>	<p>Combination of interacting elements organized to achieve one or more stated purposes</p> <p>NOTE 1: A system is sometimes considered as a product or as the services it provides.</p> <p>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.</p> <p>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.</p> <p>[source: ISO/IEC/IEEE 15288 2015]</p>



Definition	Description
<b>Systems engineering</b>	<p>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 [source: ISO/IEC/IEEE 15288 2015]</p> <p>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]</p>
<b>Systems engineering management plan (SEMP)</b>	<p>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]</p>
<b>Validation</b>	<p>Confirmation, through the provision of objective evidence, that the requirements for a specific intended use or application have been fulfilled</p> <p>NOTE 1: The objective evidence needed for a validation is the result of a test or other form of determination such as performing alternative calculations or reviewing documents.</p> <p>NOTE 2: The word “validated” is used to designate the corresponding status.</p> <p>NOTE 3: The use conditions for validation can be real or simulated.</p> <p>[source: SFS-EN ISO 9000:2015]</p> <p>NOTE 4: In this report, we state that validation is carried out to assess conformity to the stakeholder requirements whereas verification is carried out to assess conformity to the system requirements.</p>
<b>Verification</b>	<p>Confirmation, through the provision of objective evidence, that specified requirements have been fulfilled</p> <p>NOTE 1: The objective evidence needed for a verification can be the result of an inspection or of other forms of determination such as performing alternative calculations or reviewing documents.</p> <p>NOTE 2: The activities carried out for verification are sometimes called a qualification process.</p> <p>NOTE 3: The word “verified” is used to designate the corresponding status.</p> <p>[source: SFS-EN ISO 9000:2015]</p> <p>NOTE 4: In this report, we state that verification is carried out to assess conformity to the system requirements whereas validation is carried out to assess conformity to the stakeholder requirements.</p>
<b>Work product</b>	<p>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]</p>

## 2. Basis of the work

---

### 2.1 Applicable documents

The main applicable documents for qualification requirements of I&C systems are the following:

- STUK: YVL B.1. Classification of systems, structures and components of a nuclear facility
- STUK: YVL E.7. Electrical and I&C equipment of a nuclear facility
- IAEA: SSR-2/2. Safety of Nuclear Power Plants: Commissioning and Operation
- IAEA: GSR Part 4. Safety Assessment for Facilities and Activities
- IAEA: SSG-39. Design of Instrumentation and Control Systems for Nuclear Power Plants.
- Common position 2014: Licensing of safety critical software for nuclear reactors - Common position of international nuclear regulators and authorised technical support organisations
- IEC EN 60987, Hardware design requirements for computer-based systems
- IEC EN 60880, Software aspects for computer-based systems performing category A functions
- IEC EN 62138, Software aspects for computer-based systems performing category B or C functions
- IAEA: SSG-12. Licensing Process for Nuclear Installations
- IEC 61513: Nuclear power plants - Instrumentation and control important to safety - General requirements for systems
- IEC/IEEE 60780-323. Nuclear facilities – Electrical equipment important to safety – Qualification.

The most important models for model-based assurance cases are specified in the following two documents:

Object Management Group (OMG): Structured Assurance Case Metamodel (SACM).

ISO/IEC 15026-2: Systems and software engineering – Systems and software assurance – Part 2: Assurance case.

Other relevant background information:

IAEA: NP-T-1.13. Technical Challenges in the Application and Licensing of Digital Instrumentation and Control Systems in Nuclear Power Plants

ISO/IEC 15026-4: Systems and software engineering – Systems and software assurance – Part 4: Assurance in the life cycle.

ISO/IEC/IEEE 15288. 2015. Systems and software engineering – System life cycle processes.

## 2.2 Conformity assessment constructs

As depicted in Figure 2, there are four main phases in a regulated safety critical development process, to develop an object (blue rectangles), to determine the properties of the developed object (orange rectangles), to assess the conformity of the developed object to the requirements (green rectangles) and to attest the trustworthiness of the safety demonstration (pink rectangles). This categorisation also suggests four role categories, ‘testing personnel’, conformity assessors and attestors.

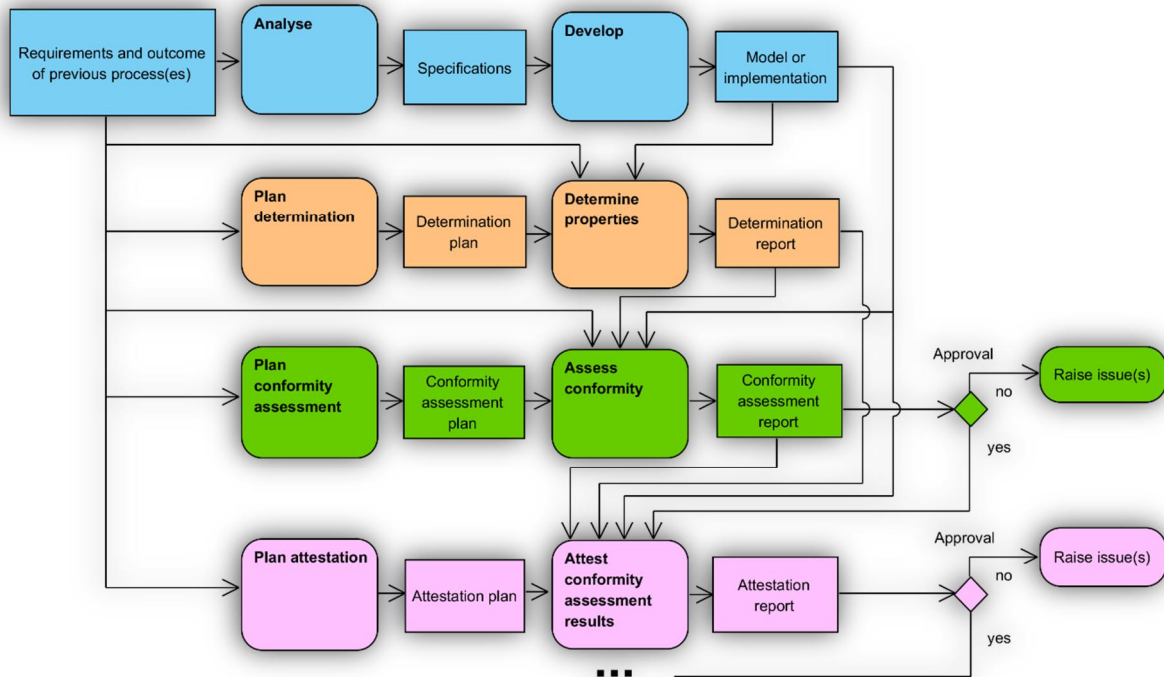


Figure 2. Develop, determine properties and assess conformity – the development process overview.

Note that the conformity assessment activities may be carried out on several levels (e.g. during verification and during validation). Also the attestation activities may be carried out on several levels, by an independent assessor within the developer organisation, by a third party assessor and by the regulator. On all the levels, the results of the previous levels are used as the main input, but also the original requirements, the system models and descriptions, and the determination reports are necessary inputs for the conformity assessments and attestations. Note also that at the different attestation levels the attestors set their own set of acceptance criteria (that are of course based on the requirements); the set of acceptance criteria is presented in the attestation plan of the particular level.

### Determination, what is it all about?

A new term, determination, is introduced in Figure 3; it is new in the engineering field, but it is defined in ISO 9000 as an “activity to find out one or more characteristics and their characteristic values”. Typical activities to find out the characteristics of the object-under-determination are testing and analysis, but there are others as depicted in Figure 3.

‘Determination’ is a good term to make a clear distinction between ‘testing’ and claiming of conformity to the requirements. The testing personnel simply determines the properties of the object-under-determination, but does not state any claims whether the properties satisfy the requirements or not; that is the responsibility of the conformity assessor. In some cases, the testing person and the conformity assessor can be one and the same person, but it is necessary to make the data model and the process model such that the two roles and their outcomes are distinct. This is due to the fact that in safety critical cases it may be required that the assessor is independent of the developers (including the testing personnel who provides the evidence, i.e. the stated actual properties of the object-under-study).

Figure 3 depicts the *Conformity assessment* constructs and the relevant constructs from the development, determination and attestation activities.

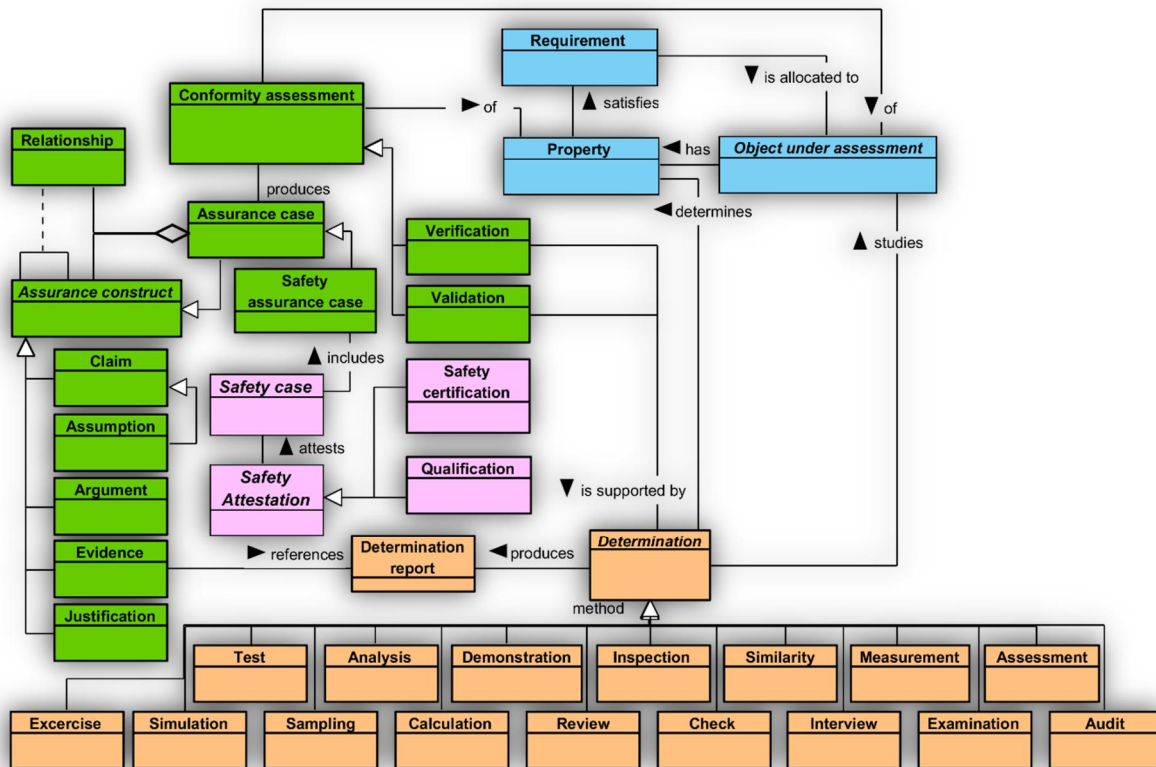


Figure 3. *Conformity assessment constructs and their relation to other relevant constructs.*

*Conformity assessment* is considered here as a general construct to model the activities to assure, through the provision of objective evidence, that the properties of the *Object under assessment* (such as systems, products, processes, persons, materials, services, functional specification or any kind of deliverables) satisfies the specified *Requirements*. Its purposes are *Verification* and *Validation*. *Conformity assessment* is supported by objective evidence (about the properties of the *Object under assessment*) determined by a *Determination* method, such as *Test*, *Analysis*, *Demonstration*, *Inspection*, *Similarity*, *Measurement*, *Assessment*, *Exercise*, *Simulation*, *Sampling*, *Calculation*, *Review*, *Check*, *Interview*, *Examination* and *Audit*. Its results are documented in a structured fashion by an *Assurance case* that consists of *Assurance constructs*, i.e. *Claims* (and *Assumptions*) and *Evidences*, and of *Arguments* that logically ties the *Evidences* to the *Claims*. The *Relationships* between the *Assurance constructs* are also part of the *Assurance case*; this completes the *Assurance case* as a structured assurance case. *Certification* and *Qualification* attest the conformity assessment results, i.e. the *Assurance cases*.

Figure 3 tries to depict that the essence of conformity assessment is to state claims (and the supporting constructs, arguments, evidence references, justifications and assumptions) that the properties of the object-under-study satisfies the specified requirements. The essence is not to produce evidence, but to evaluate the existing evidence coming from the determination activities. If dependable evidence cannot be found, the conformity assessment activities may include requesting or executing determination activities.

It should be noted that also the conformity assessment involves using the determination methods provided in Figure 3, especially *Review* method, but the conformity assessment activities differ from the determination activities in that that the conformity assessment activities are not carried out to determine the properties of the object-under-assessment but

to assess whether the properties of the object-under-assessment fulfil the requirements. Furthermore, the purpose of attestation activities (qualification and certification) is to prove that the conformity assessment results are trustworthy (i.e. to determine the properties of the safety case).

In Figure 4, an example technical process, stakeholder requirements definition process, is depicted such that the development, determination and conformity assessment activities are identified using the colour scheme of Figure 3 and Figure 2. Note that an additional colour, red, is introduced to identify configuration management activities. Note also that in this case, attestation activities are assumed not to be carried out.

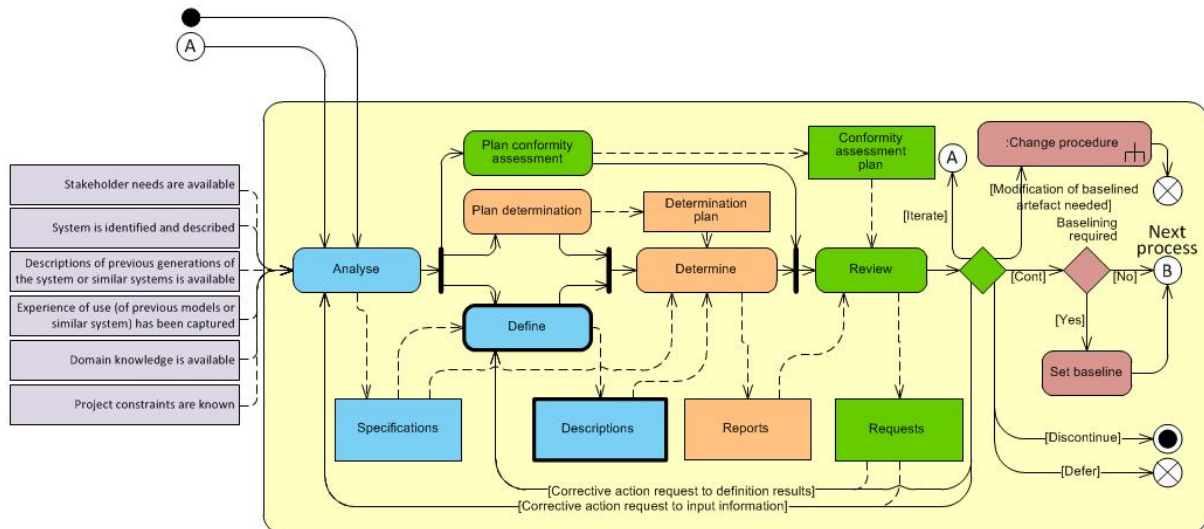


Figure 4. Example process; stakeholder requirements definition process.

Figure 4 illustrates the fact that the determination and conformity assessment activities (and the configuration management activities) are distributed into the technical processes; they do not constitute a stand-alone process. This fact has been discussed in more detailed by Alanen & Salminen (2016). Hence we conclude that qualification activities do not constitute a qualification process in accordance with the definition of *process*<sup>2</sup>; instead, a *Qualification process view*<sup>2</sup> is relevant, and we could include a new process, *Qualification management process*<sup>3</sup> similar to the one we defined for verification and validation management in (Alanen & Salminen 2016). Nevertheless, in this report we simply call the set of qualification activities a qualification process.

## 2.3 Basic statements

Based on the discussion in Section 2.1 and Section 2.2, we introduce a set of statements to elicit the mind-set of the authors. The statements are provided below:

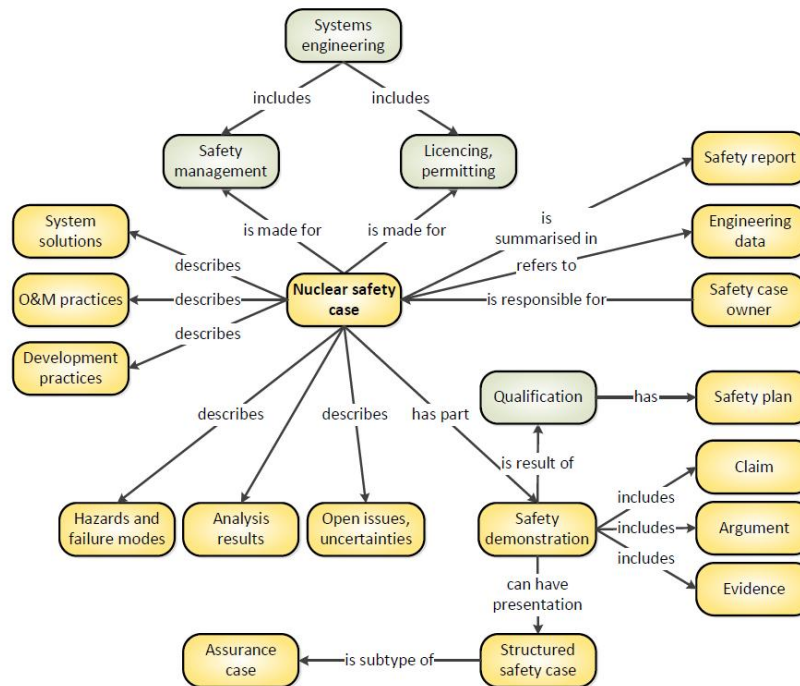
*Statement 1. In future, a structured, model based and database oriented<sup>4</sup>, design and conformity assessment environment that integrates and links engineering data and safety assurance information is the cornerstone of fluent and eloquent qualification engineering.*

<sup>2</sup> See definition of Process view in Section 1.2.

<sup>3</sup> Or, to be more general, *Compliance management*.

<sup>4</sup> XML is here considered to be 'database oriented'

*Statement 2. “Structured safety case” (a special case of assurance case), in nuclear power domain called “safety demonstration”, refers to a “formal”, basically hierarchical tree of model elements representing claims, arguments, evidences, justifications and assumptions. The term “safety case” also includes all the relevant background material of the system-under-qualification. See Figure 5.*



*Figure 5. Key concepts related to nuclear I&C architecture safety case. Work products (artefacts) are shown as yellow, processes are coloured light green. (Valkonen et al. 2016)*

*Statement 3. The goal is to adapt and simplify existing standards (ISO, OMG) and tools to the needs of the nuclear domain (in Finland) in order to make the approach understandable and allow its practical implementation (allowing model-based implementation of the assurance cases only while otherwise using traditional engineering data).*

*Statement 4. Evidence material (e.g. test results) is treated as independent artefacts that are only referenced. Online trace links and automatic change notifications (i.e. impact analysis support) are preferred, but in some cases external evidences (e.g. type approvals) have to be referenced.*

*Statement 5. Supporting elements used in an argument to determine the truth value of a claim can be a) basic evidences, b) assumptions, c) sub-claims with their own arguments and evidences or optionally d) “external assurance cases”, possibly represented as “assurance case modules” that can be subcontracted.*

*Statement 6. Claims and external assurance case modules can be allocated to their responsible owners.*

*Statement 7. An external (possibly subcontracted), foreign assurance case can also be treated as native evidence.*

*Statement 8. Stakeholder requirements are derived from relevant standards and regulations, regulatory expectations and other stakeholder needs and constraints. A qualification claim is always related to a stakeholder requirement of the particular regulator who calls for the qualification; if corresponding requirement does not exist, it shall be created if it is relevant. (Rationale: if the object-under-qualification is claimed to possess a property, but no one requires the property, the claim is needless. Furthermore, ISO/IEC 15026-4 (2012) states in its Section 7.9.2: “A set of critical properties should be determined by analysis of the complete set of requirements collected from the stakeholders...The project should prioritize properties in order to select which ones are the most critical for providing assurance claims.”) Nevertheless, in our data model we will allow orphan claims for convenience.*

*Statement 9. In Statement 8 we state that, in theory, there should be no orphan claims. Here we state that there should be no orphan requirements, i.e. requirements without claims. This includes both stakeholder requirements and system requirements. (Rationale: If there exists an accepted requirement that is not claimed to be fulfilled, or the claim is negative, the object-under-development is not ready for attestation; it is easy for the attestor to return the work back to the developing organisation by pointing out that requirements are not fulfilled, because not even the developing organisation has claimed that all the requirements are satisfied.)*

*Statement 10. The safety case shall include those requirements that are linked to the claims that are included in the assurance cases. Furthermore, the engineering artefacts (e.g. descriptions and models of system, sub-system, component, product, intended use and process [both system process and organisation process], as well as documentation and software or application) that are claimed to possess a property shall be included in the safety case. (Rationale: An integral safety case that includes a shot of the artefact versions that were prevailing in the instant of the qualification activity is necessary to support traceability with impact analysis.)*

*Statement 11. The assurance cases shall be planned during the requirements engineering work to define what kinds of evidences will be needed to fulfil the requirements, thereby providing input to design and V&V activities.*

*Statement 12. Top-level claims represent the general qualification strategy presented in qualification plan, lower-level claims typically correspond to lower level stakeholder and system requirements.*

*Statement 13. The schedule, participants, responsibilities etc. are described in a “traditional” or structured (model-based) qualification plan. The planned assurance case structure is included in the qualification plan.*

*Statement 14. During the project (during the design and V&V activities), actual evidences gradually become available and allow fixing of the truth values of the claims in a bottom-up up direction.*

*Statement 15. Issues may be raised leading to the need of better or new evidences or even changes in the system design.*

*Statement 16. When an evidence or claim is modified, the related upper-level claim becomes suspect; when a test or analysis result (used as an evidence) is modified, the evidence becomes suspect; when an artefact of the system-under-qualification is modified, the test and analysis results of the particular artefact become suspect; when a requirement that is allocated to an artefact of the system-under-qualification is modified, the particular artefact becomes suspect, and the claim that is linked to the modified requirement becomes suspect.*

*Statement 17. Qualification activities do not constitute a process. If the person responsible for all the qualification activities within an organisation wants to manage the qualification activities through a single entity, he or she should use the concept of process view. Nevertheless, we call the set of qualification activities a qualification process.*

These statements set the basis for our work presented in the following chapters.



### 3. Qualification process model

---

In this chapter, we try to crystallise what is the set of activities that is caused by the requirement to qualify an object; we state that only such activities constitute the qualification process. In Section 3.1 we discuss the key concept (qualification, certification, verification and validation). In Section 3.2 we present an example model of development process to point out, which activities belong to qualification process and which to other processes. In 3.3 and Appendix 1, we present how to implement a qualification process description in a model-based way.

#### 3.1 Description of the process under study

Qualification process is not included in the set of ISO/IEC/IEEE 15288 (2015) processes. Therefore, Alanen & Salminen (2016) introduced an additional process, *Qualification process*. The discussion in Section 2.2 of this report, however, points out that qualification activities do not constitute a stand-alone process, and a *Conformity assessment management* process should be introduced. But because qualification is defined e.g. by YVL E.7 as “...a process to demonstrate the ability to fulfil specified requirements (corresponds to the qualification process of the ISO 9000 standard)” and by ISO/IEC/IEEE 24765 (2010) as “the process of determining whether a system or component is suitable for operational use”, we call here the set of qualification activities a qualification process.

Valkonen et al. (2016) point out that qualification can be thought as a special case of validation (see definition in Section 1.2); in this report, we have elaborated this further in Section 2.2 and suggest that, verification and validation are special cases of conformity assessment, and qualification and certification are special cases of attestation. But, what is the practical difference between these four activity types? In the following indented paragraphs, we try to answer this question.

Qualification is characterised by the stakeholder whose requirements are in concern. Hence Valkonen et al. (2016) interprets Qualification in the context of nuclear I&C as follows: “*Qualification is the process to demonstrate to **the regulatory authority (or authorities)** that the requirements for a specific intended use or application have been fulfilled.*” (Boldfacing by the authors of this report.) If we apply the same interpretation to the process of validation, we may write: *Validation is the process to demonstrate **to the stakeholders** that the requirements for a specific intended use or application have been fulfilled.* Note that *Regulatory authority* is a subtype of *Stakeholder*. In this sense, qualification could be called a subtype of validation as Valkonen et al. (2016) do, but we do not do that in Figure 3, instead, we state that qualification is an additional activity to V&V activities to attest the V&V results.

Next we compare verification and validation. **Validation is carried out to assess conformity to the stakeholder requirements whereas verification is carried out to assess conformity to the system requirements.** System requirements are derived from the stakeholder requirements by the developing organisation. In principle, the stakeholder requirements are in the problem domain and the system requirements are in the solution domain (i.e. stakeholder requirements should be independent of a specific implementation technology), but very seldom the problem domain vs. solution domain distinction between the stakeholder and system requirements is clear. Nevertheless, the above distinction (stakeholder requirements vs. system requirements) between validation and verification is simple and clear. Verification is thus an internal activity of the developing organisation. The level of rigour of the verification activities in creating assurance cases is anticipated to be (much) lower than in case of validation activities. Implementation of the

tools used by the testing personnel or the internal assessors should provide an excellent user support to facilitate recording of thousands of verification claims.

The difference between the definitions of *Qualification* and *Certification* is not that clear although there is a practical difference between these two activities. Some definitions of qualification resemble the definition of certification. ISO/IEC/IEEE 24765 (2010) supplies three definitions for Certification:

1. a written guarantee that a system or component complies with its specified requirements and is acceptable for operational use
2. a formal demonstration that a system or component complies with its specified requirements and is acceptable for operational use
3. the process of confirming that a system or component complies with its specified requirements and is acceptable for operational use.

These all are very close to the interpretation of *Qualification* by Valkonen et al. (2016) (as presented above) and to the STUK definition of qualification (see Table 2 in Section 1.2). ISO 17000 (2004), however, defines *Certification* to be a “*third-party attestation related to products, processes, systems or persons*”. After reading the definition of *Attestation* in Table 2, we can conclude that *Certification* is distinguished from *Qualification* by the formalism and scope of the conformity assessment result: The certification process result (and the process itself) is more formal (a certificate) and more strictly regulated, and the result is more universal (certification makes the object-under-certification a general purpose component or sub-system in applications that can utilise the certificate). Certification is typically done for equipment or sub-systems, not for large systems; system qualification uses certificates as part of the evidence when claiming conformance of the equipment.

Most of the claims (at least the sub-claims), arguments and evidences needed for the qualification are created during the validation activities of the technical processes<sup>5</sup>. Hence, in principle, **the qualification process is assumed to only consist of the additional activities that are needed to demonstrate for the regulator that the object-under-qualification is suitable for operation.** The developer organisation has to anyway assure itself that the stakeholder requirements are satisfied, regardless of whether qualification is needed or not. This means that the V&V activities are always carried out by the licensee but the assessment of (some of the) V&V results happens only in projects with high level of rigour. Having said this, we notice that the assessment of the V&V results is the core activity of the qualification process. Thus we rephrase the boldfaced sentence as follows: **the qualification process is assumed to only consist of the additional activities to the V&V activities in high rigour projects to attest to the validity of the V&V results, which demonstrate that the object-under-qualification is suitable for operation.**

### 3.2 The resulted qualification process model

As discussed in Section 3.1, **the core activity of the qualification process is the assessment of the selected V&V results.** It is assumed here that each design artefact is verified and/or validated against the requirements the design artefact is stated to satisfy. Hence also the claims pre-exist (there is no sense in doing verification and validation without claiming conformance to the requirements). Therefore, in principle all the necessary claims,

---

<sup>5</sup> The cornerstone for reusing the validation results for qualification is a structured information model that is applied by all the technical processes, not only by conformity assessment (i.e. not only the C-A-E structure). This is discussed more in Chapter 4.

arguments and evidence pre-exist for the qualification. Nevertheless, we have to be prepared for additional validation activities initiated either by the licensee or the regulator during the qualification process. Besides selecting the existing V&V results there are other important qualification activities, such as management and planning of the qualification activities, evaluating the V&V results to be accepted for the safety case, presenting the safety case to the regulator, approving of the safety case and maintaining the safety case.

Figure 6 depicts an overview of the qualification activities among the activities of the management and technical processes. Each lane in Figure 6 represents an organisation role. Three organisation types are introduced, *Regulator*, *Licensee* and *Supplier*. The roles depicted in Figure 6 are described in Table 3.

The roles in Figure 6 and in Table 3 are only for reference; the actual set of roles varies a lot in the organisations.

Note also that instead of using the terms *Attest* and *Attestor* for the qualification activities as we did in Section 2.2. we use the terms *Assess qualification* and *Qualification assessor* (or *Inspector* at the regulator) to make the diagram easier to understand for those not familiar with the *Attest* term.

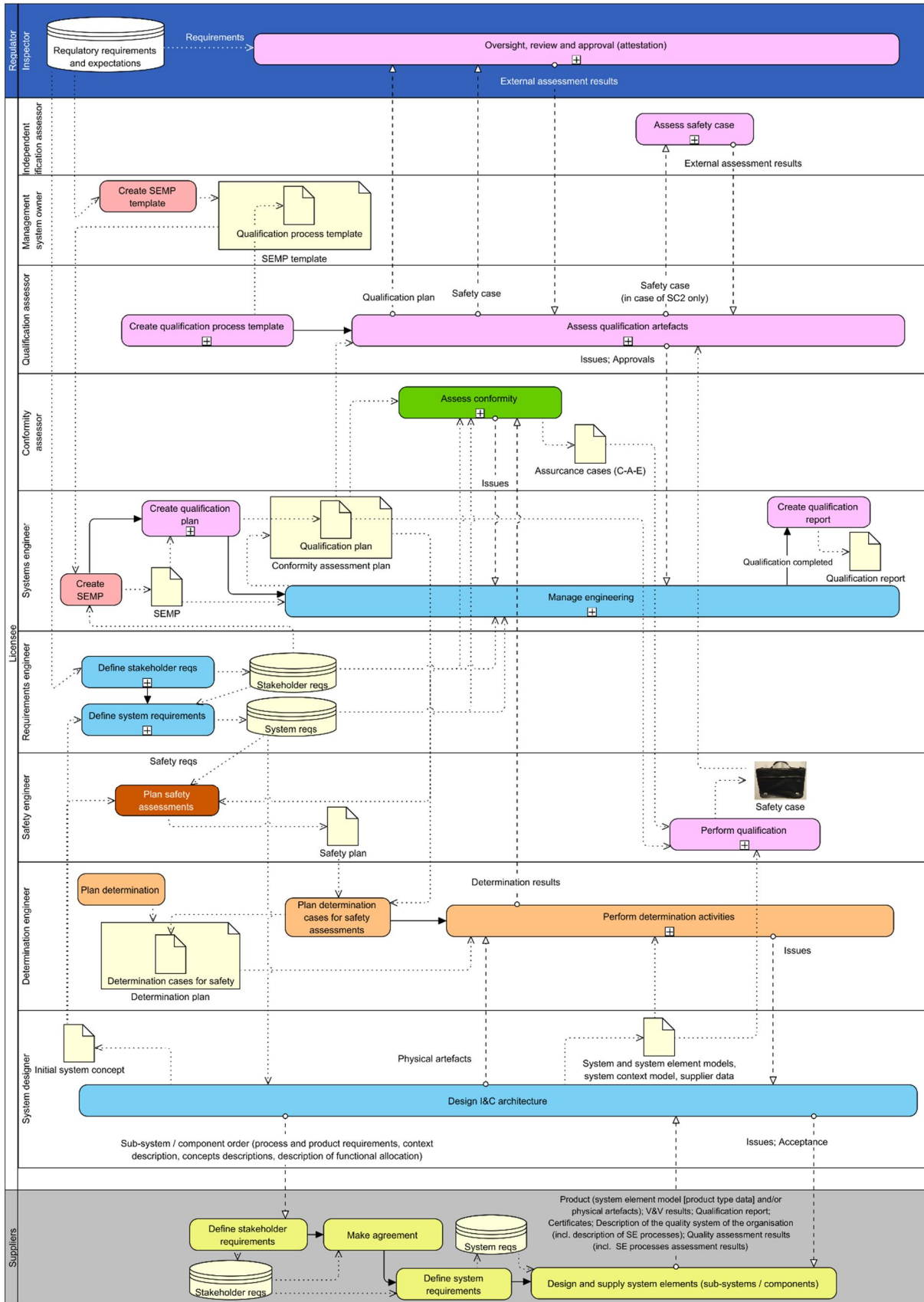


Figure 6. An overview of the qualification activities among the other activities of the management and technical processes. The figure only depicts the essential activities and information and sequence flows to support identification of the qualification activities and the related artefacts.

Table 3. Descriptions of the roles presented in Figure 6.

Role	Organisation	Description
<b>Inspector</b>	Regulator	the person (or persons) at the regulator who reviews the safety case (safety analysis report or suitability analysis) and provides feedback and the statement of the decision to the licensee; the regulator's contact person between the licensee and the regulator
<b>Independent qualification assessor</b>	Licensee or third party	an independent assessor for Safety Class 2 I&C equipment; may be internal or it may be external in cases where " <i>the electrical and I&amp;C systems and components and cables ...have a significant impact on nuclear safety</i> " (Citation from YVL E.7 [2013])
<b>Management system owner</b>	Licensee	the person who is responsible for the Management system and hence the overall Systems Engineering planning (is not carrying out SE planning of the actual projects, but provides the framework for the project SE planning)
<b>Qualification assessor</b>	Licensee	the person who is responsible for the qualification management and approval of the qualification results within the licensee. Is the licensee's contact person between the regulator and the licensee
<b>Conformity assessor</b>	Licensee	the person (or persons) who checks the determination results (tests, analysis, etc.) and their quality, and compares the results with the requirements and judges whether the object-under-assessment conforms to the requirements set for it
<b>Systems engineer</b>	Licensee	the person who orchestrates the system development including all the disciplines, such as mechanical, software and electrical engineering. Compared to Project manager, the Systems engineer is responsible for the properties of the system-of-interest, whereas the Project manager is responsible for the schedule and resources (budget, human resources, tools, facilities and services) for the work to achieve the properties. Systems engineer is a sub-contractor to the Project manager.
<b>Requirements engineer</b>	Licensee	the person who is responsible for the requirements engineering activities and their output artefacts, and for capture, analysis and formulation of input artefacts
<b>Safety engineer</b>	Licensee	the person (and his or her team) who is responsible for the management of the safety engineering activities to ensure the safety of the system.
<b>Determination engineer</b>	Licensee	traditionally called 'test engineer'; person who is responsible for carrying out the determination activities. The determination engineer can be, in big projects, the chief of the determination team or, in small projects, one of the testing persons
<b>System designer</b>	Licensee	the person (and his or her team) who is responsible for the design of the system
<b>Supplier personnel</b>	Supplier	all the persons at the supplier that participate in the project to supply the acquired product (component, equipment, design artefact, etc.)

Note that the roles in Table 3 are Systems Engineering (SE) roles, not organisation roles (see Figure 11 in Section 3.3). The idea is that the SE roles needed by the SE processes are fixed, while the organisation roles change frequently and vary a lot between different organisations. The project plan assigns an SE role to an organisation role and selects the person(s) with a corresponding organisation role to act in the assigned SE role to perform the related SE activities.

The story of Figure 6 goes as follows:

Most of the qualification requirements come from the *Regulatory requirements and expectations*. While creating the *Systems Engineering Management Plan (SEMP) template* the **Management system owner** creates the structure and placeholder for the *Qualification process template*, but the actual template is created by the **Qualification assessor**.

The **System designer** (or **System engineer**) starts the development work by creating the *Initial system concept*<sup>6</sup>. Thereafter the **Requirements engineer** *Defines the Stakeholder requirements* (which typically include both product and process requirements) derived from **Regulator**, customer, etc. documents and negotiations. The **Requirements engineer** analyses the *Stakeholder requirements*. Based on the analysis, the **Requirements engineer** *Defines the system requirements*, which are used by the **System designer** to *Design the I&C system*. Meanwhile, the **Determination engineer** creates the *Determination plan* (traditionally, Test plan), which includes, among other determination cases, the *Determination cases for safety*. These are defined by the **Determination engineer** (as depicted in Figure 6) or by the **Safety engineer** according to the *Safety plan* created by the **Safety engineer** according to the *Safety requirements*.

When a project for a certain I&C system is started, the **Systems engineer** creates the *SEMP* for the project. Thereafter, according to the *SEMP*, he or she creates the actual *Qualification plan* for the particular system (see Figure 8). The *Qualification plan* is part of the overall *Conformity assessment plan* (traditionally Validation plan) created by him or her (the activity is not depicted in the figure). The **Qualification assessor** assesses the *Qualification plan* (which is one of the *Qualification artefacts*). The **Qualification assessor** may require updates by raising *Issues*. After internal approval, the **Qualification assessor** sends the *Qualification plan* to the **Inspector** for information (Safety Class 3) or for approval (Safety Class 2). Again the **Qualification assessor** may return the *Qualification plan* to the **Systems engineer** for updates based on the feedback by the **Regulator**.

The system elements (*Sub-systems and Components, e.g. an I&C system or a smaller sub-system*) are ordered from the **Supplier**, which typically is external to the licensee. The system element alternatives can be Non-Developmental-Items (NDI), such as off-the-shelf standard components, or new designs (select or design). Figure 6 assumes that the system elements ordered by the **Licensee** are new designs in the sense that such an NDI is not available as a whole, although the ordered system element may be an integration of NDI components. If the **Licensee** acquires an NDI component directly off-the-shelf, its selection process is to be included in the *Design I&C architecture activity*. The information passed from the **Licensee** to the **Supplier** includes *list of the process and product requirements, context description, concepts descriptions and description of functional allocation*. The process requirements include requirements related to the **Supplier** organisation and its processes, especially quality management and quality assurance processes. Based on the requirements by the **Licensee** (that are *Stakeholder requirements to the*

---

<sup>6</sup> Initial system concept shall be available when requirements definition and qualification planning starts. It is impossible to start requirements definition and qualification planning if the requirements engineer and systems engineer does not know the target of the requirements and quality plan. The initial system concept shall in minimum include the title of the system and description of the added value the system should provide (i.e. its main functionality), but normally there is much more design data available (e.g. from previous system generations) when the actual requirements definition and qualification planning starts.

supplier), the **Supplier** defines the **System requirements** to be used by the **Supplier** organisation to *Design and supply the ordered system element*. The **Supplier** delivers the following information with the product: *System element model (product type data); V&V results; Qualification report; Certificates; Description of the quality system of the organisation (incl. description of SE processes); Quality assessment results (incl. SE processes assessment results)*.

As soon as the *Design artefacts* are ready for determination activities, such as testing and analysis, the **Determination engineer** (or his or her team) executes the *Determination cases*. The *Determination results* are brought to the **Conformity Assessor** who assesses them against the particular *System requirements*. The **Conformity Assessor** records his or her findings in the form of *Claim-Arguments-Evidence (C-A-E)* structure. This activity is performed regardless of whether regulated qualification is needed or not. Therefore, the colour of the activity object in Figure 6 is not pink.

When it is the time to deliver the qualification results to the **Regulator**, i.e. the *Safety case* (safety analysis report or suitability analysis), the **Safety engineer** *Performs qualification* (i.e. selects the safety related assurance cases<sup>7</sup> and assembles the *Safety case*, see Figure 9). Besides the C-A-E structured *Assurance cases*, a lot of other information is put to the *Safety case*, such as the system description (*System model* and *System element models*), system context description (*System context model*; may include domain model) and information about the supplier organisation and its quality system (*Supplier data*). The **Qualification assessor** assesses the *Safety case* (which is one the *Qualification artefacts*) (see Figure 10), and after possible update iterations, sends the *Safety case* to the **Regulator** for approval or for information<sup>8</sup>. The Regulator may raise issues, which cause an update round controlled by the *Systems engineer*.

In case of Safety Class 2 systems, there is an additional qualification phase before issuing the *Safety case* to the Regulator. The additional assessment is done by the **Independent qualification assessor**, which may be an independent organisation unit within the licensee or an independent external organisation. This assessment is also focused on the contents of the *Safety case*.

Safety case is considered in this context to be a generalisation of the I&C systems related qualification results, preliminary and final suitability analyses, and preliminary and final safety analysis reports (Figure 7).

---

<sup>7</sup> Safety related assurance cases can be called *Safety cases*; in Valkonen et al. [2016] they are called *Structured safety cases*. The problem with this phrasing is in the word 'case'. It can have two fundamental meanings, to denote a single item, such as a use case or a test case or an assurance case, that can be implemented e.g. as a single record or chain of related records in a database or as row or related rows in a spreadsheet; or, on the other hand, it can denote a briefcase that includes several documents, the main document and the attachments. In this report the latter denotation is used for *Safety case*. To emphasise that, the symbol for the *Safety case* in Figure 6 is a briefcase.

<sup>8</sup> Also in this case, feedback from the regulator can come, even refusal to approve, but the default is that the safety case is approved if no refusal is received in proper time, typically within two months.

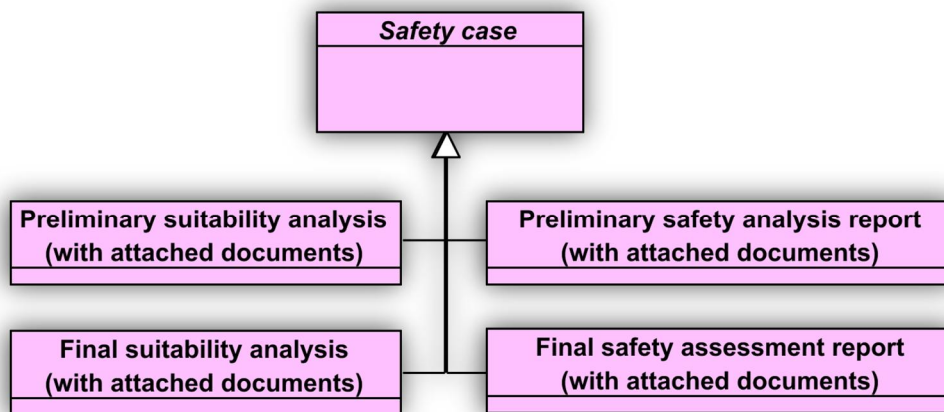


Figure 7. The four specialisations of Safety case in context of I&C systems (according to YVL E.7 [2013]).

Figure 6 does not use the term V&V (Verification and Validation), instead, we use the general term *Conformity assessment* and make a clear distinction between determination and conformity assessment as discussed in the sidebox on Page 10. The traditional interpretation of V&V is normally considered to be a combination of the Determination activities and the Conformity assessment activities.

From Figure 6 we can identify the following licensee qualification activities (the pink rounded rectangles):

- *Create qualification process template;*
- *Create qualification plan;*
- *Perform qualification;*
- *Assess qualification artefacts;*
- *Create qualification report.*

Besides the licensee activities, the regulator takes part in the qualification process. The supplier qualification activities (if such are performed) are not depicted in Figure 6. If the supplier performs qualification, it follows the model presented in Figure 6 such that the licensee is the 'regulator' to the supplier, and the supplier is the 'licensee'. In all cases, the supplier carries out V&V activities, the results of which are used by the licensee for qualification. For some of the sub-systems and components of the supplier, certification may be carried out. Hence the certification body is the 'external qualification assessor' (i.e. external attestor).

The first two activities in the list above could be grouped into an activity called *Prepare for qualification*, but we do not do that because the first two activities are only loosely coupled in the sense that the qualification process is done once for the company but the qualification plan is instantiated for each project<sup>9</sup>. Furthermore, the first activity, *Create qualification process template*, is a qualification management activity.

<sup>9</sup> Or, to be exact, for each sub-system under qualification. (The sub-systems can be developed in several parallel or consecutive projects.)



The qualification activities presented in Figure 6 consist of sub-activities, i.e. of *Tasks* (see the reference model in Figure 11). The internals of the core three qualification activities are presented in the figures below, *Create qualification plan* in Figure 8, *Perform qualification* in Figure 9, and *Assess qualification artefacts* in Figure 10. Note that the *Assess qualification artefacts* activity is a 'general purpose' activity in the sense that the activity works both for assessing the *Qualification plan* and the *Safety case*.

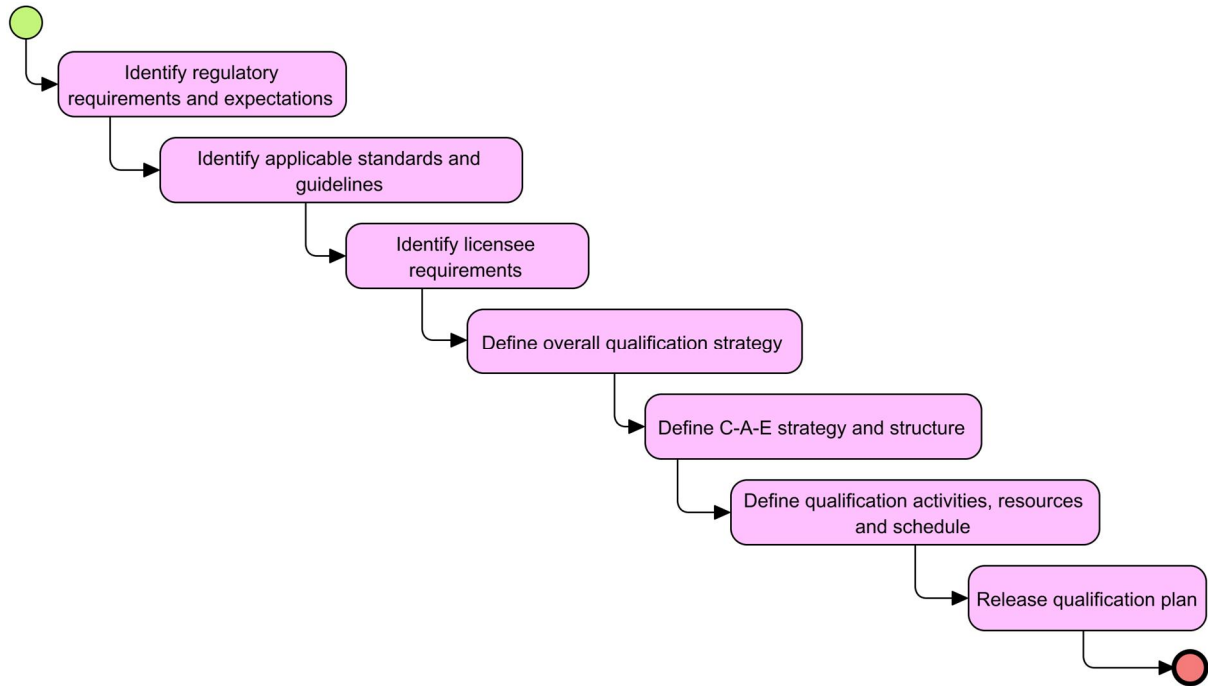


Figure 8. The procedure of the tasks within the activity *Create qualification plan*. (Developed from Valkonen et al. [2016]).

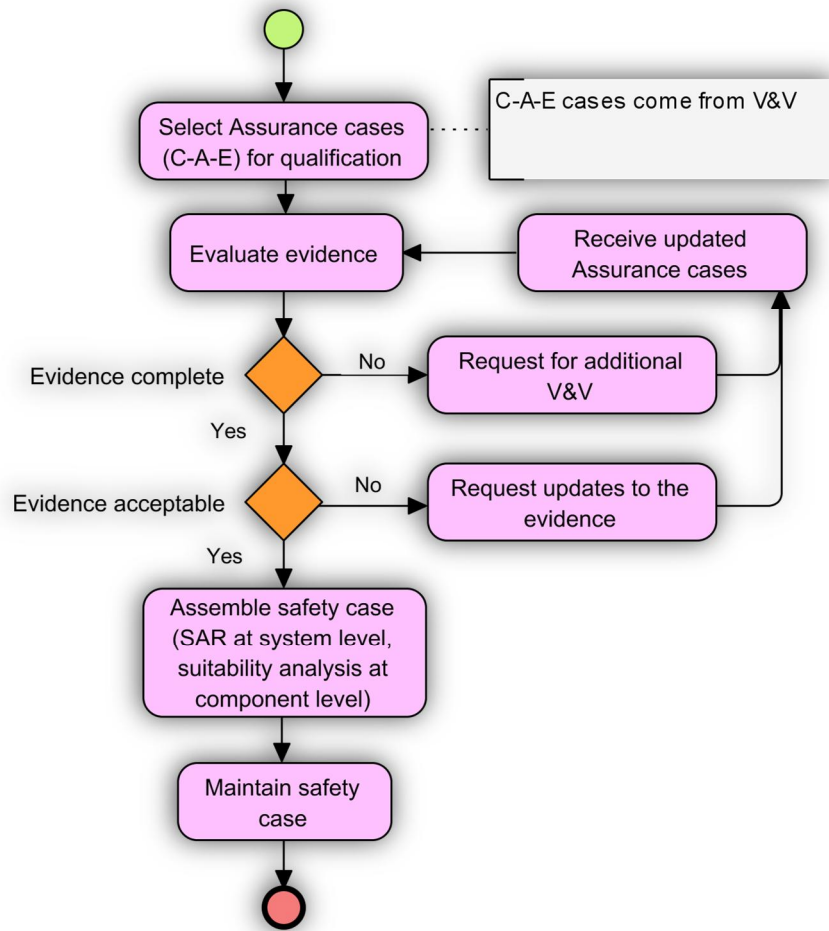


Figure 9. The procedure of the tasks within the activity Perform qualification. (Developed from Valkonen et al. [2016])

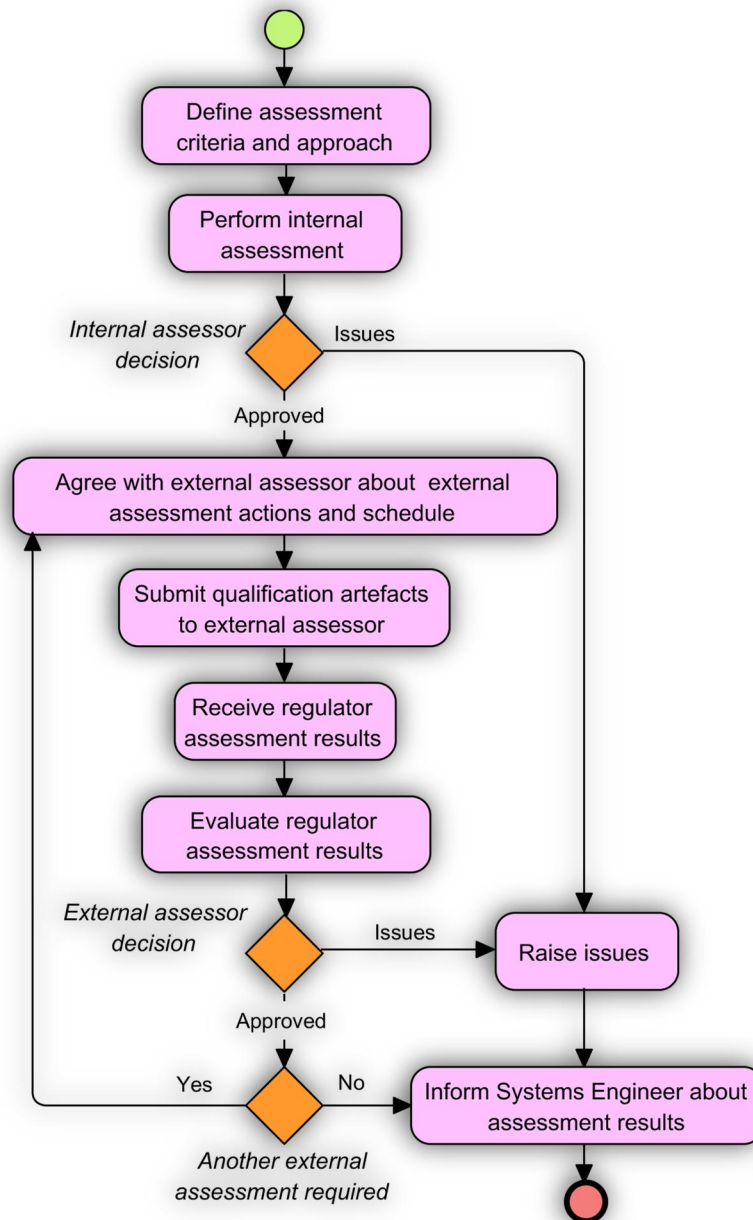


Figure 10. The procedure of the tasks within the activity Assess qualification artefacts. (Developed from Valkonen et al. [2016])

Now, we have created a reference model for the qualification activities that together constitute the qualification process (or qualification process view). In Chapter 4, we are going to develop a model for the main qualification process artefacts, i.e. the safety demonstration, which is the core of the *Safety case*. We will do it (as hinted in our activity model in Figure 6, on the *Conformity* assessor lane), by using the well-known Claim-Argument-Evidence structure for the assurance cases.

### 3.3 Method for describing the qualification process model

The qualification process model is described based on the enhanced process constructs model presented in the SAUNA SEMP report (Alanen & Salminen 2016). The process constructs model is re-depicted (with some modifications) in Figure 11. The process constructs model is the metamodel for the systems engineering process description. We do not create a separate metamodel for the qualification process, instead, we create a qualification process example, which works as a reference model for qualification processes. An example SharePoint implementation of the qualification process description using the *Enhanced process constructs model* presented in Figure 11 is provided in Appendix 1.

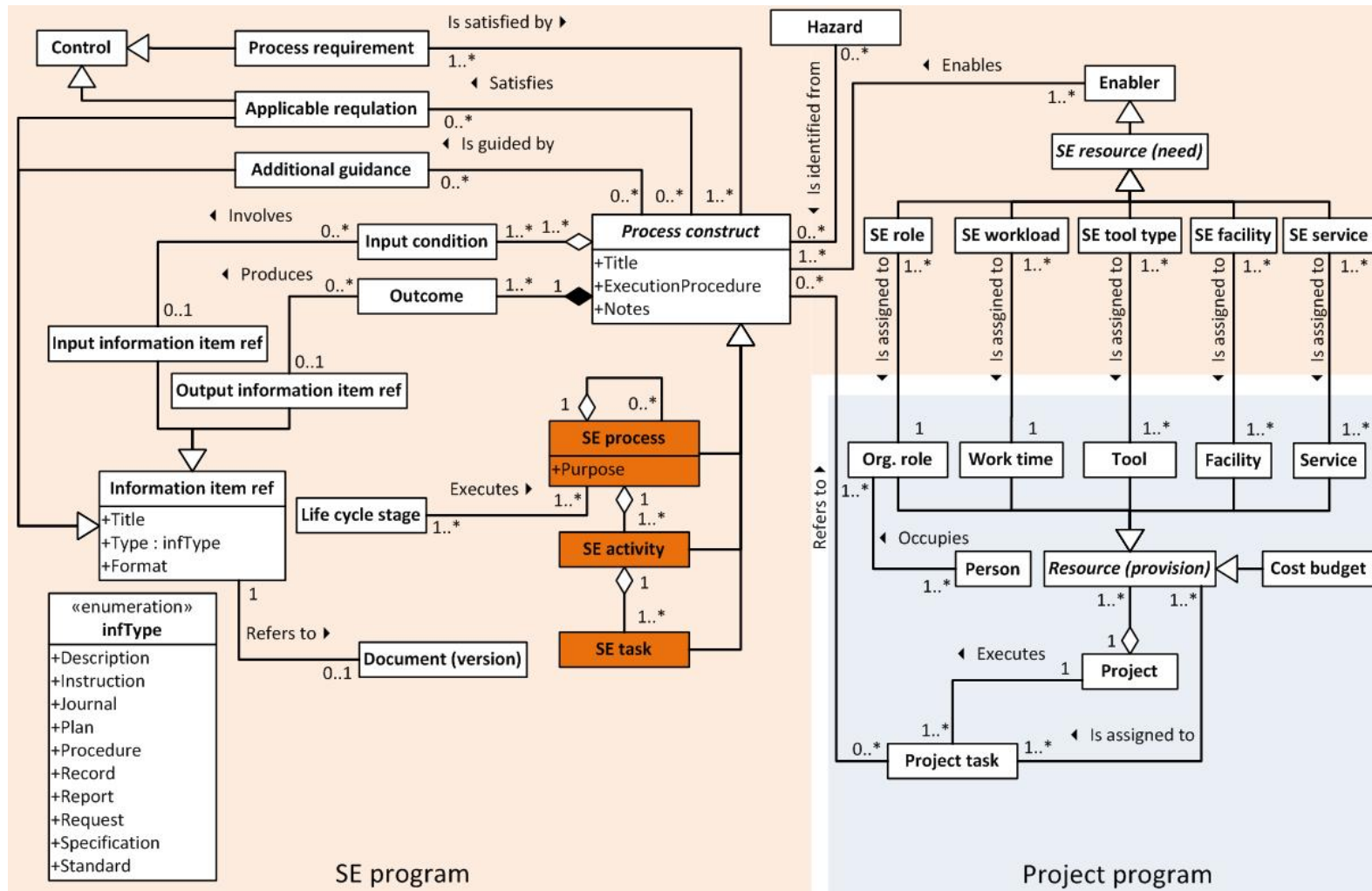


Figure 11. Enhanced process constructs model. Also the main project artefacts are added to illustrate the interface between the SE program and project program. (Modified from [Alanen & Salminen 2016].)

## 4. Safety demonstration data model

Safety demonstration is here a data package, not an activity. The core data in the safety demonstration are the safety related assurance cases, i.e. Claim-Argument-Evidence (C-A-E) structures. The most relevant reference models for assurance cases are ISO/IEC 15026-2 (2011) and SACM 2.0 (2015). These models are discussed shortly in Sections 4.1 and 4.2 respectively. In Section 4.3 we present our suggested data model for conformity assessment related artefacts; the model is demonstrated in Section 4.4. Finally, in Section 4.5, we discuss the possibility to automatically generate claim and argument sentences if the suggested data model is rigorously applied during the development process.

### 4.1 IEC/IEC 15026-2 C-A-E structure

ISO/IEC 15026-2 presents the assurance case structure both verbally and mathematically but not diagrammatically. In Figure 12 we try to translate the verbal presentation of ISO/IEC 15026-2 to UML class diagram notation.

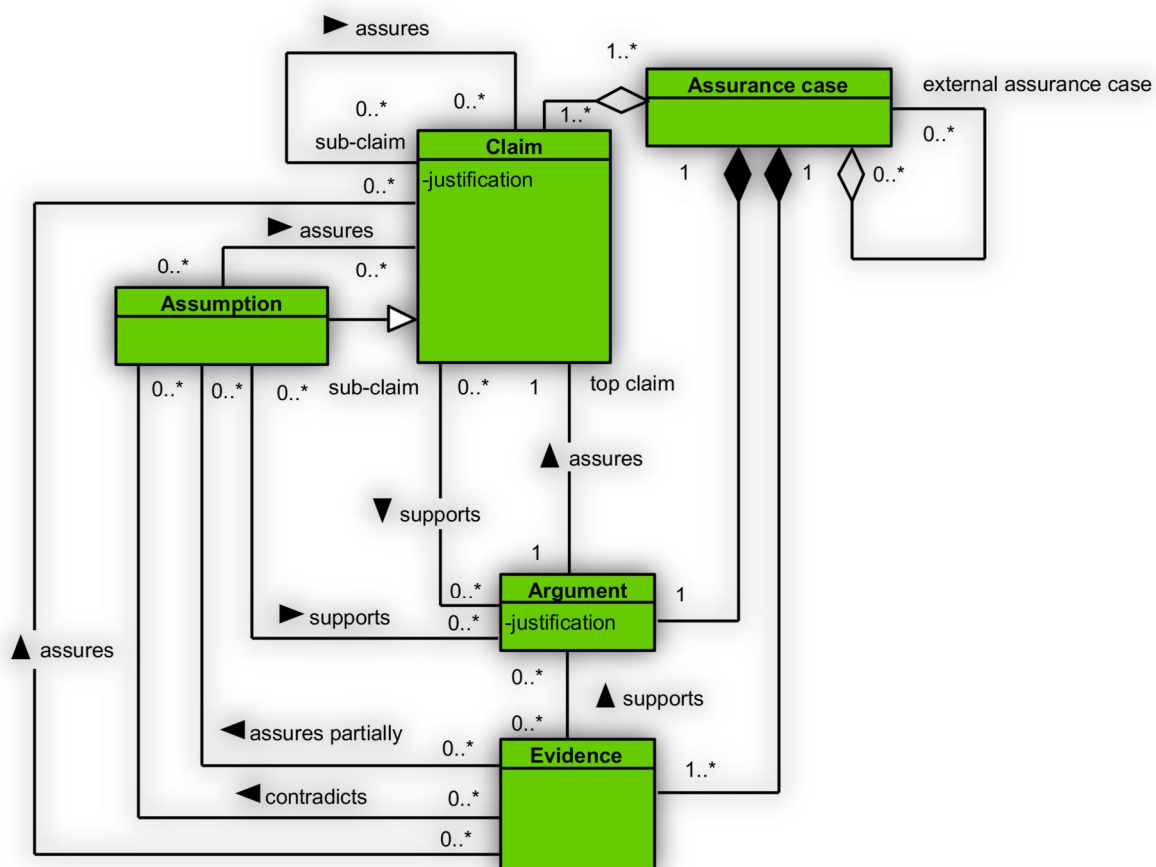


Figure 12. ISO/IEC 15026-2 assurance case structure in UML class diagram notation.

Compared to Figure 3, the model in Figure 12 does not include the relationship items of the assurance constructs into the assurance case. The omission of relationships is due to the fact that ISO/IEC 15026-2 does not explicitly include relationships into the assurance case. We do that in Figure 3 to emphasise the fact that in real implementations of the C-A-E structure, the relationships have a concrete manifestation. For example, in a database implementation, the relationships can be implemented using many-to-many relationship

tables. Such tables allow subsuming attributes into the relationships, such as rationale, creation/modification date and time, creator/modifier, and suspect flags. Suspect flagging is used to indicate changes at the artefacts linked by the relationship. Suspect flagging is done by the software tool with which the assurance cases are managed, not by persons. In fact, as discussed in Section 4.5, the contents of the claims, arguments and evidences might be possible to generate automatically after the relationships are defined, including the relationships to requirements and to the determination results (i.e. to test, analysis, etc. results). If such automatic generation works well<sup>10</sup>, the main job in creating the assurance cases is in setting up the relationships, and hence the relationships artefacts become the core content of the assurance cases.

## 4.2 SACM 2.0 C-A-E structure

The current formal version of Structured Assurance Case Metamodel (SACM) (in autumn 2016) is version 1.1, but a beta version of the upcoming SACM 2.0 is available at OMG (Object Management Group). The original SACM (1.0) was a result of combining two different specifications, Structured Assurance Evidence Metamodel (SAEM) and Argumentation Metamodel (ARG). Version 1.1 is a clean-up version from version 1.0. But version 2.0 is much more radical update to make the SACM cohesive and simpler. Version 2.0 also accommodates ideas from OPENCROSS Common Certification Language and the pattern metamodel and concepts from the OMG Structured Pattern Metamodel Standard (SPMS). The original goal of SACM 2.0 was to be more compliant with ISO 15026-2, but the specification does not state how well the compliance has been achieved. (OMG 2016)

The core contents of SACM 2.0 are the SACM Argumentation Metamodel and the SACM Artefact Metamodel. Together with the SACM Terminology Metamodel element, the elements of the two core metamodels are included to comprise assurance cases according to the SACM Package Metamodel. The base model elements for all of these are defined in the SACM Base Metamodel.

To grasp the essence of the SACM 2.0 metamodels, a stripped down version of the SACM 2.0 is depicted in Figure 13 such that only the core of the metamodels are shown; e.g. the following is excluded: asset and package citations to packages other than the current package, package bindings, package interfaces, the base elements metamodel and the terminology metamodel (except the main terminology package). The story of the model in Figure 13 goes as follows:

The *AssuranceCasePackage* consists of three packets, *TerminologyPackage*, *ArgumentPackage* and *ArtefactPackage*.

The *TerminologyPackage* defines the structure of the vocabulary (the internal structure of the package is not depicted in Figure 13).

The *ArgumentPackage* provides the *Claims* and their argumentation (*ArgumentReasoning*), the *ArtefactElementCitations* (*externalReferences* or relationships to *ArtefactElements*), and the relationships (*AssertedRelationships*) between *Claims* and *ArgumentReasoning*; the *AssertedRelationships* are considered assertions as well as the *Claims*. The following *AssertedRelationships* are supported, *AssertedEvidence* (e.g. between *Claim* and *ArtefactElementCitation* [e.g. to an evidence]), *AssertedCounterEvidence* (e.g. between *Claim* and *ArtefactElementCitation* [e.g. to a counter evidence]), *AssertedChallenge* (e.g. between two *Claims*), *AssertedInference* (e.g. between two *Claims*) and *AssertedContext* (e.g.

---

<sup>10</sup> This is a matter of further research.

between *Claim* and *ArtefactElementCitation* [to context information]). An *ArgumentPackage* can include lower level *ArgumentPackages*.

The *ArtefactPackage* provides any kind of work products (*Artefacts*) such as evidence and contextual information, but it also provides *ArtefactAssests* that are not work products, namely *Resource* (that provide physical access to *Artefacts*), *Activities* (the qualification process activities that use or produce the *Artefacts*), *Participants* (people, organisations and tools) and *Technique* (engineering techniques used e.g. in creation, inspection, review or analysis). An *Artefact* can be characterised in more detailed by *ArtefactProperties*, and its status changes can be recorded in *ArtefactEvents*. Both *ArtefactProperties* and *ArtefactEvents* are considered to be *ArtefactAssests* as well. Furthermore, the relationships (*ArtefactAssestRelationships*) between the *ArtefactAssets* are considered to be *ArtefactAssests*. There are several types of *ArtefactAssestRelationships*. (The relationship types are not depicted in Figure 13 to keep the diagram light.) The relationship types are *ArtefactRelationship* (between *Artefacts* or their *ArtefactAssetCitations*), *ActivityRelationship* (between *Activities* or their *ArtefactAssetCitations*), *ArtefactActivityRelationShip* (between *Artefacts* and *Activities* or their *ArtefactAssetCitations*), *ArtefactTechniqueRelationship* (between *Artefacts* and *Techniques* or their *ArtefactAssetCitations*), *ParticipantRoleRelationShip* (between *Participants* or their *ArtefactAssetCitations* and any other *ArtefactAsset*) and *ArtefactResourceRelationship* (between *Artefacts* and *Resources* or their *ArtefactAssetCitations*). (The *ArtefactAssestCitation* is also an *ArtefactAsset*, but this is not depicted in Figure 13.)

The SACM 2.0 metamodel is very clear compared to the earlier version of 1.1, and is thus expected to be implemented into various assurance case tools, but the metamodel may also be implementable by any database oriented<sup>11</sup> repository management tool.

---

<sup>11</sup> See Footnote 4.



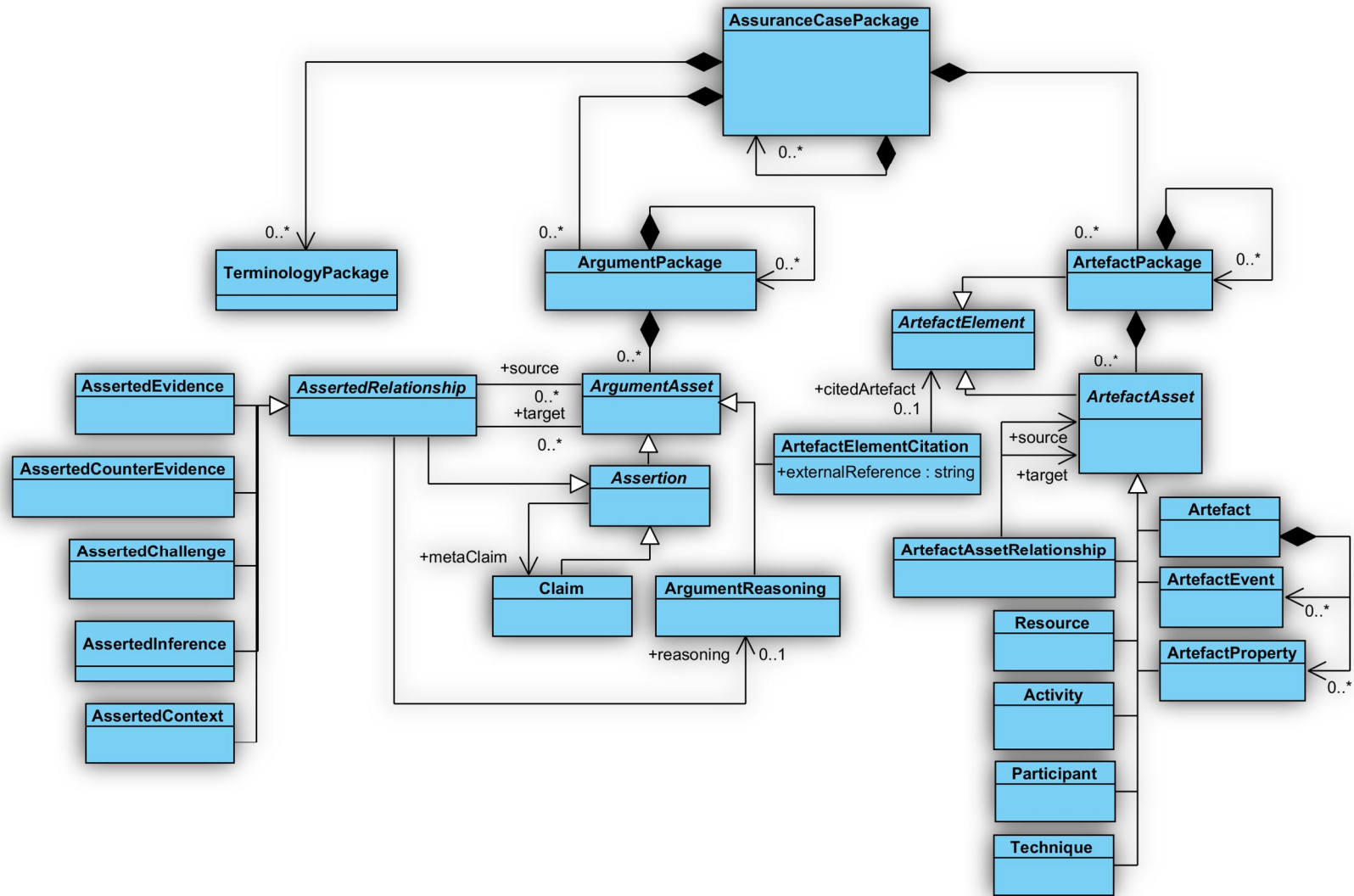


Figure 13. A stripped down reproduction of SACM metamodels. (Do not use this when applying SACM 2.0; use the original model instead.)

### 4.3 Suggested data model

Our suggested data model, presented in Figure 15, is a synthesis of the data model in Figure 3, of ISO/IEC 15026-2 presented in Figure 12 and of the Requirements and V&V artefacts model of SEAModel<sub>NPP</sub> presented by Tommila & Alanen (2015). It also has a good analogy with the SACM 2.0 model; for example, if *ArgumentElementCitation* of SACM 2.0 (see Figure 13) is rephrased *Evidence* according to our model and if the reader notices that the *ArgumentReasoning* of SACM 2.0 is enclosed into *Claim* in our model as an attribute (*argument*)<sup>12</sup>, the analogy is evident.

The objective of the synthesis has been simplicity to facilitate a short step migration from document centric development, determination (test, analysis, etc.) and conformity assessment to model-based systems engineering. Another objective has been to provide a model that can be implemented with database oriented software tools. The ultimate motivation, however, is to provide a systematic model for the development, determination and conformity artefacts such that the safety of the object-under-study is assured in a very accurate manner.

Before presenting the detailed data model, we provide in Figure 14 an overview of the core systems engineering work that is carried out regardless of the way in which the engineering data is managed.

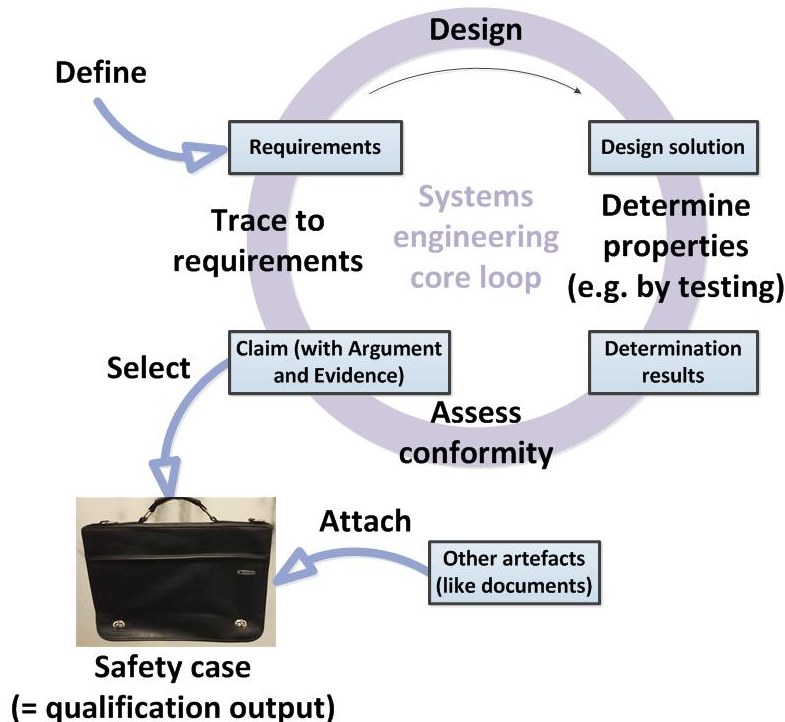


Figure 14. Systems engineering core loop.

The class diagram presented in Figure 15 provides a detailed model of the artefacts within the systems engineering core loop of Figure 14.

<sup>12</sup> The argument is not presented as an independent model element because we define that a claim has only one argument and an argument is related to only one claim, i.e. the relationship is one-to-one relationship. Furthermore, the lifecycle of the claim and argument is considered to be concurrent. The motivation for not making independent model elements is in making the model and its implementation as simple as possible. Nevertheless, if needed, the argument can be separated from claim.

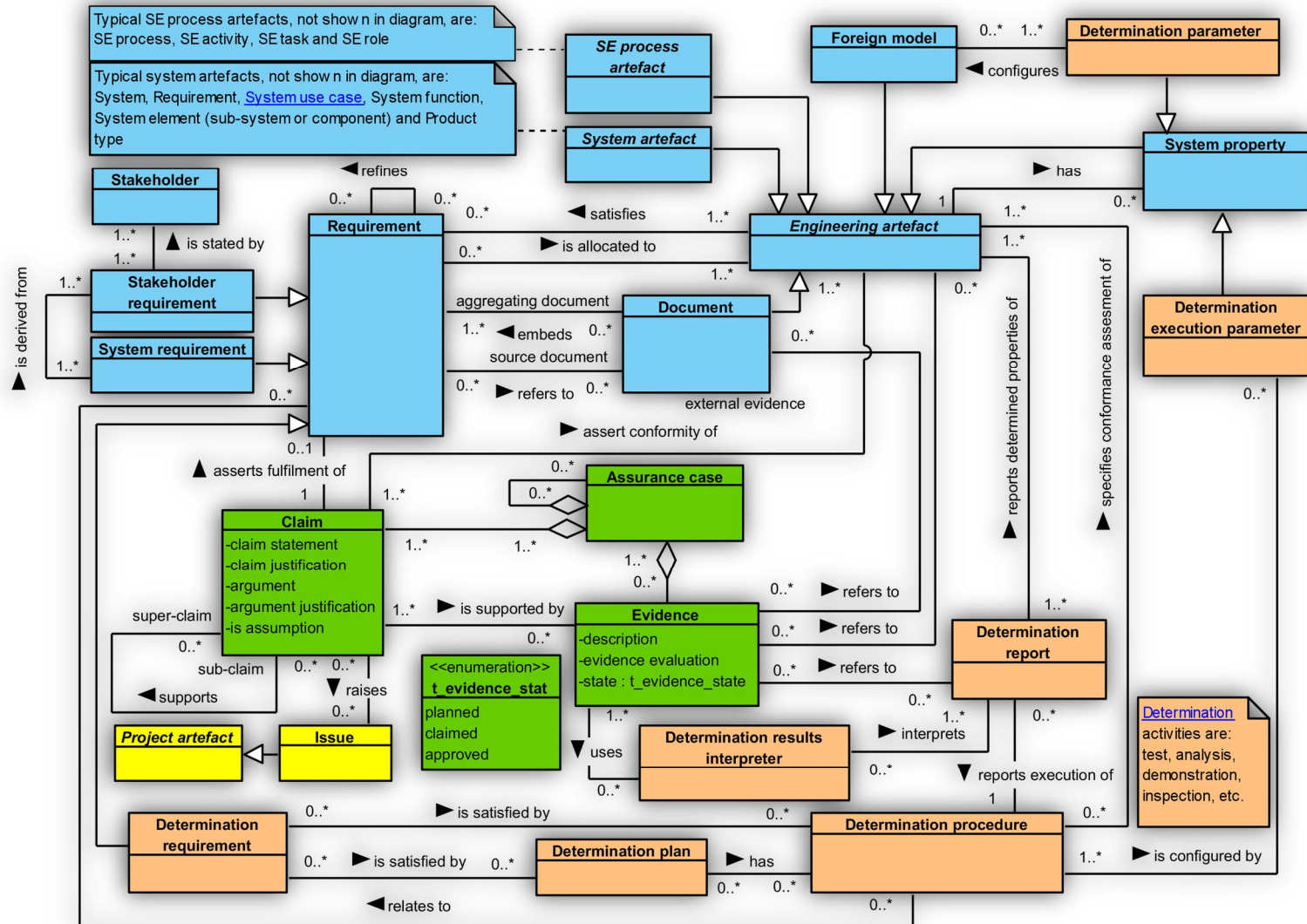


Figure 15. Our suggested data model for the main development artefacts, determination artefacts and conformity artefacts.

The story of Figure 15 goes as follows:

The *Stakeholders* set *Stakeholder requirements*. The *System requirements* are derived from the *Stakeholder requirements*. The *Requirements* are refined by child *Requirements*. The engineers start to create their work items, i.e. *Engineering artefacts*, such as *System use cases*, *System functions*, *System elements* (and their physical implementations, *Product types*). The *system requirements* are allocated to *Engineering artefacts*. The *Properties* of the *Engineering artefacts* shall satisfy the *System requirements* and thus finally the *Stakeholder requirements*. When the set of *System properties* of an *Engineering artefact* satisfy all the *Requirements*, the *Engineering artefact* can be claimed to satisfy its requirements.

To verify or validate the created *Engineering artefacts*, their *System properties* are determined according to *Determination procedures*, which are planned in the *Determination plan*. The results of the *Determination procedures* are reported in *Determination reports*. For some of the *Determination reports*, an additional tool, *Determination results interpreter*, may be needed to interpret the results or to reproduce the results. Unexpected determination results, reported in *Determination reports*, may raise *Issues*. Some of the *Determination procedures* may involve using *Foreign models*, such as simulation models. The *Determination procedures* set the appropriate *Determination parameters*, such as simulation model parameters. The *Determination procedures* also set *Determination execution parameters*, such as the number of simulation runs.

The *Requirements* for an *Engineering artefact* are *Claimed* to be satisfied based on the *Evidence*, which may refer to the *Determination reports*, some relevant external *Documents* or any *Engineering artefact* relevant as an evidence (e.g. existence of a certain *System element*, such as an emergency stop switch, can be used as an evidence). The *Evidence* element is thus only a reference; it does not contain the actual evidence. Nevertheless, it has got attributes of its own, such as *evidence evaluation* to store the results of *Evaluate evidence* task presented in Figure 9. The attribute *evidence evaluation* cannot be directly put to the *Determination reports* to qualify the determination results to be used as an evidence due to the fact that a *Determination report* may work well as an evidence to one claim but not for another claim.

The data model in Figure 15 to produce C-A-E cases does not depict a separate *Relationship* artefact as was depicted in Figure 3 and in the SACM 2.0 metamodel (see Figure 13). The reason for this is that the *Relationship* artefact is depicted in a complementing diagram of the SEAModel as shown by Tommila & Alanen (2015; Figure 47). Nevertheless, the *Relationships* are highly relevant due to the fact that they provide the traceability links. With a proper software tool, it is possible to arrange impact analysis to mark the relevant *Claims* suspect if the *Requirement* claimed to be satisfied, the *Evidence* or the *Engineering artefact* under assurance changes.

Using the data model in Figure 15 requires that the requirements structure and hierarchy is well planned, because the claim structure precisely follows the requirements structure. However, as stated in Statement 8 in Section 2.3, the data model allows orphan claims for convenience to support flexibility in claim structure.

Figure 15 does not incorporate the risk assessment artefacts; the reader is advised to consult the *Risk assessment artefacts model* by Tommila & Alanen (2015; Section 9.6.1) to complement Figure 15 with the risk assessment model of the SEAModel. Risk assessment activities can be considered as determination activities, i.e. to determine the hazard properties of the object-under-development.

Such data models can be implemented by various database oriented<sup>13</sup> software tools; consult Alanen et al. (2015; Sections 4 and 5) about some suggestions for an implementation platform. See also a practical implementation in Tommila & Alanen (2015; Section 10.1) of a similar traceability model.

#### 4.4 A case example using the suggested data model

As a case example, we consider an I&C system that applies a *Synchro transducer*. We take one environmental requirement, *Dry heat temperature*, as an example requirement, the route of which we will follow, according to our data model presented in Figure 15, up till the conformity assessment. The case example is presented in Figure 16.

Note that the **case example provides the supplier view** to produce well-formed assurance cases into the qualification report of the supplier, which is then used by the licensee in its safety case (suitability analysis or safety analysis report). The licensee case, however, would be very similar. This will be discussed briefly in the end of this section.

In Figure 16, there are some relations not presented in the data model in Figure 15. Such relations are the relation (*refers to*) between *Determination procedure* and *Document*, the relation (*describes*) between *Product type* and *Document* (datasheet), and the relation (*imports*) between *Product property* and *Document* (datasheet). These are relations are presented in Tommila & Alanen (2015) (relation *describes* presented there as its reciprocal, *is described by*).

---

<sup>13</sup> See footnote 4.

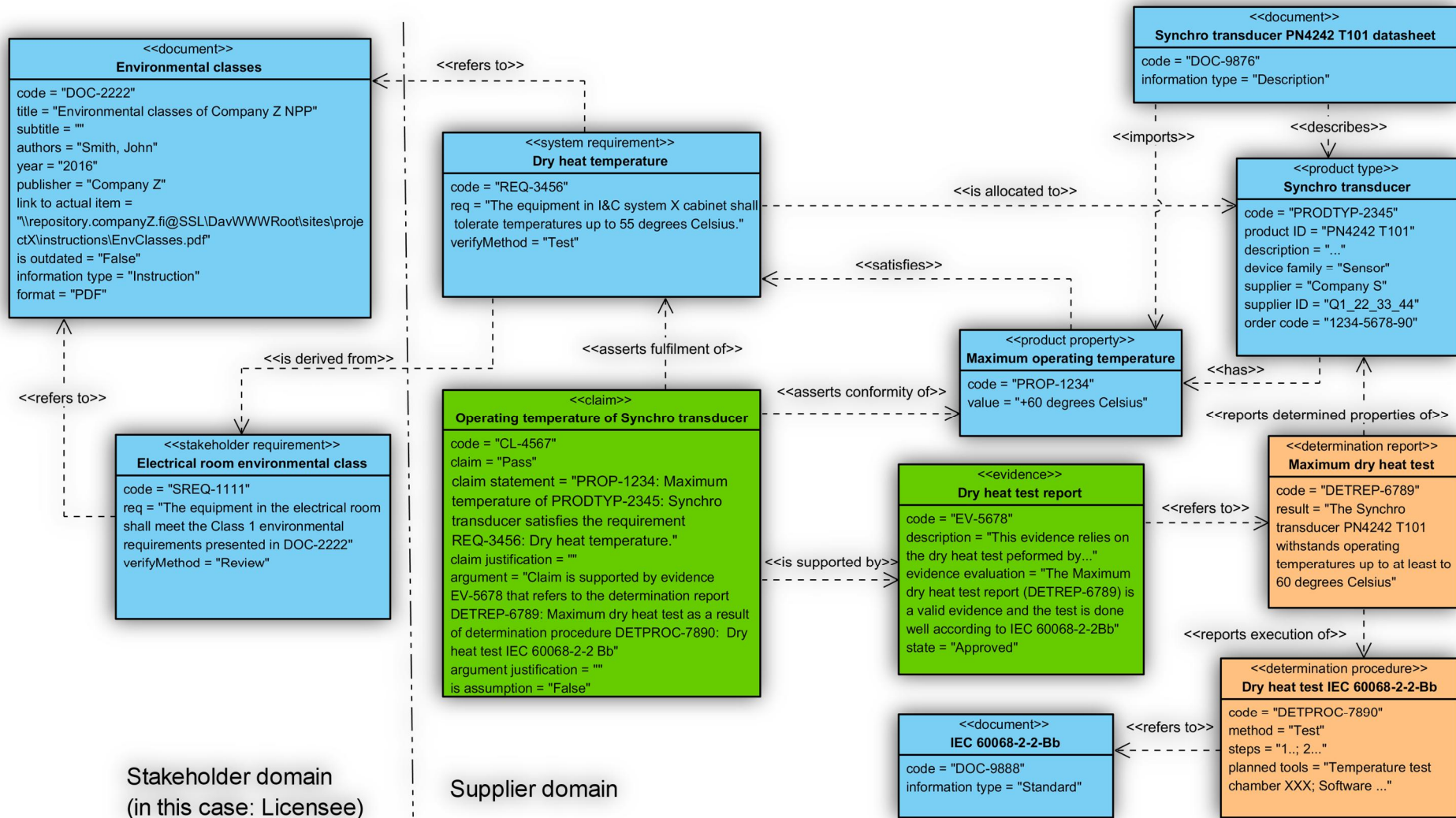


Figure 16. Case example for a single requirement of a synchro transducer; the supplier view.

The story of the case example in Figure 16 goes as follows:

The *Stakeholder* (here: licensee, Company Z) orders *I&C System X* from a *Supplier* (Company S).

The stakeholder defines the *Stakeholder requirements*, such as environmental requirements, for the *I&C System X*. The environmental requirements for the I&C system are categorised into several classes. For example, *the equipment in electrical room shall meet Class 1 requirements (SREQ-1111)*. To resolve the Class 1 specifications, a document '*Environmental classes of Company Z NPP*' is referred to through *Document object DOC-2222*.

One of the components of the I&C System X, is a *Synchro transducer*. From the stakeholder requirement (*SREQ-1111: Environmental class*) the supplier derives a *System requirement* concerning the maximum dry heat temperature: *REQ-3456: Dry heat temperature: The equipment in I&C system X cabinet shall tolerate temperatures up to 55 °C*<sup>14</sup>. It is *allocated*, among others, to the *Synchro transducer (PRODTYP-2345)*. One of the properties of the *Synchro transducer* is its *Maximum operating temperature (PROP-1234)*. The designers claim that the *Synchro transducer* tolerates 60 °C, but the actual value of the property is determined by carrying out a *Determination procedure (DETPROC-7890)*, which is a test according to IEC 60068-2-2 Bb (a standard, which is referred to through *Document object DOC-9888*). The result of the *Determination procedure* is reported in a *Determination report (DETREP-6789)*; the result is that the *Synchro transducer* tolerates 60 °C. A datasheet, *DOC-9876: Synchro transducer PN4242 T101 datasheet*, is created to describe the *Synchro transducer*. The datasheet *imports* (either manually or, preferably, through a database query) the *Maximum operating temperature property (PROP-1234)*.

Now it is the time for the conformance assessor to assess whether the *Synchro transducer* conforms to its *Dry heat temperature (REQ-3456)* requirement or not. He or she claims that it does, because there is a valid evidence, the *Determination report (DETREP-6789)*. To use the *Determination report* as an evidence to refer to, he or she creates an *Evidence object Dry heat test report (EV-5678)* to refer to the *Determination report*. Furthermore, the conformance assessor evaluates the *Determination report* to ensure about its adequacy and quality, and the assessor records the result of the evaluation into the *Evidence object (EV-5678)*. The conformance assessor completes the *Claim (CL-4567)* by writing the *claim statement, claim justification, argument and argument justification*.

As a result, we have an assurance case that, in principle, consists of only the *Claim* (including its *Argument*) and *Evidence*, but in practice, nearly all of the artefacts depicted in the supplier domain in Figure 16. Case example for a single requirement of a synchro transducer; the supplier view. are relevant for the *Qualification assessor* and *Inspector* to assess the completeness and quality of the assurance cases. Hence it is suggested that, in the future, the Safety case (at least its *Assurance cases*) are presented by a software tool using the data model, not as a document or set of documents. Such a tool can provide visual traceability features and impact analysis.

---

<sup>14</sup> REQ-3456 is also traced to the source of the temperature value, i.e. DOC-2222, because a change in the value is not reflected as a change in SREQ-1111 due to the fact that requirement text in SREQ-1111 will not change even though the values in DOC-2222 change, and hence suspect flagging will not propagate to REQ-3456 without the direct trace to DOC-2222.

Traceability is provided by the trace links shown in Figure 16. Implementation of a trace link is a record (or similar) in a database with attributes of its own, such as *suspect in*, *suspect out*, *rationale*, *modifier* and *modification date*. The first two are maintained by the software to indicate that the traced item has been changed; the next one, *rationale*, is edited by the person who creates the links; the last two are updated by the software tool. With such an arrangement, traceability, impact analysis and knowledge about the persons and dates is superior over the traditional document centric qualification engineering. This benefits the safety of the system-under-development.

For the licensee, the process is the same. For example, when claiming suitability of the *Synchro transducer* the licensee has the dry heat temperature requirement in its database; the requirement is allocated to the particular *Synchro transducer*; the properties of the *Synchro transducer* are determined by reviewing the datasheet and the supplier assurance case or, as preferred, the whole chain of artefacts depicted in Figure 16. But the licensee can also perform an additional test according to IEC 60068-2-2 Bb if needed. In that case, there are three evidences, datasheet, supplier assurance case and the licensee test report.

#### 4.5 Automatic generation of claim and argument sentences

The model in Figure 16 can be used to create structured claims, such as:

*Code: CL-4567;*

*Title: **Operating temperature of Synchro transducer;***

*Claim: “**PROP-1234: Maximum operating temperature of PRODTYP-2345: Synchro transducer satisfies the requirement REQ-3456: Dry heat temperature.**”*

And it can be used to create structured argumentation sentences, such as:

*“**Claim (CL-4567: Operating temperature of Synchro transducer satisfies its requirements)** is supported by evidence **EV-5678** that refers to the determination report **DETREP-6789: Maximum dry heat test** as a result of **determination procedure DETPROC-7890: Dry heat test IEC 60068-2-2 Bb.**”*

The bold-faced texts can be retrieved from the engineering database, the pieces of glue text come from a claim or argument template respectively.

This type of sentences may sound futile as such due to the fact that they do not include all the actual information, such as the property values, but only references to that information; in fact, the sentences are futile on paper, but in electronic format (such as hypertext or hint texts when cursor is hovered over the reference) the sentences become live and sensible.

Such a structured (model-based) way of storing information opens thus the way for automatic generation of claim and argument sentences, provided that the engineers record the information to the correct model elements and then link the model elements according to the data model presented in Figure 15. This diminishes the amount of storytelling by engineers and makes the claims and arguments more coherent. The reasoning above points out the potential of model-based systems engineering over traditional document centric engineering.

Note also that the data model can be used to manually create well-formed determination requirements, such as:

*“Conformity assessment of **PROP-1234: Maximum operating temperature of SYSEL-2345: Synchro transducer** for the purpose of **Validation** shall be supported by determination through **Testing** according to IEC 60068-2-2 Bb.”*



The *Determination requirement* nor the *Determination plan* is not depicted in Figure 16 to make the message of example easier to comprehend.

The discussion and the sentence examples above point out the potential of the automatic generation of claim and argument sentences for simple cases, such as the case model in Figure 16. It is a matter of more comprehensive and real life demonstration to study feasibility of automatic generation of claim and argument sentences in more complex cases.

## 5. Summary and conclusions

---

In this report, we have discussed the basic terms and concepts relating to the qualification process of I&C systems, their equipment and components in nuclear power plants. We have done that to make it clear, what activities belong to the qualification process and what activities belong to other processes, such as V&V processes. We have presented a qualification process example and a safety demonstration data metamodel, which we suggest to be used in qualification of I&C systems, equipment and components. We also have demonstrated the applicability of the safety demonstration data metamodel with a simple case example.

Applying model-based engineering in the way presented in this report helps assuring the safety of complex systems, such as the I&C systems of nuclear power plants, due to the fact that the engineering and conformity assessment effort can be managed more systematically. The systematic process and data models help identify gaps in fulfilling the process and product safety requirement. Identification of gaps can be arranged to be performed by a software tool, for example by identifying requirements that do not have a corresponding claim, by identifying arguments without evidence and by identifying determination results that are not used as evidence (perhaps to hide negative test results).

Kelly (2008) warns about typical safety case traps, where the safety cases do not bring added value to the safety or to the safety assurance costs. The lessons learned from the traps reported by Kelly can be summarised as follows: Produce the safety case to improve safety, not to produce overwhelming amount of text documents with beautiful claim-argument-evidence diagrams that try to hide from unskilled assessors the truth that the design needs to be updated to fulfil the safety requirements.

The model-based scheme, we have studied in this report, to produce and manage safety demonstration help avoid the safety case traps due to the fact that the time is not spent in storytelling, but in creating a well-structured requirements and engineering database according to a data model such as the one presented in Chapter 4.

An interesting subject for further research and demonstration is automatic generation of claims and arguments provided that:

- the trace links are set correctly according to the chosen data model;
- the requirements that specify the critical properties to be claimed are marked in the requirements database;
- the structure of the requirements is done well such that the claim structure can directly follow the requirements structure.

Automatic generation of claims and arguments was discussed in Section 4.5.

The next step to increase the readiness level of the model-based qualification process would be to make a demonstration using a real case of an I&C system of a nuclear facility to study the feasibility and potential of our model to automatically create Claim-Argument-Evidence reports.

## References

---

- Alanen, J., Isto, P., Tommila, T. & Tikka, P. 2015. Requirements traceability in simulation driven development. Espoo: VTT. VTT Technology: 236. 81 p. + app. 30 p.
- Alanen, J. & Salminen K. 2016. Systems Engineering Management Plan template - V1. Espoo: VTT. VTT Research Report: VTT-R-00153-16. 78 p. + app. 12 p.
- Common position 2014. Licensing of safety critical software for nuclear reactors – Common position of international nuclear regulators and authorised technical support organisations. Revision 2014.
- IAEA. 2010. Licensing Process for Nuclear Installations. Specific Safety Guide No. SSG-12, 80 p.
- INCOSE 2007. Systems Engineering Handbook – A Guide for system life cycle processes and activities. Seattle: International Council on Systems Engineering (INCOSE). INCOSE-TP-2003-002-03.1
- IEC 61513. 2011. Nuclear power plants - Instrumentation and control important to safety - General requirements for systems. Geneva: International Electrotechnical Commission (IEC). 205 p.
- 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 15026-2. 2011. Systems and software engineering – Systems and software assurance – Part 2: Assurance case. Geneva: International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC). 10 p.
- ISO/IEC 15026-4. 2012. Systems and software engineering – Systems and software assurance – Part 4: Assurance in the life cycle. Geneva: International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC). 10 p
- ISO/IEC/IEEE 24765. 2010. Systems and software engineering – Vocabulary. Geneva: International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) and New York: Institute of Electrical and Electronics Engineers (IEEE). 410 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 24765. 2010. Systems and software engineering – Vocabulary. Geneva: International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) and New York: Institute of Electrical and Electronics Engineers (IEEE). 410 p.
- Kelly, T. 2008. Are 'Safety Cases' Working? Safety Critical Systems Club Newsletter, Volume 17, No. 2, January 2008, pages 31-3
- OMG. 2016. Structured Assurance Case Metamodel (SACM), version 2.0 (draft, Beta1). Object Management Group (OMG), 41 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.
- Valkonen, J., Tommila, T., Linnosmaa, J. & Varkoi, T. 2016. Safety demonstration of nuclear I&C - an introduction. SAUNA Task 3.1 report. Espoo: VTT. VTT Research Report: VTT-R-00167-16. 34 p. + app. 4p.
- YVL B.1. 2013. Safety design of a nuclear power plant. The Radiation and Nuclear Safety Authority (STUK), 15 November 2013, 46 p.
- YVL E.7. 2013. Electrical and I&C equipment of a nuclear facility. The Radiation and Nuclear Safety Authority (STUK), 15 November 2013, 34 p.

## **Appendix 1. Quality process template (draft)**

---

In this appendix, we present a draft implementation of quality process template that follows the enhanced process constructs model presented in Section 3.3. The implementation uses MS SharePoint, its lists to store the model data and wiki pages to aggregate the model data to be presented as a document. The template document is issued as a PDF document, which will be provided in the following pages.

# Qualification process

---

## Document info

### Document identification

Title

DocumentID	<input type="checkbox"/> Modified By	Modified	Version	Issuing organisation
DOCW-00085	<input checked="" type="checkbox"/> Alanen Jarmo	15/11/2016 15:39	1.13	VTT


### Change log

Version	Date	Status (draft /proposal /approved)	Author(s) / Reviewer(s) / Approver, Organisation	Remarks of changes
0.1	08.01.2016	Draft	Jarmo Alanen, VTT	Created
1.13	15.11.2016	Draft	Jarmo Alanen, VTT	Draft

## Introduction

### Process identification

The process is identified as follows:

Code	Title	Category	Modified	Modified By
Code		PRCSS-70		
Title		Qualification process		
Category		Agreements and authorisation management		
Modified		30/09/2016 13:28		
Modified By		 Alanen Jarmo		

### Definitions

The main terms related to this process are defined as follows:

✓ Title	Description	Source
Artefact	A synonym to <i>Work product</i>	
Assurance case	<p>1. Reasoned, auditable artefact created that supports the contention that its top-level claim (or set of claims), is satisfied, including systematic argumentation and its underlying evidence and explicit assumptions that support the claims(s)</p> <p>NOTE 1: An assurance case contains the following and their relationships:</p> <ul style="list-style-type: none"> <li>• one or more claims about properties</li> <li>• arguments that logically link the evidence and any assumptions to the claims(s)</li> <li>• a body of evidence and possibly assumptions supporting these arguments for the claim(s)</li> <li>• justification of the choice of top-level claim and the method of reasoning</li> </ul> <p>2. A collection of auditable claims, arguments, and evidence created to support the contention that a defined system/service will satisfy its assurance requirements.</p>	1. ISO/IEC 15026-1 2013; 2. Structured Assurance Case Metamodel (SACM) Version 2.0 (December 2015 draft)
Attestation	<p><b>Issue of a statement, based on a decision following review, that fulfilment of specified requirements has been demonstrated</b></p> <p>NOTE: In this context, attestation is considered to include the review activity (which we call assessment), although in case of certification at component level, the attestation may be independent of the review. Furthermore, the activities to prepare for the approval are included in the set of attestation activities.</p>	ISO 17000:2004
Certification	Third-party attestation related to products, processes, systems or persons	ISO 17000:2004
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 information item or a collection of information items, or any other engineering artefact, like a requirement statement or a complete list of requirements can be a CI.</p>	ISO/IEC/IEEE 15288 2015, except the notes, which are by the authors of this report
Conformity assessment	Demonstration that specified requirements relating to a product, process, system, person or body are fulfilled	IEC Glossary
Determination	Activity to find out one or more characteristics and their characteristic values	ISO 9000:2015
Information item	<p>Separately identifiable body of information that is produced, stored, and delivered for human use; a special case of a Work product</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 configuration item, 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>	ISO/IEC/IEEE 15289 2015 and ISO/IEC TR 24774 2010, except the notes, which are by 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.	

Title	Description	Source
Process view	<p>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.</p> <p>Description of how a specified purpose and set of outcomes can be achieved by employing the activities and tasks of existing processes</p>	<p>ISO/IEC/IEEE 15288 2015, except the note, which is by the authors of this report</p> <p>ISO/IEC 15026-1 2013, which transcribes the definition from ISO/IEC/IEEE 15288 2015</p>
Qualification	<p>1) Qualification shall refer to a process to demonstrate the ability to fulfil specified requirements (corresponds to the qualification process of the ISO 9000 standard). [Source YVL Glossary by STUK] [ISO 9000:2015 does not define the term qualification (process) any more]</p> <p>2) Process of determining whether a system or component is suitable for operational use.</p> <ul style="list-style-type: none"> <li>• Qualification is generally performed in the context of a specific set of qualification requirements for the specific facility and class of system and for the specific application.</li> <li>• Qualification may be accomplished in stages: e.g., first, by the qualification of pre-existing equipment (usually early in the system realization process), then, in a second step, by the qualification of the integrated system (i.e. in the final realized design).</li> <li>• Qualification may rely on activities performed outside the framework of a specific facility design (this is called 'generic qualification' or 'prequalification').</li> <li>• Prequalification may significantly reduce the necessary effort in facility specific qualification; however, the application specific qualification requirements must still be met and be shown to be met.</li> </ul>	<p>Several sources; see the definition.</p>
	<p>Equipment qualification. Generation and maintenance of evidence to ensure that equipment will operate on demand, under specified service conditions, to meet system performance requirements.</p> <p>See IAEA GSR Part 4 (Rev. 1).</p> <ul style="list-style-type: none"> <li>• More specific terms are used for particular equipment or particular conditions; for example, seismic qualification is a form of equipment qualification that relates to conditions that could be encountered in the event of earthquakes.</li> <li>• The proof that an item of equipment can perform its function, which is an important part of equipment qualification, is sometimes termed substantiation.</li> </ul>	
	<p>[Source IAEA Safety glossary]</p> <p>NOTE 1: In this context, we consider that qualification is an attestation activity required by an authority (internal or external), and we emphasise the distinction between validation and qualification by considering that the qualification process is assumed to only consist of the additional activities after the V&amp;V activities in high rigour projects to attest the V&amp;V results. We see this distinction important and commendable to provide for well capsulated qualification and V&amp;V processes.</p> <p>NOTE 2: In some contexts, licensing is used as a synonym for qualification; in other cases, the term licensing is only used for plant level authorisation. Due to the vague usage of the term licensing, we do not define nor use the term licensing in this context.</p>	
Safety demonstration	<p>The set of arguments and evidence elements which support a selected set of claims on the safety of the operation of a system important to safety used in a given plant environment.</p> <p>NOTE 1: When safety demonstration is presented in a structured fashion it can be called a safety related assurance case.</p> <p>NOTE 2: In some contexts, safety demonstration is treated as an activity; here we treat it as an artefact according to Common position (2014); qualification is the activity that assembles the safety demonstration.</p>	<p>Common position 2014, except NOTE1 and NOTE 2, which are by VTT.</p>
System	<p>Combination of interacting elements organized to achieve one or more stated purposes</p> <p>NOTE 1: A system is sometimes considered as a product or as the services it provides.</p> <p>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.</p>	<p>ISO/IEC/IEEE 15288 2015</p>



✓ Title	Description	Source
Systems engineering	<p>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.</p> <p>1. 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</p> <p>2. 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.</p>	1. ISO/IEC/IEEE 15288 2015; 2. 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	INCOSE 2015
Validation	<p>Confirmation, through the provision of objective evidence, that the requirements for a specific intended use or application have been fulfilled</p> <p>NOTE 1: The objective evidence needed for a validation is the result of a test or other form of determination such as performing alternative calculations or reviewing documents.</p> <p>NOTE 2: The word "validated" is used to designate the corresponding status.</p> <p>NOTE 3: The use conditions for validation can be real or simulated.</p> <p>NOTE 4: In this context, we consider validation to be determination plus conformity assessment against stakeholder requirements.</p>	SFS-EN ISO 9000:2015 except NOTE 4.
Verification	<p>Confirmation, through the provision of objective evidence, that specified requirements have been fulfilled</p> <p>NOTE 1: The objective evidence needed for a verification can be the result of an inspection or of other forms of determination such as performing alternative calculations or reviewing documents.</p> <p>NOTE 2: The activities carried out for verification are sometimes called a qualification process.</p> <p>NOTE 3: The word "verified" is used to designate the corresponding status.</p> <p>NOTE 4: In this context, we consider verification to be determination plus conformity assessment against system requirements.</p>	SFS-EN ISO 9000:2015, except NOTE 4
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.	ISO/IEC TR 24774 2010

## Controls

### Process requirements and recommendations

The following tables (Table DOCW-00085-1 and Table DOCW-00085-2) list the requirements and recommendations for this particular process.

Table DOCW-00085-1. YVL Requirements for this process.

Type	ID Location	Description in English
SectionLevel1 : 3 Management of design (3)		
SectionLevel2 : 3.9 Qualification (3)		
□	YVL-B.1-3.9-362	362. The systems, structures and components important to safety shall be qualified for their intended use. The qualification process shall demonstrate that the systems, structures and systems are suitable for intended use and satisfy the relevant safety requirements. Aside from the assurance of the correctness of the design bases and the sufficiency of the quality management of design and implementation, the qualification process shall also include environmental qualification.
□	YVL-B.1-3.9-363	363. A qualification plan shall be prepared and implemented for the system to guide the qualification process. The qualification plan shall <ol style="list-style-type: none"> <li>1. present the data generated in connection with the quality assurance stages (verification and validation) of the systems, structures and components to be used for qualification purposes;</li> <li>2. identify the external assessments, tests and analyses to be used the purpose of qualification, including the methods to be used, their relevance and the performer;</li> <li>3. present a qualification roadmap complete with estimated timetables and dependencies relative to the progress of the project; and</li> <li>4. specify the documentation to be produced in connection with the qualification process and its submission for regulatory review.</li> </ol>
	YVL-B.1-3.9-364	

- 364. The licensee shall evaluate the acceptability of the qualification results and present a justified conclusion drawn from the results.

## ▣ SectionLevel1 : 5 Qualification of electrical and I&C systems, equipment and cables (71)

### ▣ SectionLevel2 : 5.1 General qualification requirements (3)

- [YVL-E.7-5.1-501](#) 501. The electrical and I&C systems of a nuclear facility and their components and cables shall be suitable for their intended purpose and location of use.
- [YVL-E.7-5.1-502](#) 502. Safety-classified electrical and I&C equipment and cables shall be qualified for their intended purpose and location of use.
- [YVL-E.7-5.1-504](#) 504. During qualification, the component's maximum storage life and service life shall be identified, after which the qualification shall be performed again or the component replaced, if the operation of the component is required under accident conditions, or if rapidly ageing parts have been identified in the component (see para. 354).

### ▣ SectionLevel2 : 5.10 Type approval (9)

- [YVL-E.7-5.10-569](#) 569. Type approval shall be acquired for the following equipment:
- I&C system platforms in safety class 2
  - software-based I&C priority units in safety class 2
  - I&C equipment in safety class 2 to be qualified to accident conditions
  - electrical equipment in safety class 2 to be qualified to accident conditions, excluding electric motors and electric valve actuators whose requirements are discussed in Guides YVL E.8 and E.9
  - cables in safety class 2 to be qualified to accident conditions
  - essential accident instrumentation in safety class 3 to be qualified to accident conditions.
- [YVL-E.7-5.10-570](#) 570. The prerequisite for the type approval of equipment shall be a type inspection certificate issued by a third party confirming the acceptability of the design and implementation of the equipment against the equipment rated values. A third-party assessment of the type conformity of the quality assurance-based production process, or a third-party certificate of conformity that confirms the type conformity of the manufactured equipment based on product-specific inspection and testing, shall also be required. The type inspection and verification of conformity shall follow modules B and D of Decision 768/2008/EC [5] of the European Parliament and of the Council. Module F may be used instead of module D.
- [YVL-E.7-5.10-571](#) 571. The third party authorised to perform the type inspection and type conformity assessment of an component shall be a certification body that has been accredited for the conformity evaluation of the applied standards under standard SFS-EN ISO/IEC 17065 [6], or an inspection organisation accredited for a similar task under standard SFS-EN ISO/IEC 17020 [7]. In order to supervise the testing, the certification body or inspection organisation shall have applicable qualifications under standard SFS-EN ISO/IEC 17025 [8]. The certification body or inspection organisation shall also be a notified body appropriate for the task.
- [YVL-E.7-5.10-572](#) 572. The accreditation decision pertaining to the organisation performing type inspections and type conformity evaluations shall be appended to the preliminary suitability analysis. If the same organisation is to submit multiple type approvals, the accreditation decision may be delivered only once, but a reference to the documentation submitted earlier shall be made in the preliminary suitability analysis.
- [YVL-E.7-5.10-573](#) 573. In the type inspection, the third party shall inspect the component as a combination of design type and product type as referred to in module B of the Decision [5].
- [YVL-E.7-5.10-574](#) 574. The type inspection certificate or appendices thereto shall indicate all the information confirmed with a type inspection (technical breakdown) and any limitations on operation required to assess the acceptability of the component for its intended use.
- [YVL-E.7-5.10-575](#) 575. A document prepared by a third party concerning the approval of the quality system pursuant to module D of the Decision [5] shall be appended to the type approval documentation.
- [YVL-E.7-5.10-576](#) 576. If module F of the Decision [5] is used, the conformity certificate issued on the basis of product-specific inspections and testing shall indicate the following:
- the unique identifiers of the delivery batch, and the unique identifiers of the components inspected from the delivery batch
  - inspections performed and tests supervised by a third party (scope of product-specific inspection) in order to confirm the conformity to requirements of the de-livery batch
  - the conformity certificate shall refer to the type inspection certificate, and it shall confirm that the components in the delivery batch correspond to the component type for which the type inspection certificate has been issued.
- [YVL-E.7-5.10-577](#) 577. The type approval of a component containing software-based technology shall cover the assessment of both software and hardware.

### ▣ SectionLevel2 : 5.2 Qualification plan (9)

- [YVL-E.7-5.2-505](#) 505. The licensee shall prepare a special system or component-specific qualification plan for the validation of electrical and I&C systems, equipment and cables in safety classes 2 and 3.
- [YVL-E.7-5.2-506](#) 506. The qualification plan shall be prepared in accordance with a procedure part of the licensee's quality management system.
- [YVL-E.7-5.2-507](#) 507. The qualification plan of electrical and I&C systems, equipment and cables in safety classes 2 and 3 shall discuss the following subareas:
- applicable standards
  - design and manufacturing process
  - tests
  - organisations to be used in the qualification
  - analyses
  - operating experience feedback.
- [YVL-E.7-5.2-508](#) 508. The suitability analyses to be prepared shall be presented in the qualification plan of an electrical and I&C system in safety classes 2 and 3.
- [YVL-E.7-5.2-509](#) 509. Information on any previous type approvals or tests that the licensee wishes to use in the validation shall be enclosed with the qualification plan of electrical and I&C systems in safety classes 2 and 3.

- ☐ YVL-E.7-5.2-510 510. The qualification plan of electrical and I&C systems, equipment and cables in safety class 2 shall present the procedure whereby the acceptability of the validation procedure of electrical and I&C systems, equipment and cables in safety class 2 is independently assessed (para. 351).
- ☐ YVL-E.7-5.2-511 511. The qualification plan shall identify all software tools used in the design and implementation of software-based electrical and I&C systems and equipment in safety class 2, such as compilers, code generators, analysers etc.
- ☐ YVL-E.7-5.2-512 512. The qualification plan shall identify all software-based testing and analysis methods used in the design and implementation of electrical and I&C systems and equipment in safety class 2.
- ☐ YVL-E.7-5.2-513 513. The qualification plan of electrical and I&C systems, equipment and cables in safety classes 2 and 3 shall be updated, if changes are introduced into the requirement specification such that this affects the qualification, or if information is revealed that may be seen to affect the qualification process and, thus, the qualification plan.
- ☐ SectionLevel2 : 5.3 Tests included in qualification (10)
- ☐ YVL-E.7-5.3-514 514. Test plans shall be drawn up for the qualification tests of electrical and I&C systems, equipment and cables in safety classes 2 and 3.
- ☐ YVL-E.7-5.3-515 515. The tests shall be performed in accordance with the qualification test plan (para. 514) by independent testers who are independent of the design and manufacture of the electrical or I&C system, component or cable in safety class 2 or 3.
- ☐ YVL-E.7-5.3-516 516. The qualification test plan (para. 514), the test acceptance criteria and the test results shall be documented in a manner that allows them to be evaluated by the author of the final suitability analysis and, if necessary, by an authority.
- ☐ YVL-E.7-5.3-517 517. Testing and analyses shall be used to ensure that the electrical or I&C systems or equipment in safety class 2 contain no unnecessary functions that could be detrimental to safety.
- ☐ YVL-E.7-5.3-518 518. The sufficiency of the electrical and I&C system or component tests in safety class 2 shall be justified, and the coverage of the tests shall be analysed against the requirements and rated values.
- ☐ YVL-E.7-5.3-519 519. After the factory tests, the licensee shall assess the conformity to requirements of an electrical or I&C system, component or cable in safety class 2 or 3 before the product may be moved to the facility.
- ☐ YVL-E.7-5.3-520 520. An assessment pursuant to para. 519 shall be appended to the final suitability analysis.
- ☐ YVL-E.7-5.3-521 521. The schedule for the delivery and installation of an electrical and I&C system, component or cable in safety class 2 or 3 shall be planned in a manner that allows for implementing the modification planning and modifications that may be required after the factory tests in accordance with procedures that are in line with the safety significance of the system or component.
- ☐ YVL-E.7-5.3-522 522. The final testing of the electrical or I&C systems or components in safety classes 2 and 3 shall be performed at the facility in the actual operating environment.
- ☐ YVL-E.7-5.3-523 523. Whenever possible, the final testing at the facility (para. 522) shall demonstrate that the electrical or I&C systems, components or cables in safety classes 2 and 3 correspond to the functional and performance requirements set for them.
- ☐ SectionLevel2 : 5.4 Assessment of the design and manufacturing process of electrical and I&C equipment (5)
- ☐ YVL-E.7-5.4-525 525. A nuclear facility's electrical and I&C equipment and cables in safety classes 2 and 3 shall be designed and documented in a manner that allows for ensuring at the various phases of the design and manufacturing process the correct transfer of the set requirements to the final product that will be taken into use.
- ☐ YVL-E.7-5.4-526 526. The design, manufacture and testing processes of a nuclear facility's electrical and I&C equipment and cables in safety classes 2 and 3 shall be managed in a manner that allows for ensuring the correct transfer of the set requirements to the final product that will be taken into use.
- ☐ YVL-E.7-5.4-527 527. The design, manufacture and testing processes of a nuclear facility's electrical and I&C equipment and cables in safety class 3 shall be evaluated in a way that allows for ensuring the correct transfer of the set requirements to the final product that will be taken into use.
- ☐ YVL-E.7-5.4-528 528. The results of the design, manufacture and testing processes of a nuclear facility's electrical and I&C equipment and cables in safety class 2 shall be independently verified in a manner that allows for ensuring the correct transfer of the set requirements to the final product that will be taken into use.
- ☐ YVL-E.7-5.4-529 529. The assessment of the design and manufacture process shall be presented in the final suitability analysis according to the requirements laid down in section 3.4.2.
- ☐ SectionLevel2 : 5.5 Compatibility with the electrical network (11)
- ☐ YVL-E.7-5.5-530 530. The effects that the variations of voltage and frequency occurring in the external power transmission grid and the nuclear facility's internal electrical networks have on the equipment of the nuclear facility shall be analysed.
- ☐ YVL-E.7-5.5-531 531. The variations of voltage and frequency occurring in the external power transmission grid and the nuclear facility's internal electrical networks shall be taken into account in the dimensioning of components.
- ☐ YVL-E.7-5.5-532 532. The variations of voltage and frequency occurring in the external power transmission grid and the nuclear facility's internal electrical networks shall be taken into account in the qualification of components.
- ☐ YVL-E.7-5.5-533 533. The qualification of an electrical or I&C equipment in safety classes 2 or 3 shall assess the operation and rise in temperature of the equipment, when its terminals are under the following conditions:
- rated current and voltage continuously
  - undervoltages of varying duration, with a simultaneous frequency variation of the most unfavourable type in terms of the component
  - overvoltages of varying duration, with a simultaneous frequency variation of the most unfavourable type in terms of the component
  - fast voltage transients
  - highest input voltage ripple
  - for components supplying electrical power, short-circuit scenarios and load start-up current peaks.

- ☐ [YVL-E.7-5.5-534](#) 534. The assessment conducted under para. 533 shall take into account any changes in the load condition of the component as the supply voltage and frequency change.
- ☐ [YVL-E.7-5.5-535](#) 535. The assessment conducted under para. 533 shall assess the startability of a component under voltage disturbance scenarios.
- ☐ [YVL-E.7-5.5-538](#) 538. The experimental parameters of the component under nominal conditions shall be available when using the method described in para. 537.
- ☐ [YVL-E.7-5.5-539](#) 539. The qualification of components containing electronics for the voltage and frequency variations described in para. 533 shall be based on tests.
- ☐ [YVL-E.7-5.5-540](#) 540. The rise in temperature of the electrical or I&C equipment in safety classes 2 and 3 shall be defined in the nominal state according to the rated values of the component and by using type tests defined in the standards, if the power loss of the component is high enough for the component to be considered to warm up substantially due to the internal power loss.
- ☐ [YVL-E.7-5.5-541](#) 541. When determining the rise in temperature of electrical or I&C equipment connected to a battery-backed direct current network, the trickle charge voltage for a set of accumulators shall be used as the supply voltage.
- ☐ [YVL-E.7-5.5-542](#) 542. The rise in temperature of the electrical and I&C equipment or cable in its nominal state shall be taken into account when qualifying the component or cable to the prevailing environmental conditions.

▣ SectionLevel2 : 5.6 Qualification to environmental conditions (14)

- ☐ [YVL-E.7-5.6-543](#) 543. The environmental conditions and stresses of a nuclear facility's safety-classified electrical and I&C systems, components and cables shall be defined in all planned operational conditions and during storage and transport.
- ☐ [YVL-E.7-5.6-544](#) 544. The electrical and I&C systems, components and cables shall be of such design that their operability is maintained within the set requirements during their entire planned service life.
- ☐ [YVL-E.7-5.6-545](#) 545. The validation of safety-classified electrical and I&C equipment and cables to the planned environmental conditions and stresses shall be performed by means of tests and analyses pursuant to standards.
- ☐ [YVL-E.7-5.6-546](#) 546. The tests and analyses laid down in para. 545 shall correspond to the combined effects of the most unfavourable operational and environmental conditions possible.
- ☐ [YVL-E.7-5.6-547](#) 547. The selection of structures and materials for electrical and I&C equipment and cables of safety classes 2 and 3 needed during or after accidents shall be such that, for their entire planned service life, their required operating capability in accidents will be in compliance with the set requirements.
- ☐ [YVL-E.7-5.6-548](#) 548. The performance of electrical and I&C equipment and cables needed during or after accidents shall be demonstrated by means of type tests.
- ☐ [YVL-E.7-5.6-549](#) 549. The type tests defined in para. 548 shall form a uniform series of tests during which the same test pieces are subjected to the design basis operating and environmental stresses of the planned location of use.
- ☐ [YVL-E.7-5.6-550](#) 550. Prior to accident condition testing, the test pieces of electrical and I&C equipment and cables shall be artificially aged to correspond to their planned service life.
- ☐ [YVL-E.7-5.6-551](#) 551. The artificial ageing of electrical and I&C equipment and cables shall be carried out in a way that represents actual ageing with an adequate degree of confidence.
- ☐ [YVL-E.7-5.6-552](#) 552. A test of electrical and I&C equipment and cable simulating an accident shall cover exposure to radiation and stresses caused by temperature, pressure and humidity equivalent to accident conditions as well as rapid changes in the conditions.
- ☐ [YVL-E.7-5.6-553](#) 553. The composition of the water used in the test of electrical and I&C equipment and cable simulating an accident shall, as far as possible, be equivalent to water in real accident conditions.
- ☐ [YVL-E.7-5.6-554](#) 554. If there is a possibility of the electrical and I&C equipment or cable submerging in water in an accident and if it is required to function under such conditions, its capability to function in such a situation shall also be demonstrated.
- ☐ [YVL-E.7-5.6-555](#) 555. The tests of an electrical and I&C equipment and cable simulating an accident shall be designed to verify, with a sufficient degree of confidence, the operability of the component or cable under accident conditions during their entire planned service life.
- ☐ [YVL-E.7-5.6-556](#) 556. If the electrical and I&C equipment or cable must function under severe reactor accidents, it shall be validated by a manner applicable to severe reactor accidents (high temperatures, radiation doses, and hydrogen fires shall be taken into account, for example).

▣ SectionLevel2 : 5.7 Electromagnetic compatibility (1)

- ☐ [YVL-E.7-5.7-558](#) 558. The EMC conformity of electrical and I&C equipment and installations shall be demonstrated by means of EMC tests or analyses pursuant to standards.

▣ SectionLevel2 : 5.8 Qualification by means of analyses (1)

- ☐ [YVL-E.7-5.8-560](#) 560. The qualification of electrical and I&C systems and equipment shall cover the validation of functional and performance requirements by means of analyses, if the meeting of the requirements cannot be demonstrated by means of other qualification activities.

▣ SectionLevel2 : 5.9 Operating experience feedback (8)

- ☐ [YVL-E.7-5.9-561](#) 561. An operating experience analysis shall be prepared for the electrical and I&C systems in safety class 2 or 3 and the components thereof.
- ☐ [YVL-E.7-5.9-562](#) 562. The operating experience feedback used in the operating experience analysis of the electrical and I&C systems in safety class 2 or 3 and the components thereof shall be collected following a procedure for which instructions are provided.
- ☐ [YVL-E.7-5.9-563](#) 563. The operating experience analysis of the software-based electrical and I&C systems in safety class 2 or 3 and the components thereof shall also take into account any software used.

- ☐ [YVL-E.7-5.9-564](#) 564. The operating experience analysis of the software-based electrical and I&C systems in safety class 2 or 3 and the components thereof shall also take into account the change and version history of the software.
- ☐ [YVL-E.7-5.9-565](#) 565. The comprehensiveness of the operating experience collection process, the length of the collection period and their significance in terms of the reliability of the data shall be evaluated in the operating experience analysis.
- ☐ [YVL-E.7-5.9-566](#) 566. The operating experience feedback used in the analysis shall be representative of the safety function reviewed.
- ☐ [YVL-E.7-5.9-567](#) 567. The use of operating experience feedback from hardware or software versions, set-ups and operational profiles other than those that are planned to be taken into use for the validation of a system or component shall be justified.
- ☐ [YVL-E.7-5.9-568](#) 568. A component cannot be qualified on the basis of operating experience feedback only.

## ☐ SectionLevel1 : 6 Qualification of software of safety-classified equipment (50)

### ☐ SectionLevel2 : 6.1 Special requirements for software-based equipment (13)

- ☐ [YVL-E.7-6.1-601](#) 601. The publication [4] "Licensing of safety critical software for nuclear reactors, Common position of seven European nuclear regulators and authorised technical support organisations, Revision 2010" presents in great detail some differences between the requirement levels concerning the design, implementation and maintenance of software in different safety classes. The requirements of this publication shall be taken into account, when applicable, in the design of I&C systems and equipment in safety classes 2 and 3.
- ☐ [YVL-E.7-6.1-602](#) 602. The design and implementation of software in safety classes 2 and 3 shall adhere to applicable nuclear industry standards.
- ☐ [YVL-E.7-6.1-603](#) 603. The design of software in safety class 2 systems and equipment shall aim at clarity and simplicity.
- ☐ [YVL-E.7-6.1-604](#) 604. The structure of software in safety class 2 shall minimise the propagation of the effects of a single software error.
- ☐ [YVL-E.7-6.1-605](#) 605. The structure of software in safety class 2 shall enable the verification of the requirements set for the system.
- ☐ [YVL-E.7-6.1-606](#) 606. The program execution cycle of software in safety classes 2 and 3 shall be defined.
- ☐ [YVL-E.7-6.1-607](#) 607. Those software parts that are unnecessary for functional performance shall be identified and their safety significance shall be analysed and taken into account in the design of the system in safety class 2.
- ☐ [YVL-E.7-6.1-608](#) 608. The failure mechanisms of software in safety classes 2 and 3 shall be identified and analysed to a sufficient extent.
- ☐ [YVL-E.7-6.1-609](#) 609. Software-based systems and components in safety classes 2 and 3 shall be equipped with self-diagnostics corresponding to their safety significance and the reliability requirements set by the periodic test interval.
- ☐ [YVL-E.7-6.1-610](#) 610. The coverage of the self-diagnostics and periodic tests of the software-based I&C systems and components in safety class 2 shall be analysed.
- ☐ [YVL-E.7-6.1-611](#) 611. The effects of failures in the self-diagnostics function of a software-based system or component in safety class 2 on the operation of the protection I&C systems shall be analysed.
- ☐ [YVL-E.7-6.1-612](#) 612. The requirements set for software in safety class 2 or 3 shall be derivable in a traceable manner from component or system level requirements.
- ☐ [YVL-E.7-6.1-613](#) 613. Paras 601–612 shall also apply to data transfer and data buses between different software.

### ☐ SectionLevel2 : 6.2 Qualification of the system platform software and the application software (7)

- ☐ [YVL-E.7-6.2-614](#) 614. The qualification plan of a programmable system in safety class 2 or 3 (see section 5.2) shall cover the qualification of the system platform software and the application software.
- ☐ [YVL-E.7-6.2-615](#) 615. The type approval of a system platform or component (see section 5.10) shall also cover the system platform software.
- ☐ [YVL-E.7-6.2-616](#) 616. For system platforms or components in safety class 3 for which a type approval pursuant to section 5.10 is not required, an assessment of the system platform software shall be performed under an applicable standard on the basis of the reliability objective set for the system or component.
- ☐ [YVL-E.7-6.2-617](#) 617. The evaluation report defined in para. 616 shall present the observations made in the inspection, the need for any corrective actions, and a justified decision on the acceptability of the software for the intended purpose of use.
- ☐ [YVL-E.7-6.2-618](#) 618. An analysis of the capability of the design process and conformity to standards of the design process of the system platform software and application software shall form a part of the demonstration of reliability of a software-based system or component in safety class 2 or 3.
- ☐ [YVL-E.7-6.2-619](#) 619. An analysis of the qualifications of the personnel participating in design and testing shall form a part of the demonstration of reliability of a software-based system or component in safety class 2 or 3.
- ☐ [YVL-E.7-6.2-620](#) 620. As a part of the demonstration of the reliability of a software-based system or equipment in safety class 2 or 3, an analysis of the standards used and their applicability shall be made.

### ☐ SectionLevel2 : 6.3 Software design procedures and processes (4)

- ☐ [YVL-E.7-6.3-621](#) 621. A life cycle model under an applicable standard shall be defined for the manufacture of software in safety class 2 or 3.
- ☐ [YVL-E.7-6.3-622](#) 622. The methods used in the design, testing and quality assurance of software in safety classes 2 and 3 shall be defined.
- ☐ [YVL-E.7-6.3-623](#) 623. Any conditions and limitations presented in the type approval of the system platform (para. 615) or the assessment of the system platform (para. 616) shall be taken into account in the design and implementation of application software in safety class 2 or 3.
- ☐ [YVL-E.7-6.3-624](#)

624. The design, manufacture and testing processes of a nuclear facility's software in safety class 2 shall be independently assessed after each phase in a manner that allows for ensuring the correct transfer of the set requirements to the final product that will be taken into use.

SectionLevel2 : 6.4 Software tools (6)

- ☐ [YVL-E.7-6.4-625](#) 625. The operating experience feedback from tools used in the design, implementation and testing of software of systems and equipment in safety class 2 shall be collected and documented in a comprehensive and systematic manner.
- ☐ [YVL-E.7-6.4-626](#) 626. The software tools of systems and equipment in safety class 2 shall be covered by comprehensive configuration management.
- ☐ [YVL-E.7-6.4-627](#) 627. The design and implementation of software of safety class 3 systems and equipment shall utilise software tools whose configuration management, maintenance and fault data collection are appropriately documented.
- ☐ [YVL-E.7-6.4-628](#) 628. The configuration management, maintenance and modification design of tools used for configuration and object code generation in safety classes 2 and 3 shall be implemented using procedures which consider the safety significance of the system or component.
- ☐ [YVL-E.7-6.4-629](#) 629. The impact of a potential tool-induced error on safety shall be accounted for when specifying the qualification procedures of software tools in safety class 2.
- ☐ [YVL-E.7-6.4-630](#) 630. In the case of a software tool error, the procedures used to ensure the safe functioning of systems installed at the facility shall be documented.

SectionLevel2 : 6.5 Cybersecurity and isolation of data transfer (7)

- ☐ [YVL-E.7-6.5-631](#) 631. The design, operation and maintenance of electrical and I&C systems and components shall take into account cybersecurity matters in accordance with the licensee's information security procedures.
- ☐ [YVL-E.7-6.5-632](#) 632. Unauthorised access to rooms and to any software of equipment important to the facility's safety and disturbance-free operation shall be prevented by sufficient physical protection, technical and administrative security measures. Requirements related to security arrangements at a nuclear facility are provided in Guide YVL A.11 and requirements for information security are provided in Guide YVL A.12.
- ☐ [YVL-E.7-6.5-633](#) 633. The installation of unauthorised parts of software during design, manufacture, commissioning, periodic testing and maintenance shall be reliably prevented.
- ☐ [YVL-E.7-6.5-634](#) 634. Accesses to the software of electrical and I&C systems and components, and any modifications made thereto during such accesses, shall be traceable.
- ☐ [YVL-E.7-6.5-635](#) 635. No physical possibility shall exist for the establishment of a data transfer connection to the software-based systems important to the safety of a nuclear facility from outside the system inwards.
- ☐ [YVL-E.7-6.5-636](#) 636. A software-based arrangement of unidirectional data transfer shall not be considered a sufficient means of protection to meet the requirement laid down of para. 635.
- ☐ [YVL-E.7-6.5-637](#) 637. As regards para. 635, the software-based systems that are essential to the safety of the nuclear facility shall be identified and specified in the licensee's information security procedures.

SectionLevel2 : 6.6 Existing software (4)

- ☐ [YVL-E.7-6.6-639](#) 639. Existing software is subject to the same requirements as software to be developed.
- ☐ [YVL-E.7-6.6-640](#) 640. Any deficiencies in the documentation and implementation of the design process of existing software may be substituted for by means of analyses and testing, while taking into account the requirements set by the safety class and safety significance.
- ☐ [YVL-E.7-6.6-641](#) 641. Software structure and functions shall be analysed, and the functions to be excluded from use documented, for the suitability analysis of existing software.
- ☐ [YVL-E.7-6.6-642](#) 642. The documentation of the existing software and system shall enable the configuration management and modification planning of the system or software.

SectionLevel2 : 6.7 Software testing (9)

- ☐ [YVL-E.7-6.7-643](#) 643. A testing plan shall exist for all software.
- ☐ [YVL-E.7-6.7-644](#) 644. The software testing plan shall be aligned with the testing plans of the component and system.
- ☐ [YVL-E.7-6.7-645](#) 645. The test plan and procedures used for a system or component belonging to safety class 2 or 3 shall be sufficient, taking into account the safety significance and reliability target of the system or component.
- ☐ [YVL-E.7-6.7-646](#) 646. The software shall also be tested in the equipment to be installed at the facility.
- ☐ [YVL-E.7-6.7-647](#) 647. The final testing of a system or component belonging to safety class 2 or 3 shall cover all functions with their timings, including, as far as practically possible, the self-diagnostic functions.
- ☐ [YVL-E.7-6.7-648](#) 648. The testing of the software shall include static and dynamic tests.
- ☐ [YVL-E.7-6.7-649](#) 649. The software test cases shall also include transient situations used in transient and accident analyses.
- ☐ [YVL-E.7-6.7-650](#) 650. The coverage of the tests of safety classes 2 and 3 software shall be analysed against the requirements at the different phases of testing.
- ☐ [YVL-E.7-6.7-651](#) 651. Justification shall be provided for the selection and number of the final tests of software in safety classes 2 and 3.

## Table DOCW-00085-2. Other requirements for this process.

[+](#) [new item](#) or [edit](#) this list

✓	Source_	SourceDetails	Requirement	Rationale
		4.48		



Source_	SourceDetails	Requirement	Rationale
REF-86: SSR-2/2		Appropriate concepts and the scope and process of equipment qualification shall be established, and effective and practicable methods shall be used to upgrade and preserve equipment qualification. A programme to establish, to confirm and to maintain required equipment qualification shall be launched from the initial phases of design, supply and installation of the equipment. The effectiveness of equipment qualification programmes shall be periodically reviewed.	
REF-86: SSR-2/2	4.49	The scope and details of the equipment qualification process, in terms of the required inspection area(s), method(s) of non-destructive testing, possible defects inspected for and required effectiveness of inspection, shall be documented and submitted to the regulatory body for review and approval. Relevant national and international experience shall be taken into account in accordance with national regulations.	
REF-73: SSR-2/1	5.48	The environmental conditions considered in the qualification programme for items important to safety at a nuclear power plant shall include the variations in ambient environmental conditions that are anticipated in the design basis for the plant.	
REF-73: SSR-2/1	5.49	The qualification programme for items important to safety shall include the consideration of ageing effects caused by environmental factors (such as conditions of vibration, irradiation, humidity or temperature) over the expected service life of the items important to safety. When the items important to safety are subject to natural external events and are required to perform a safety function during or following such an event, the qualification programme shall replicate as far as is practicable the conditions imposed on the items important to safety by the natural event, either by test or by analysis or by a combination of both.	
REF-73: SSR-2/1	5.50	Any environmental conditions that could reasonably be anticipated and that could arise in specific operational states, such as in periodic testing of the containment leak rate, shall be included in the qualification programme.	
REF-87: IEC EN 61513	Subclause 6.5.2 Para 3	If pre-qualification of pre-existing equipment is relied on, application-specific qualification shall be performed.	
REF-87: IEC EN 61513	Subclause 6.5.2 Para a)	Depending on the extent of the available documentation and evidence of pre-qualification, an appropriate application-specific qualification program shall be defined and included in the qualification plan.	
REF-87: IEC EN 61513	Subclause 6.5.2 Para b)	The application-specific qualification shall address the properties and characteristics not covered by pre-qualification.	
REF-87: IEC EN 61513	Subclause 6.5.2 Para c)	The application-specific qualification shall address the differences between the qualification methodology and procedures applied for pre-qualification, and those imposed by the system requirement specification that is addressed by subclause 6.2.2.7 of IEC 61513 (2011).	
REF-87: IEC EN 61513	Subclause 6.5.2 Para before para c)	The system qualification process may be accomplished in stages: first by qualifying the individual hardware and software components of an I&C system, and then by qualifying the integrated I&C system (i.e. the final realized design).	
REF-87: IEC EN 61513	Subclause 6.5.2 Para d) first sentence	The qualification of the hardware and system software of a system built up by configuring an equipment family or connecting pre-existing components may be derived from the qualification performed on individual components and configurations of interconnected components.	
REF-87: IEC EN 61513	Subclause 6.5.2 Para d) last sentence	If the allowance granted by REQ-21 is exploited, an analysis shall be completed to demonstrate that the qualification covers the final configuration of the	

Source_	SourceDetails	Requirement	Rationale
		system used in the plant, including mounting arrangement, load and temperature distribution inside the cabinets.	
REF-87: IEC EN 61513	Subclause 6.5.2 para e)	Based on the analysis required by REQ-22, the qualification plan should identify all novel features of the system design and define whether complementary qualification tests and evaluations are to be carried out.	
REF-87: IEC EN 61513	Subclause 6.5.3.1 Para 1	A qualification plan shall be developed which identifies all the topics (see figure below) to be evaluated and assessed in order to qualify the system and the functions important to safety that it implements and to maintain the qualified status.	

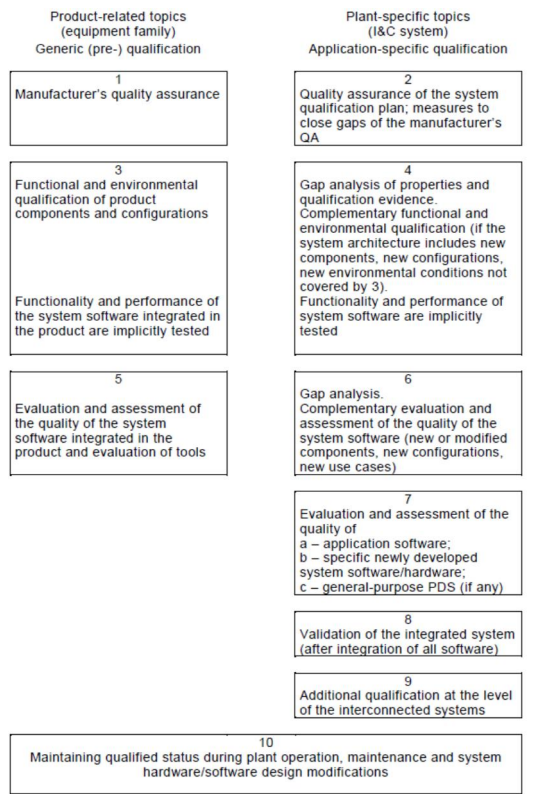


Figure 6 – Product- and plant-application-specific topics to be addressed in the system qualification plan

(Figure 6 from IEC 61513:2011)

REF-87: IEC EN 61513	Subclause 6.5.3.1 NOTE para	Any modifications to the pre-existing component or COTS product design constitute a change of version and the qualification will need to be reassessed.
REF-87: IEC EN 61513	Subclause 6.5.3.2 Para 2	Type testing is the preferred method for functional and environmental qualification (i.e. hardware qualification).
REF-87: IEC EN 61513	Subclause 6.5.3.2 Para a) first sentence	Class 1 and class 2 systems shall be qualified for their environmental conditions in accordance with the requirements of IEC 60780 and IEC 60980.
REF-87: IEC EN 61513	Subclause 6.5.3.2 Para a) last sentence	Qualification for environmental conditions shall include those environmental conditions specified in 6.2.2.6 [of IEC 61513:2011].
REF-87: IEC EN 61513	Subclause 6.5.3.2 Para b) first sentence	Class 3 systems for which specific environmental qualification is required (e.g. resistance to seismic conditions, or operation under specific environmental conditions), may be qualified to industrial standards.
REF-87: IEC EN 61513	Subclause 6.5.3.2 Para b) second sentence	Claims for Class 3 system operation in abnormal environmental conditions, seismic qualification to industrial standards or other credited functional performances shall be justified by documentary evidence.



Source_	SourceDetails	Requirement	Rationale
REF-87: IEC EN 61513	Subclause 6.5.3.2 Para b) third sentence	Where significant ageing factors of Class 3 system exist, and when qualified life cannot be demonstrated in accordance with the definition given in IEC 60780, an on-going qualification program shall be proposed and justified compliant with IEC 60780.	
REF-87: IEC EN 61513	Subclause 6.5.3.2 Para c)	EMC qualification shall be performed in accordance with the applicable requirements of the IEC 61000-4 series.	
REF-87: IEC EN 61513	Subclause 6.5.3.2 Para d) first bullet	Test sequences to check the functional characteristics under normal ambient conditions and at all specified limits of operation, including acceptance criteria, shall be defined for the testing of components or configurations of components or the whole system as appropriate.	
REF-87: IEC EN 61513	Subclause 6.5.3.2 Para d) second bullet	Test sequences to check the specified self-surveillance, fail-safe characteristics and degraded modes of operation, including acceptance criteria, shall be defined for the testing of components or configurations of components or the whole system as appropriate.	
REF-87: IEC EN 61513	Subclause 6.5.3.2 Para d) third bullet	Test sequences to demonstrate the resistance to the relevant environmental conditions (including seismic and electromagnetic environment), including acceptance criteria, shall be defined for the testing of components or configurations of components or the whole system as appropriate.	
REF-87: IEC EN 61513	Subclause 6.5.3.2 Para e)	Analyses should be performed to justify system characteristics which cannot be adequately substantiated by other means	
REF-87: IEC EN 61513	Subclause 6.5.3.3 Para 1	For pre-existing software (PDS), feedback of operating experience may constitute under certain conditions a compensating factor for lack of information of the development process.	
REF-87: IEC EN 61513	Subclause 6.5.3.3 Para a)	System software shall be qualified.	"...to provide adequate assurance that the software quality is appropriate for achieving the required reliability of the functions performed by the system." (Para a)
REF-87: IEC EN 61513	Subclause 6.5.3.3 Para a)	Application software shall be qualified.	"...to provide adequate assurance that the software quality is appropriate for achieving the required reliability of the functions performed by the system." (Para a)
REF-87: IEC EN 61513	Subclause 6.5.3.3 Para b)	For class 1 systems, newly developed software shall be qualified in accordance with the requirements of IEC 60880.	
REF-87: IEC EN 61513	Subclause 6.5.3.3 Para c)	Software of pre-existing equipment selected for class 1 systems should have been developed according to recognised guides and standards appropriate to the high level of quality required for category A functions (see 7.2.2.1 of IEC 61226:2009).	
REF-87: IEC EN 61513	Subclause 6.5.3.3 Para c)	Software of pre-existing equipment (such as tools) selected for class 1 systems shall meet the requirements of IEC 60880 (SW) and IEC 60987 (HW).	

Source_	SourceDetails	Requirement	Rationale
REF-87: IEC EN 61513	Subclause 6.5.3.3 Para d)	Software of pre-existing equipment selected for class 2 systems should have been developed according to recognised guides and standards.	
REF-87: IEC EN 61513	Subclause 6.5.3.3 Para d)	If REQ-43 cannot be fulfilled, the software of pre-existing equipment selected for class 2 systems may be qualified according to the criteria of IEC 62138, taking into account a documented history of satisfactory operation of the software in similar applications.	
REF-87: IEC EN 61513	Subclause 6.5.3.3 Para e)	IEC 62138 shall be used for criteria for qualification of software for class 3 systems .	
REF-87: IEC EN 61513	Subclause 6.5.4 Para a)	A plan shall be developed for the additional testing that may be required at the level of the interconnected I&C systems to complete their individual qualification.	
REF-87: IEC EN 61513	Subclause 6.5.4 Para b)	The feasibility and consistency of the additional testing shall be verified as part of the verification of the I&C architectural design.	
REF-87: IEC EN 61513	Subclause 6.5.4 Para a)	A complementary plan shall be established for maintaining the qualification during operation and maintenance of the system when replacing parts of the system with other parts which are not identical and in the case of functional modifications.	
REF-87: IEC EN 61513	Subclause 6.5.5 Para b)	The complementary plan shall allow the identification of modules that carry out category A and B functions respectively, to ensure consistency with the validated versions.	
REF-87: IEC EN 61513	Subclause 6.5.5 NOTE para	Complementary plan required in REQ-48 should be established sufficiently early.	
REF-87: IEC EN 61513	Subclause 6.5.5 NOTE Para	Guidance on qualification of modifications should be establish already during the initial design process.	
REF-87: IEC EN 61513	Subclause 6.5.5 NOTE para	Guidance on qualification of modifications should be available latest during commissioning.	
REF-87: IEC EN 61513	Subclause 6.5.6 Para a)	Qualification information which will be provided to the licensing authority should be listed.	
REF-87: IEC EN 61513	Subclause 6.5.6 Para a)	The quality information list should distinguish between information necessary before the installation of a system and information to be provided by the licence applicant in parallel with installation and commissioning, for example test reports.	
REF-87: IEC EN 61513	Subclause 6.5.6 Para b) second sentence	Types of information in the qualification information list should include: <ul style="list-style-type: none"> <li>· descriptions (extensive representations of facts),</li> <li>· explanations (representations of facts with reasoning),</li> <li>· demonstrations,</li> <li>· justifications,</li> <li>· proofs (traceable declarations which prove assertions).</li> </ul>	
REF-87: IEC EN 61513	Subclause 6.5.6 Para c)	The documentation may be grouped according to the purpose for which it is needed.	
REF-87: IEC EN 61513	Subclause 6.5.6 Para c) first bullet	The qualification information content shall include preliminary safety analysis report and summarising documents.	"... in order to assess the conceptual and basic design of the system" (Para c) first bullet)
REF-87: IEC EN 61513	Subclause 6.5.6 Para c) second bullet	The qualification information content shall include detailed descriptions of the whole system or parts of it.	"...to allow independent verification and

Source_	SourceDetails	Requirement	Rationale
REF-87: IEC EN 61513	Subclause 6.5.6 Para c) third bullet	The qualification information content shall include detailed or summary explanations, demonstrations or proofs.	validation." ((Para c) second bullet)  " ... to justify design decisions and to simplify the independent verification and validation process." (Para c) third bullet)
REF-87: IEC EN 61513	Subclause 6.5.6 Para c) fourth bullet	The qualification information content shall include information concerning installation, integration, commissioning, factory and site acceptance tests.	"...in order to verify those parts of the safety life cycle which are between design and operation" (Para c) fourth bullet)
REF-87: IEC EN 61513	Subclause 6.5.6 Para c) fifth bullet	The qualification information content shall include documentation of information necessary for operation of the system.	"...in order to verify procedures to maintain the quality of the system in the long term." (Para c) fifth bullet)

## Applicable regulations

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

### ApplicableRegulations

REF-18: GSR Part 4; REF-82: YVL E.7; REF-84: YVL B.1; REF-86: SSR-2/2; REF-87: IEC EN 61513; REF-88: SSG-39; REF-89: Common position 2014; REF-90: IEC EN 60987; REF-91: IEC EN 60880; REF-92: IEC EN 62138; REF-93: SSG-12; REF-97: IEC/IEEE 60780-323

## Purpose

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 operational use and satisfy the relevant safety requirements.

## Notes

## 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-00085-3.

Table DOCW-00085-3. Input conditions of this process.

Code	Title	RelatedInfItem
INCND-7	Qualification life cycle model is identified	... REF-79: Plan - Project plan
INCND-8	Stakeholder requirements are known	... REF-94: Specification - Stakeholder Requirements Specification (StRS)
INCND-9	...	...


## 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-00085-4.

Table DOCW-00085-4. Roles and responsibilities for this process.

✓ 	Code	Title	Description	DescriptionOfResponsibility
	SEROLE-3	Systems Engineer	...	The person who orchestrates the system development including all the disciplines, such as mechanical, software and electrical engineering. Compared to Project manager, the Systems engineer is responsible for the properties of the system-of-interest, whereas the Project manager is responsible for the schedule and resources (budget, human resources, tools, facilities and services) for the work to achieve the properties. Systems engineer is a sub-contractor to the Project manager.
	SEROLE-4	Requirements Engineer	...	The person who is responsible for the requirements engineering activities and their output artefacts, and for capture, analysis and formulation of input artefacts
	SEROLE-5	Safety engineer	...	The person (and his or her team) who is responsible for the management of the safety engineering activities to ensure the safety of the system.
	SEROLE-63	Authority's inspector (STUK: tarkastaja)	...	The person (or persons) at the regulator who reviews the safety case (safety assessment report or suitability analysis) and provides feedback and the statement of the decision to the licensee; the regulator's contact person between the licensee and the regulator
	SEROLE-66	Independent qualification assessor	...	An independent assessor for Safety Class 2 I&C equipment; may be internal or it may be external in cases where "the electrical and I&C systems and components and cables ...have a significant impact on nuclear safety" (Citation from YVL E.7 [2013])
	SEROLE-67	Management system owner	...	The person who is responsible for the Management system and hence the overall Systems Engineering planning (is not carrying out SE planning of the actual projects, but provides the framework for the project SE planning)
	SEROLE-68	Qualification assessor	...	The person who is responsible for the qualification management and approval of the qualification results within the licensee. Is the licensee's contact person between the regulator and the licensee
	SEROLE-69	Conformity assessor	...	The person (or persons) who checks the determination results (tests, analysis, etc.) and their quality, and compares the results with the requirements and judges whether the object-under-assessment conforms to the requirements set for it
	SEROLE-70	Determination engineer	...	Traditionally called 'test engineer'; person who is responsible for carrying out the determination activities. The determination engineer can be, in big projects, the chief of the determination team or, in small projects, one of the testing persons
	SEROLE-71	System designer	...	The person (and his or her team) who is responsible for the design of the system

## Estimated workloads

The workload estimates are listed in Table DOCW-00085-5.

Table DOCW-00085-5. Estimated workloads for this process.

✓  Code Title Description

There are no items to show in this view of the "SE workloads" list.

## Needed tool types

The tool type that are needed to facilitate execution of this process possible are listed in Table DOCW-00085-6.

Table DOCW-00085-6. Tool types needed by this process.

✓ Code Title Description

There are no items to show in this view of the "SE tool types" list.

## Needed facilities

The facilities that are needed to execute this process are listed in Table DOCW-00085-7.

Table DOCW-00085-7. Facilities needed for this process.

Code Title Description

There are no items to show in this view of the "SE facilities" list. To add a new item, click "New".

## Needed services

The services that are needed to execute this process are listed in Table DOCW-00085-8.

### Table DOCW-00085-8. Services needed by this process.

<input type="checkbox"/>	 Code	Title	Description
--------------------------	--	-------	-------------

There are no items to show in this view of the "SE services" list. To add a new item, click "New".

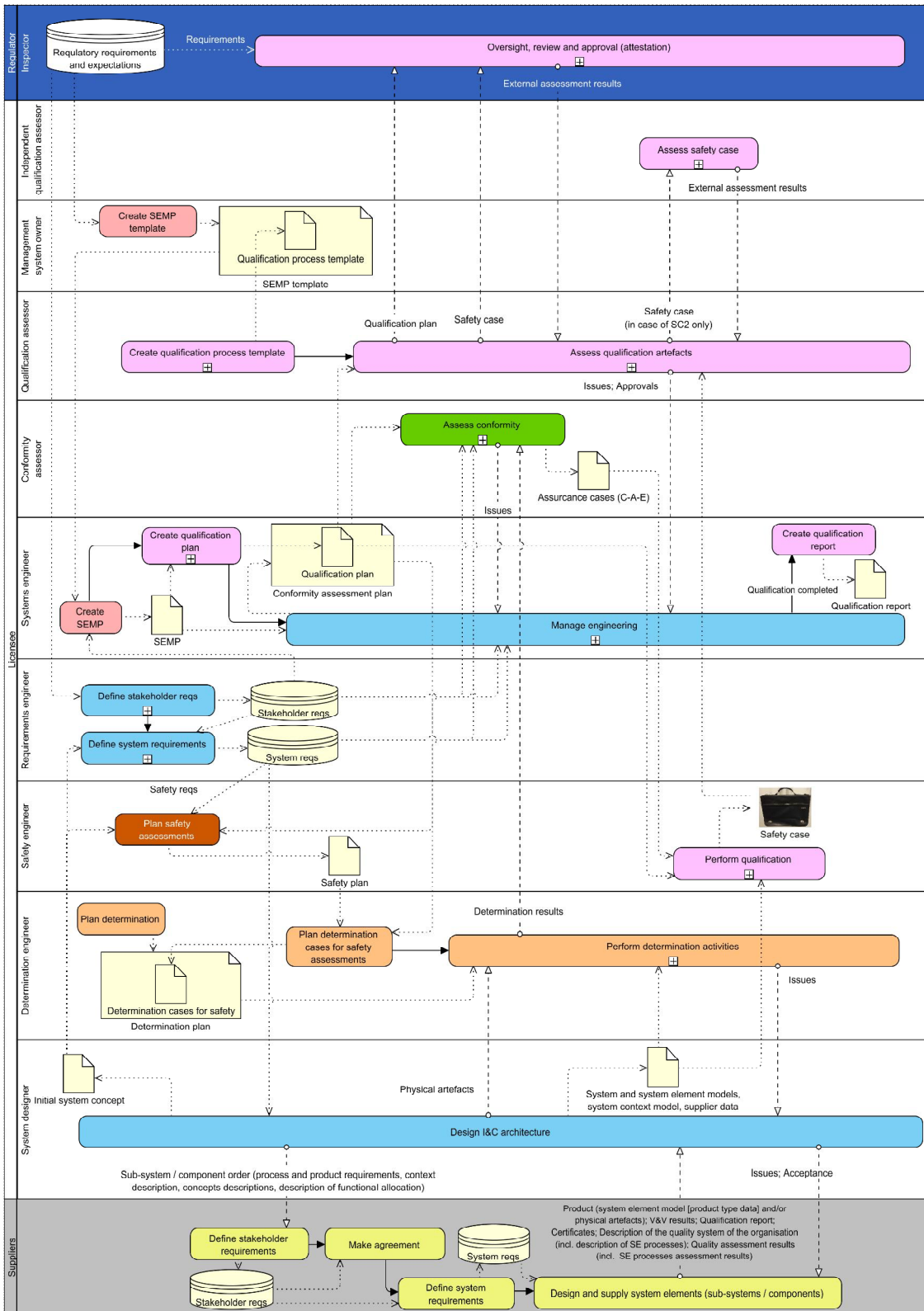
## Execution procedure

---

The qualification process consists of four activities:

- Create qualification plan;
- Perform qualification;
- Assess qualification artefacts;
- Create qualification report.

These activities are distributed to the other systems engineering activities as depicted in the figure below. The figure is an overview of the other SE activities and does not contain all activities, artefacts and information flows.



## Activities

The activities of this process are listed below in Table DOCW-00085-9.

Table DOCW-00085-9. Activities of this process.

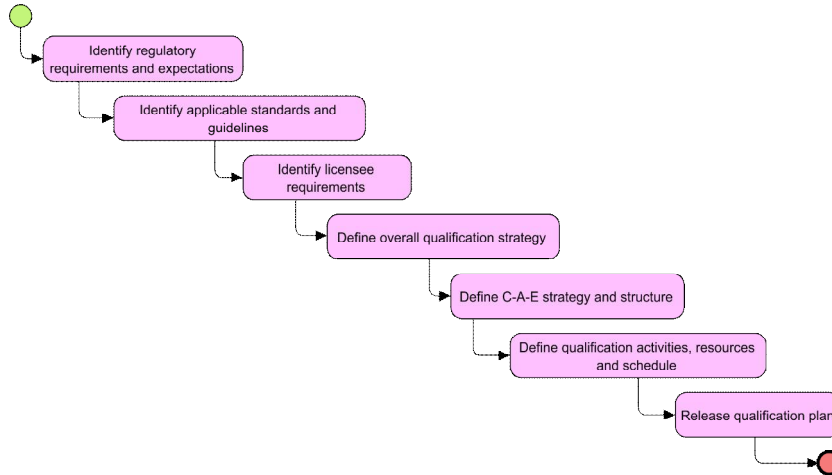
Title	ExecutionProcedure	RelatedRoles
-------	--------------------	--------------

✓ Title  
Create qualification plan

ExecutionProcedure

... The execution of this activity is depicted in the following activity diagram.

RelatedRoles  
Systems Engineer

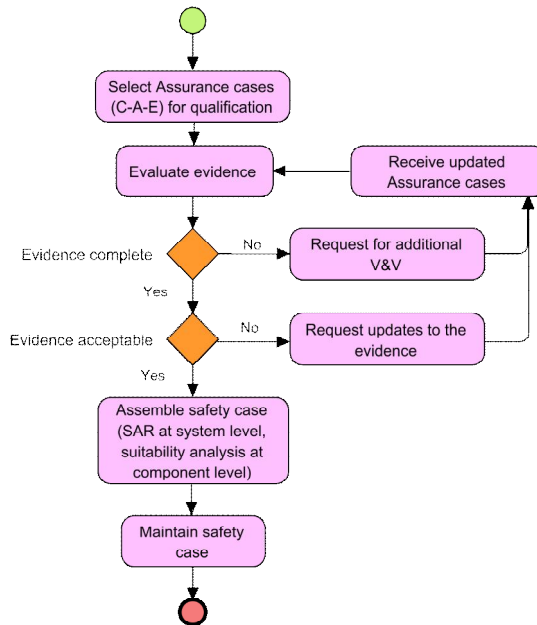


The procedure is thus as follows:...

Perform qualification

... The execution of this activity is depicted in the following activity diagram.

Safety engineer



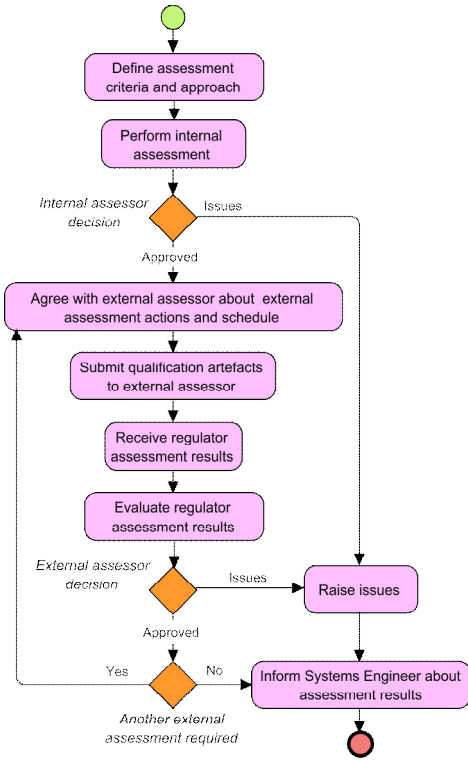
The procedure is thus as follows: ...

Assess qualification artefacts

... The execution of this activity is depicted in the following activity diagram.

Qualificatio  
assessor

✓ Title ExecutionProcedure RelatedRoles



The procedure is thus as follows:...

Create qualification report

... The execution of this activity goes as follows: ...

Systems Engineer



## Tasks

The tasks of the activities of this process are listed below in Table DOCW-00085-10.

Table DOCW-00085-10. The tasks of this process grouped by Activity.

Task title ExecutionProcedure Role assigned to

### Activity : a) Create qualification plan (7)

Task title	<a href="#">Identify regulatory requirements and expectations</a>
ExecutionProcedure	This task is carried out as follows: ...
Role assigned to	<a href="#">Systems Engineer</a>
Task title	<a href="#">Identify applicable standards and guidelines</a>
ExecutionProcedure	This task is carried out as follows: ...
Role assigned to	<a href="#">Systems Engineer</a>
Task title	<a href="#">Identify licensee requirements</a> <span style="color: green;">NEW</span>
ExecutionProcedure	This task is carried out as follows: ...
Role assigned to	<a href="#">Systems Engineer</a>
Task title	<a href="#">Define overall qualification strategy</a>
ExecutionProcedure	This task is carried out as follows: ...
Role assigned to	<a href="#">Systems Engineer</a>
Task title	<a href="#">Define C-A-E strategy and structure</a>
ExecutionProcedure	This task is carried out as follows: ...
Role assigned to	<a href="#">Systems Engineer</a>
Task title	<a href="#">Define qualification activities, resources and schedule</a>
ExecutionProcedure	This task is carried out as follows: ...
Role assigned to	<a href="#">Systems Engineer</a>



Task title	<a href="#">Release qualification plan</a>
ExecutionProcedure	This task is carried out as follows: ...
Role assigned to	<a href="#">Systems Engineer</a>

#### Activity : b) Perform qualification (7)

Task title	<a href="#">Select Assurance cases (C-A-E) for qualification</a>
ExecutionProcedure	This task is carried out as follows: ...
Role assigned to	<a href="#">Safety engineer</a>

Task title	<a href="#">Evaluate evidence</a>
ExecutionProcedure	This task is carried out as follows: ...
Role assigned to	<a href="#">Safety engineer</a>

Task title	<a href="#">Request for additional V&amp;V</a>
ExecutionProcedure	This task is carried out as follows: ...
Role assigned to	<a href="#">Safety engineer</a>

Task title	<a href="#">Request updates to the evidence</a>
ExecutionProcedure	This task is carried out as follows: ...
Role assigned to	<a href="#">Safety engineer</a>

Task title	<a href="#">Receive updated Assurance cases</a>
ExecutionProcedure	This task is carried out as follows: ...
Role assigned to	<a href="#">Safety engineer</a>

Task title	<a href="#">Assemble safety case (SAR at system level, suitability analysis at component level)</a>
ExecutionProcedure	This task is carried out as follows: ...
Role assigned to	<a href="#">Safety engineer</a>

Task title	<a href="#">Maintain safety case</a>
ExecutionProcedure	This task is carried out as follows: ...
Role assigned to	<a href="#">Safety engineer</a>

#### Activity : c) Assess qualification artefacts (8)

Task title	<a href="#">Define assessment criteria and approach</a>
ExecutionProcedure	This task is carried out as follows: ...
Role assigned to	<a href="#">Qualification assessor</a>

Task title	<a href="#">Perform internal assessment</a>
ExecutionProcedure	This task is carried out as follows: ...
Role assigned to	<a href="#">Qualification assessor</a>

Task title	<a href="#">Agree with external assessor about external assessment actions and schedule</a>
ExecutionProcedure	This task is carried out as follows: ...
Role assigned to	<a href="#">Qualification assessor</a>

Task title	<a href="#">Submit qualification artefacts to external assessor</a>
ExecutionProcedure	This task is carried out as follows: ...
Role assigned to	<a href="#">Qualification assessor</a>

Task title	<a href="#">Receive regulator assessment results</a>
ExecutionProcedure	This task is carried out as follows: ...
Role assigned to	<a href="#">Qualification assessor</a>

Task title	<a href="#">Evaluate regulator assessment results</a>
ExecutionProcedure	This task is carried out as follows: ...
Role assigned to	<a href="#">Qualification assessor</a>

Task title	<a href="#">Raise issues</a>
ExecutionProcedure	This task is carried out as follows: ...
Role assigned to	<a href="#">Qualification assessor</a>

Task title	<a href="#">Inform Systems Engineer about assessment results</a>
ExecutionProcedure	This task is carried out as follows: ...
Role assigned to	<a href="#">Qualification assessor</a>

#### Activity : d) Create qualification report (4)

Task title	<a href="#">Obtain and record assessor's approval that the system meets the regulator needs</a>
ExecutionProcedure	This task is carried out as follows: ...
Role assigned to	<a href="#">Systems Engineer</a>

Task title	<a href="#">Create baseline of the qualified system model and of the qualification results</a>
ExecutionProcedure	This task is carried out as follows: ...

Role assigned to	Systems Engineer
Task title	Manage traceability of the qualified system
ExecutionProcedure	This task is carried out as follows: ...
Role assigned to	Systems Engineer
Task title	Release the Qualification report
ExecutionProcedure	This task is carried out as follows: ...
Role assigned to	Systems Engineer

## Outcomes and corresponding information items

The outcomes from this process are listed below in Table DOCW-00085-11.

Table DOCW-00085-11. Outcomes from this process.

✓	🔊	Code	Title	Description	RelatedInfItem	RelatedActivity
		OTCM-10	Qualification criteria for regulatory requirements are defined.	...		
		OTCM-11	System specific qualification plan is prepared	...	REF-95: Qualification plan	SEACT-19: Create qualification plan
		OTCM-12	Objective evidence that the system satisfies regulator needs is provided.	...		
		OTCM-13	Regulator review results are available and anomalies are identified.	...		
		OTCM-14	The system is qualified.	...		
		OTCM-15	Baseline and traceability and of the qualified system is established	...		
		OTCM-16	Qualification results are reported	...	REF-96: Qualification report	SEACT-22: Create qualification report

## Interactions with other processes

---

## Process assessment criteria

---

## Improvement Plan

---

## Additional guidance

In the following, additional guidance on the execution of this particular process is provided. The guidance is not normative, but is supplied as a background and training information.

AdditionalGuidance

---