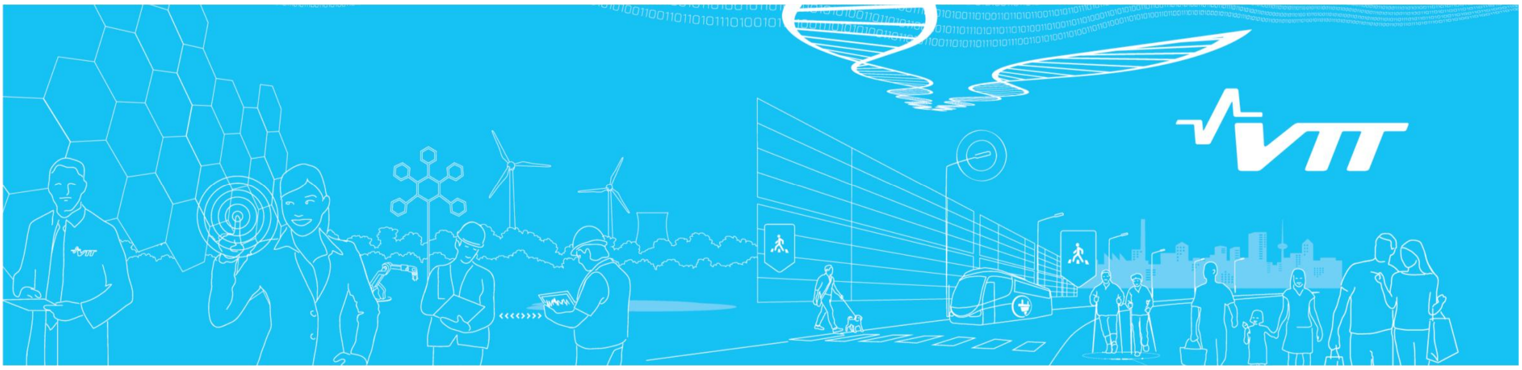


RESEARCH REPORT

VTT-R-00167-16

Safety demonstration of nuclear I&C – an introduction

SAUNA Task 3.1 report

Authors: Janne Valkonen, Teemu Tommila, Joonas Linnosmaa
VTT Technical research centre of Finland Ltd

Timo Varkoi
Finnish Software Measurement Association – FiSMA ry

Confidentiality: Public

Report's title

Safety demonstration of nuclear I&C – an introduction, SAUNA Task 3.1 report

Customer, contact person, address VYR	**Order reference** SAFIR 5/2015
Project name Integrated safety assessment and justification of nuclear power plant automation	**Project number/Short name** 102392/SAUNA
Author(s) Janne Valkonen, Teemu Tommila, Joonas Linnosmaa, Timo Varkoi	**Pages** 38
Keywords Safety demonstration, qualification, safety case, assurance, systems engineering	**Report identification code** VTT-R-00167-16

Summary

This research report describes and discusses the principles of safety justification of nuclear power plants with the focus on instrumentation and control (I&C) systems and the Finnish regulatory practices. The main goals of this report are to introduce the basic ideas and applications of structured safety demonstration and to suggest next development steps. The challenges of safety justification practises are introduced, and the terminology related to safety demonstration is described. The licensing process of nuclear facilities in Finland is described from the safety demonstration viewpoint and general Systems Engineering processes are introduced. Several system life cycle standards are introduced together with a summary of software tools available for supporting generation of structured safety demonstration. On the basis of this report, two main directions for further research can be identified: 1) the qualification process of I&C systems and equipment should be refined covering, for example, terminology, activities, phases, documents and participant roles in various types of I&C projects, 2) practical guidance should be provided for organising the qualification documentation and for presenting the reasoning behind safety claims in understandable, unarguable and traceable ways.

Confidentiality	Public

Espoo 27.1.2016

Written by	**Reviewed by**	**Accepted by**
Janne Valkonen Senior Scientist	Jussi Lahtinen Research Scientist	Riikka Virkkunen Head of Research Area

VTT's contact address

VTT Technical Research Centre of Finland Ltd, P.O. Box 1000, FI-02044 VTT, Finland

Distribution (customer and VTT)

SAFIR2018 programme, VTT Kirjaamo

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.

Preface

This report has been prepared under the research project “Integrated safety assessment and justification of nuclear power plant automation” (SAUNA), which is part of the Finnish Research Programme on Nuclear Power Plant Safety 2015–2018 (SAFIR2018). The overall objective of SAUNA is to create an integrated approach and set of methodologies for safety assessments and preparation of transparent safety demonstrations. This report provides an introduction to structured safety demonstrations of nuclear instrumentation and control and suggests some clarifications to certain terminology and practices. It describes the work in progress that will be continued in the forthcoming projects.

We wish to express our gratitude to the representatives of the organizations involved in the work, and all those who have given their valuable input in the meetings and discussions during the project.

Espoo 27.1.2016

Authors

Contents

Preface..3

Contents..4

1. Introduction..5

1.1 The need for transparent safety justification..5
1.2 Challenges of the current practice..5
1.3 Possible solutions..6
1.4 Goals of this report..6

2. Safety demonstration – the basic idea..6

2.1 What is safety demonstration..6
2.2 Features of a good safety demonstration..9
2.3 Applications of structured safety justification in nuclear I&C....................................10

3. Safety demonstration as part of the licensing process..11

3.1 Overview of the Finnish regulatory practice..12
3.2 Systems engineering and safety demonstration..14
3.3 On the qualification process..17

4. Standards and tools..22

4.1 System life cycle related standards..22
4.1.1 ISO/IEC/IEEE 15288 Systems and software engineering - System life cycle processes..22
4.1.2 ISO/IEC/IEEE 15289 Systems and software engineering - Content of life-cycle information products (documentation)..23
4.1.3 ISO/IEC 24748 Systems and software engineering - Life cycle management23
4.2 Assurance standards and models..24
4.2.1 ISO/IEC 15026 Systems and Software Engineering—Systems and Software Assurance..24
4.2.2 OMG Structured Assurance Case metamodel..26
4.2.3 Assurance case components..27
4.3 Software tools..28

5. Summary and conclusions..31

References..33

Appendix A: Glossary..35

1. Introduction

1.1 The need for transparent safety justification

Several major accidents that have occurred in various domains in recent years have raised fundamental questions about the safety of complex man-made systems. How should these systems be designed, constructed, operated and maintained to keep the risks at an acceptable level, and how to make it without rendering them economically infeasible? In regulated areas, such as nuclear facilities, the authorities demand for a documented justification of safety. Often this means compliance to prescriptive regulations and standards. There are also authorities that rather give the overall goals and leave it to the license applicant to show that all risks have been properly managed. However, due to the dependencies and uncertainties inherent in new technologies, human beings and the natural environment, there are no final answers to the questions about system safety, especially in unexpected situations. Instead, it is about building confidence in that the system can be trusted on, not only by the developers and owners themselves but also by the society and public. For this to be possible, a safety justification should be logically unarguable, unbiased, comprehensive, transparent and accessible to all relevant parties.

These challenges are present in all engineering disciplines and human organisations. In particular, computer software is claimed to introduce new types of dependences and failure mechanisms. As digital Instrumentation and Control (I&C) systems are now commonplace in new nuclear power plants and modernisations of old ones, licensing of safety critical software has become an issue. As stated by a group of regulator's and safety authorities' experts (Common position 2014) the assessment of software cannot be limited to verification and testing of the end product, i.e. the computer code. Other factors such as the quality of the processes and methods for specifying, designing and coding have an important impact on the implementation. Existing standards provide limited guidance on the regulatory and safety assessment of these factors. There is a need to introduce greater consistency and more mutual acceptance into current regulatory practices in various countries. In its report (Common position 2014), the task force defines *safety demonstration* as a set of arguments and evidence elements which support a selected set of claims on the dependability, in particular the safety, of the operation of a system important to safety used in a given plant environment. Evidence is produced throughout the system life cycle, and it evolves with the project. Therefore, a *safety plan* shall be agreed upon at the beginning of the project between the licensor and the licensee to identify how the safety demonstration will be achieved.

1.2 Challenges of the current practice

In nuclear power, safety justification is typically documented in preliminary and final *Safety Analysis Reports* (SAR), applicants own safety assessments and their background material. *Suitability analysis* is the corresponding design artefact in case of individual components like devices and cables. A SAR of a system or whole plant can be seen as a summary of various technical documents and safety analysis results. It describes the design bases and solutions used in system design, primarily to show how the safety requirements have been fulfilled. In addition to licensing purposes, SARs are often used as design specifications internally by the project organisation.

Traditionally, a SAR is a non-structured textual system description with references to other documents, drawings, plans, analysis results and topical reports. In addition, the designer, the applicant and a third party prepare "safety assessments" to demonstrate how the solutions and development processes satisfy the regulatory requirements. According to some studies, arguments showing how the evidence supports the safety claims are not necessarily present in an explicit form (Hauge et al. 2014). On the other hand, safety justifications can be structured but notoriously long, complicated, overly technical and difficult to follow (ONR

2014). The definition of a *safety demonstration* from Common position (2014) above clearly suggests a structured approach. Therefore, the working hypothesis behind this research report has been that there is some place for improvement in justifying the safety or nuclear I&C systems.

1.3 Possible solutions

Justification of safety in one form or another has been traditionally considered critical for the use of nuclear energy. In fact, the idea of explicit, logics-based argumentation has been around for a while (Toulmin 1958), and it has been applied in many critical domains, including nuclear, as structured *safety cases*. Broadening the scope to other critical system properties has led to international standardisation of “assurance cases” (ISO 15026). In nuclear power, a task force of several regulators uses the corresponding term “safety demonstration” (Common position 2014), and in Sweden Elforsk (2013) has published a guide for planning its preparation. In addition to a significant body of literature, international standards (ISO 15026, OMG 2015) and software tools (Linnosmaa 2016) exist for the development, maintenance and exchange of assurance/safety case information.

1.4 Goals of this report

However, as has been seen in several discussions and workshops, the current practice is still far away from the ideal, and there seems to be considerable confusion concerning the key terms. The purpose of this report is to suggest some clarifications. We argue that a more structured approach would be useful in safety justification of nuclear power plant systems, both in terms of confidence building and efficient qualification and licensing processes. There are some needs for improvement in the current practice and also potential solutions to them. However, there has been some debate going on around the usefulness of structured safety cases (Leveson 2011). Moreover, it is not clear how the principles and tools could be adapted to the current Systems Engineering (SE), qualification and licensing processes. Therefore, the main goal of this report is to introduce the basic ideas and applications of structured safety demonstration and to suggest next development steps. Even if safety demonstration is relevant for all power plant elements and engineering disciplines, our focus is on software based I&C systems including both technical (HW, SW) aspects, development processes and human factors in the project organisation.

2. Safety demonstration – the basic idea

2.1 What is safety demonstration

Briefly, herein the term safety demonstration is defined according to the safety critical task force’s definition in (Common position 2014): 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. It is important to note that in this definition, safety demonstration is an artefact, not a process. It is a set of information stored in databases or in human-readable documents.

Sometimes safety demonstration is mixed with the term safety case. Typically safety case is defined as a structured and comprehensive set of documentation providing a convincing argument that a system is safe for a given application in a given environment. Herein the term safety case is used as an informal overall term referring to totality of the safety justification and all the supporting material, see Figure 1. As such, it is more than just claims, arguments and evidences including, for example system description, testing reports, hazards, failure modes and analysis results etc. (see ONR 2013). The term justification is used as a general term, and safety cases and safety demonstrations are its specialisations. Structured safety case is a special application of the (structured) assurance case focussing on safety and based on a defined information model of claims, arguments, evidences, etc. (see Section 4.2.2).

When looking, for example, at the YVL guides, it becomes clear that some sort of justification is required for decisions having potential safety impacts. Reasons and rationale are a key element of transparency and traceability. Therefore, justifications should be explicit and well written. Common position (2014) states that a safety demonstration may or may not use the structured safety case formalism. However, the reasoning should be clearly visible in a well-written safety demonstration.

The term licensing may also be a bit confusing. In the Finnish practise, licensing applies to the whole nuclear power plant. The license applicant prepares the material needed for the license application which is reviewed by the regulator and processed by the government and the parliament. In general, licensing covers several types of licenses related to design and construction of the plant, such as construction license and operation license. However, by definition and usage of the term, “license” covers also several other permissions and authorizations that are needed for construction and operation of a nuclear power plant, e.g. an environmental license. As a process, licensing includes several activities like qualification, planning, issue tracking, and communication and negotiations with the supplier and the regulator. On the regulator’s side, licensing includes activities like communication, analysis of submitted material, decisions, issue tracking, etc.

According to the Finnish Nuclear Energy Decree (Section 112, 732/2008), the licensing documents, such as FSAR (Final Safety Analysis Report), have to be updated every time they are affected by a modification of the plant. They are living documents describing the actual status of affairs.

In practise, the only modification of the plant which has to be licensed is the power uprate, the maximum thermal output of the reactor being one of the few elements mentioned directly in the licenses permitted to the license holder. According to (Raetzke & Micklinghoff 2006) the power uprates in Finnish reactors have been implemented as part of the renewal of the operating license, so there has never been a separate modification procedure that needed political decision making. Any other modifications of the plant which have an effect on safety, and which involve changes in the documents already approved by STUK, have to be approved by STUK before they are carried out. Thus, licensing is literally speaking a rather restricted term in the Finnish practise.

In YVL guides, the term qualification (of systems and components) refers to a process to demonstrate the ability to fulfil specified requirements. As it is defined, qualification is about “demonstrating safety” and therefore carried out by the license applicant together with its contractors. However, the license applicant carries the ultimate responsibility of safety and demonstrating it. So, the process of developing a safety demonstration has currently no established name but it could be called qualification with its broadest meaning. Safety demonstration planning (resulting in a safety demonstration plan or a qualification plan) is part of licensing planning or qualification planning.

YVL guides require that the licensee prepares a Preliminary Safety Analysis Report (PSAR) in the construction license stage of a newbuild project and a Final Safety Analysis Report in the operation license stage. The experience of the authors is that SARs contain a limited amount of explicit safety justification. No detailed requirements are given in the YVL guides on how argumentation should be made (Tommila et al. 2014).

In contrast to the above definitions, Elforsk (2013) interprets safety demonstration as a process more or less equivalent to qualification and calls its result a “safety demonstration case”. In practise, the term licensing is used quite often as a synonym to what qualification means in this document, totally ignoring the political decision making and official granting of a license. Sometimes, outside Finland, the term qualification is used only on component level instead of a system and equipment level.

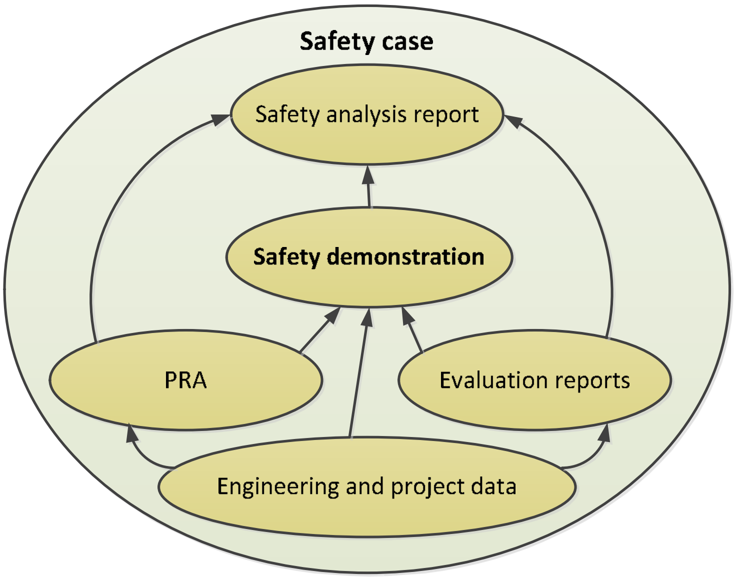


Figure 1. Position of safety demonstration in the overall safety justification material.

In our understanding, safety demonstration is a structured set of information justifying selected claims about system safety. Figure 1 illustrates its role in the totality of qualification material, the “safety case”. Definitions of all key terms in this report can be found in Appendix A. As the work is still in progress (in SAFIR2018), the meaning and relations of some terms may still need clarification and justification. An informal mind map of some concepts is shown in Figure 2.

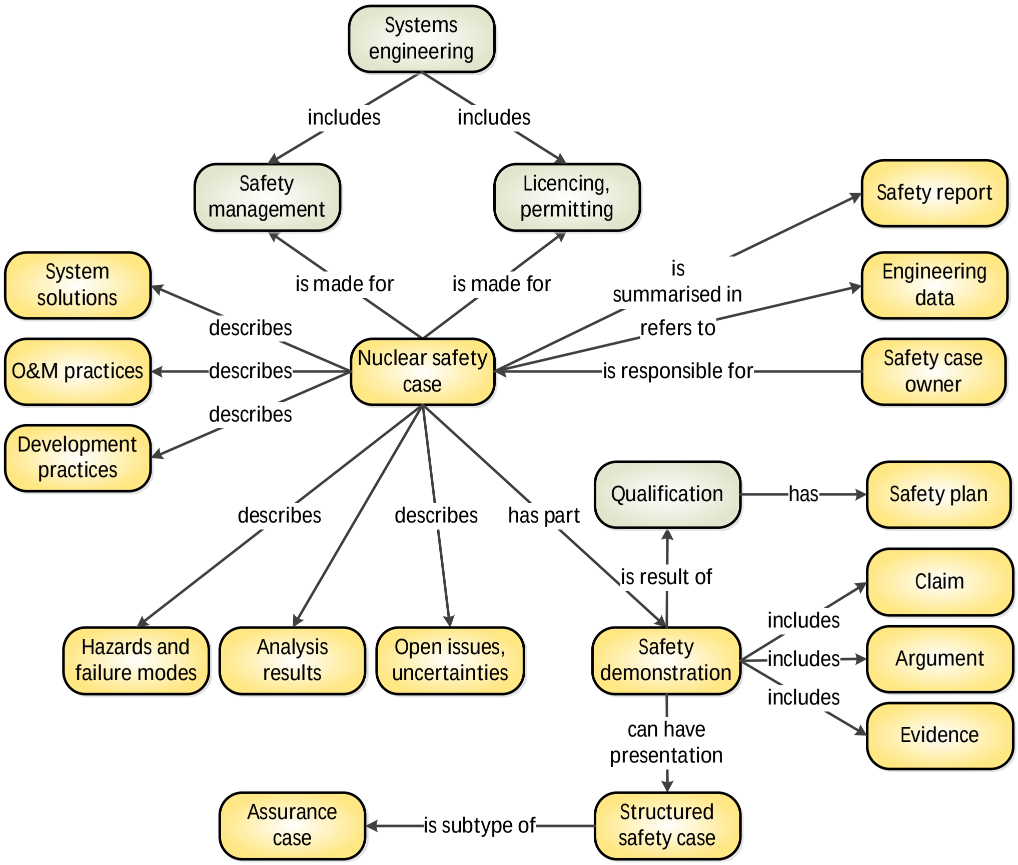


Figure 2. Key concepts related to a nuclear safety case. Artefacts are shown as yellow and processes as green boxes.

2.2 Features of a good safety demonstration

The UK Nuclear Safety Case Forum consists of nuclear site licensees and other companies with nuclear operations in the UK. They have produced guides providing a tool kit of methods and processes that nuclear operators can use if appropriate to their sites and facilities. (ONR 2014) provides guidance on writing safety cases right first time. It should be noted that definitions of terms such as safety case and safety demonstration differ between ONR and this report. However, in this Section we list some features that good safety demonstration (as defined in Section 2.1) should have. The opinions are based on (ONR 2014) and our own experience.

It is essential to establish clear ownership of the safety demonstration. It is expected that the owner is the person who has or will have ultimate responsibility for the safety of the plant and personnel operating it. It is important that the safety demonstration is considered as belonging to the plant and the people who operate and maintain it. The safety demonstration must not be considered as belonging to the authors of the documentation.

In addition to the owner (or a few owners) of the safety demonstration, it is important to involve right persons for generating it. Designers, operators, maintainers, and plant managers represent different views on the plant safety and they should be involved in the development of safety demonstration. Key responsibilities should be identified including how confirmation of the validity of the safety demonstration will be established and who will confirm that the safety demonstration is in line with the current status of the plant or design. People responsible of safety demonstration should be able to identify any relevant learning from experience and ensure that it is appropriately incorporated into the safety demonstration generation process. Any known problems that have been experienced with previous safety demonstrations should be taken into account with proper solutions and mitigations.

Good safety demonstration should focus on what the key users and stakeholders need to know. Overall, it should tell a story. It also should enable to easily identify the key hazards and risks on the plant and how the safety and engineering substantiation are linked together. Safety demonstration should be complete and valid.

The depth of the safety demonstration should be proportionate to the hazards, complexity and safety significance of the assessed operation. Over-pessimism should be avoided because it artificially inflates the significance of a hazard. Also groundless optimism should be avoided. The degree of scrutiny applied to the safety demonstration should be proportionate to the credible conservative consequences of potential accidents, noting that the declared consequences in the safety demonstration are themselves subject to independent review.

A usable, and therefore useful, safety demonstration should be accessible, easy to understand, succinct and document-lite. The term document-lite reflects the need for a focussed, well-structured safety demonstration that clearly presents the safety arguments and the information necessary to operate safely. Technical detail and supporting information should be presented in lower level documentation to avoid overly long and irrelevant justifications. Length can also be the enemy of clarity, so succinctness can improve the understanding of those who read the safety demonstration.

2.3 Applications of structured safety justification in nuclear I&C

As described above, the basic idea of a “structured safety demonstration” is to provide transparent and logically sound evaluation of system safety by arguing explicitly whether the collected evidence supports the selected claims about various safety properties. A safety demonstration is supposed to be unbiased and open-minded with respect to uncertainties in the data and potential weaknesses in the reasoning. The general principles can be applied in various ways, for example by formulating traditional Safety Analysis Reports more carefully or by introducing more formal information models and software tools. As such, the basic idea of structured argumentation is generic and has many potential applications in the nuclear domain, for example:

- Assessment of engineering artefacts, organisations and working processes: Many kinds of safety analyses are required and needed during the design, qualification and licensing of a nuclear power plant. In critical cases, independent third party assessments are also required by the regulatory guides. Just like safety justifications, assessment results should be understandable and unarguable. Application-specific requirements and other criteria of a “good” solution can be taken as claims. Observations from available documentation, interviews and test results provide the evidence. The general criteria and argument structure defines the skeleton of the assessment method. Possible applications include, for example, assessment of:
    - requirement specifications,
    - development processes,
    - safety culture,
    - results of model checking,
    - usability of control rooms,
    - PSA results,
    - compliance with standards and regulations.

- Suitability analysis of equipment and components: The purpose of *suitability analysis* is to show that a device (e.g. instrument, process controller, electrical equipment or cable) is suitable for its intended use in the specified operating environment. In the preliminary version, the specifications, i.e. requirements, are verified prior to procurement actions. The final version ensures that the selected device fulfils its specifications, e.g. on the basis of type tests, supplier audits and operational experiences (see YVL E.7 2013). So, suitability analysis can be seen as a small-scale safety demonstration.

- System-level Safety Analysis Reports: For construction license the applicant shall provide a *Preliminary Safety Analysis Report* (PSAR). It describes how the system has been designed to fulfil relevant regulatory requirements (YVL B.1 2013). The *Final Safety Analysis Report* (FSAR) shall provide an as-built description of the plant prior to the loading of nuclear fuel into the reactor. The final safety analysis report shall be regularly updated during the operation of the nuclear power plant. When modifications are made, the system's *conceptual design plan* shall correspond to that of the preliminary safety analysis report. Additionally, the conceptual design plan shall contain a report on quality management principles. Basically, the information provided by the applicant should allow the regulator to perform a safety assessment of the system. In addition, a safety assessment independent of the designer drawn up by the licensee is required. So, it is possible to see here two potential applications of structured safety demonstration, one by the regulator and another by the license applicant.

- Plant-level Safety Analysis Reports: SARs are written both on system level (above) and plant level. The SAR of the whole plant integrates the descriptions, assessments and safety demonstrations of all plant elements and life-cycle activities. Today, the documentation is typically organised according to the NRC's Standard Review Plan for the Review of Safety Analysis Reports (NUREG-0800 2011). A SAR provides an overview of the plant-wide design principles and the technical implementation of each safety-classified system and its relationship with the overall plant complex (YVL B.1 2013). Furthermore, a SAR shall include the licence applicant's own assessment on how the plant and the participating organisations satisfy Finnish safety and quality requirements. Here, the principles of structured safety demonstration could be useful.

- Assessment of safety demonstrations: Preparing a safety demonstration of a complex system is a challenging process covering the whole system life-cycle. There are many reasons for the safety demonstration to become flawed (see e.g. Greenwell 2006). Therefore, it should be reviewed by an independent party. Therefore, the assessment of a safety demonstration, such as a Safety Analysis Report or Suitability Analysis is itself also a special case of structured safety demonstration.

3. Safety demonstration as part of the licensing process

The previous chapter focussed on safety demonstration as an engineering artefact. The idea of this chapter is to discuss the activities and resources needed to produce a safety demonstration and to get regulatory approval for it.

On plant level, licensing is an authorisation process resulting in a license granted to the license applicant. It includes activities performed both by the regulator and the applicant throughout the whole life-cycle. Nuclear projects normally take a long time (Figure 3). Actions must be carefully planned, and early dialog to clarify regulatory expectations is recommended to minimise licensing and financial risks. Therefore, the applicant should have an overall (multi-step) licensing plan associated with the project plan. Since our focus is on

I&C systems, we mostly use the term qualification instead of licensing. The general background for this discussion is Systems Engineering (SE).

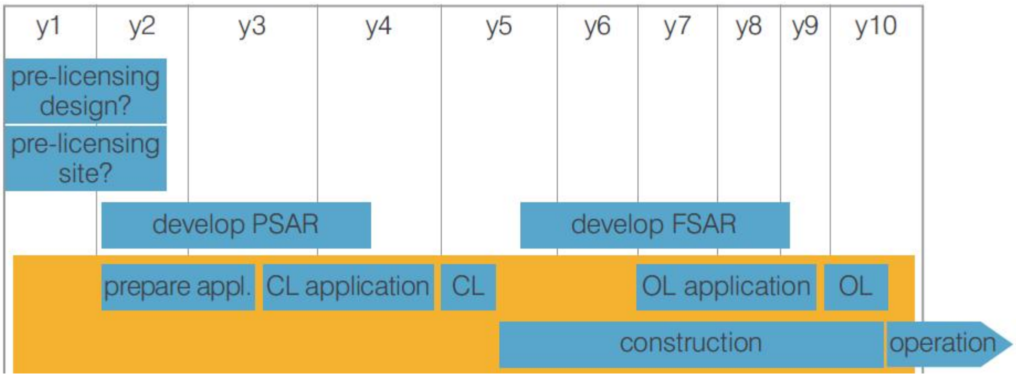


Figure 3. Example of licensing activities and steps for a Nuclear Power Plant (excerpt from WNA 2015, CL=Construction License, OL=Operating License).

3.1 Overview of the Finnish regulatory practice

A regulatory body is an organisation designated by the government of a state as having legal authority for conducting the regulatory process. In Finland it is the Radiation and Nuclear Safety Authority (STUK). Among other tasks it contributes to the processing of applications for licenses, controls compliance with the license conditions, and formulates the detailed requirements for plants, systems and personnel. Compliance is verified through review of documentation and inspections carried out at the plant site or at subcontractors' premises. STUK also inspects the plans for significant plant modifications and oversees the modification work. (www.stuk.fi)

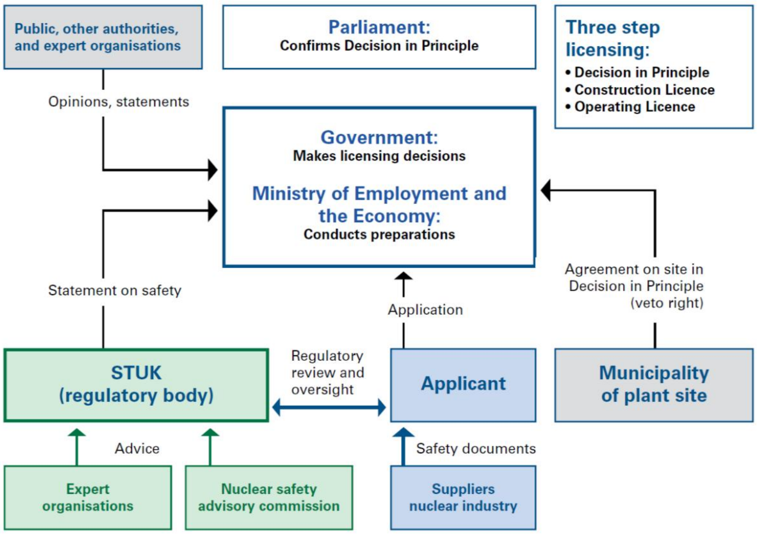

Public, other authorities, and expert organisations
Parliament: Confirms Decision in Principle
Three step licensing:
• Decision in Principle
• Construction Licence
• Operating Licence
Opinions, statements
Government: Makes licensing decisions
Ministry of Employment and the Economy: Conducts preparations
Statement on safety
Application
Agreement on site in Decision in Principle (veto right)
STUK (regulatory body)
Regulatory review and oversight
Applicant
Municipality of plant site
Advice
Safety documents
Expert organisations
Nuclear safety advisory commission
Suppliers nuclear industry

Figure 4. Licensing of nuclear facilities in Finland (STUK 2010).

In Finland, licensing of a whole nuclear power plant takes place in three steps, the *decision-in-principle*, the *construction licence* and the *operating licence*. Participating organisations and information flows are illustrated in Figure 4. The licensee is responsible for ensuring the safety of the nuclear power plant. Before operating the plant, STUK must be provided with documentation proving that the plant was designed and implemented in compliance with safety requirements. In addition, evidence must be provided verifying that the prerequisites exist for safe operation, for example, that personnel has been trained and verified to be competent and that instructions exist for plant operation, maintenance and preparedness arrangements. (Modified from www.stuk.fi.)

In this report we are most interested in I&C and the related “regulatory review and oversight” shown in Figure 4. Even if expressions like “licensing of digital I&C” can be found in the literature, the term *qualification* applies in Finland to I&C and electrical systems and to the components used in them. I&C systems are “licenced as part of the whole plant”. In addition, the term “permitting” is used in some occasions. In new-builds qualification of I&C systems is embedded in the overall licensing process. In general, for example in modifications and upgrades, the qualification is controlled by the system-specific approval *decisions* made by STUK rather than to the plant level licensing steps.

Annex B of YVL A.1 (2013) sets requirements for submission of documents to STUK. Here a document is understood as a set of information in human-perceivable form, for example as textual, graphical, audible presentations and messages. When agreed with STUK, a document can be sent as a hardcopy (on paper) or delivered electronically on a storage media or over a communication network (e.g. e-mail or database access). Documents can be updated and re-submitted as new versions over a longer time period. Submission of formal documents, such as license applications, shall be followed by a covering letter and have a front sheet containing the necessary identifications and status data. A document can be sent for information or for approval. It shall describe the extent and independence of the document review carried out and a justification for the conformance and acceptability. Due consideration shall be given to any information available that can be used for assuring safety. Compliance with regulations and guides does not entitle anyone to ignore information that could yield improved safety or contradict with what is proposed. If the pre-inspection by STUK indicates substantial shortcomings, it will be returned to the licence applicant without closer scrutiny. If so, STUK will suspend the processing of the document and demand additional information. When compliance problems are discovered, STUK raises *issues* to be resolved by the applicant. If the shortcomings are negligible, a normal *request for further clarification* will be made. So, tracking of open issues is an essential activity on both sides.

The amount of information is large. More than three thousand documents were submitted to STUK in 2014 the average review time being about three months and the total work amount about 145 person-years. In its work, STUK uses information technology tools for requirements management and records management. STUK has also launched a project on an electronic service system that offers licensees the opportunity to submit applications to STUK for processing in electronic format. (STUK 2015a)

It is not easy to collect a clear overall picture of the design and qualification activities in the current practice. There are differences in project types (newbuild, modification) and scopes (whole plant, system, component). Terms and requirements are distributed in many standards and regulatory guides. Concerning I&C systems, the communication between the license applicant and the regulator is described especially in YVL guides B.1 and E.7. For electrical and I&C equipment and cables YVL E.7 (2013) gives a good summary of documents to be submitted to STUK at different life cycle phases. In addition, it presents some examples for different cases. As an example, Figure 5 shows the main development steps and the qualification information submitted to STUK. The figure also illustrates the idea that qualification is planned already during the conceptual design phase. Once completed, the preliminary safety or suitability analysis documents, including assessment results and the licensee’s conclusion of suitability, are submitted to STUK for approval or for information depending on the safety class. They shall be accompanied by various documents, such as requirements specification and its independent evaluation, descriptions of the component and its manufacturer, quality and qualification plans, etc.

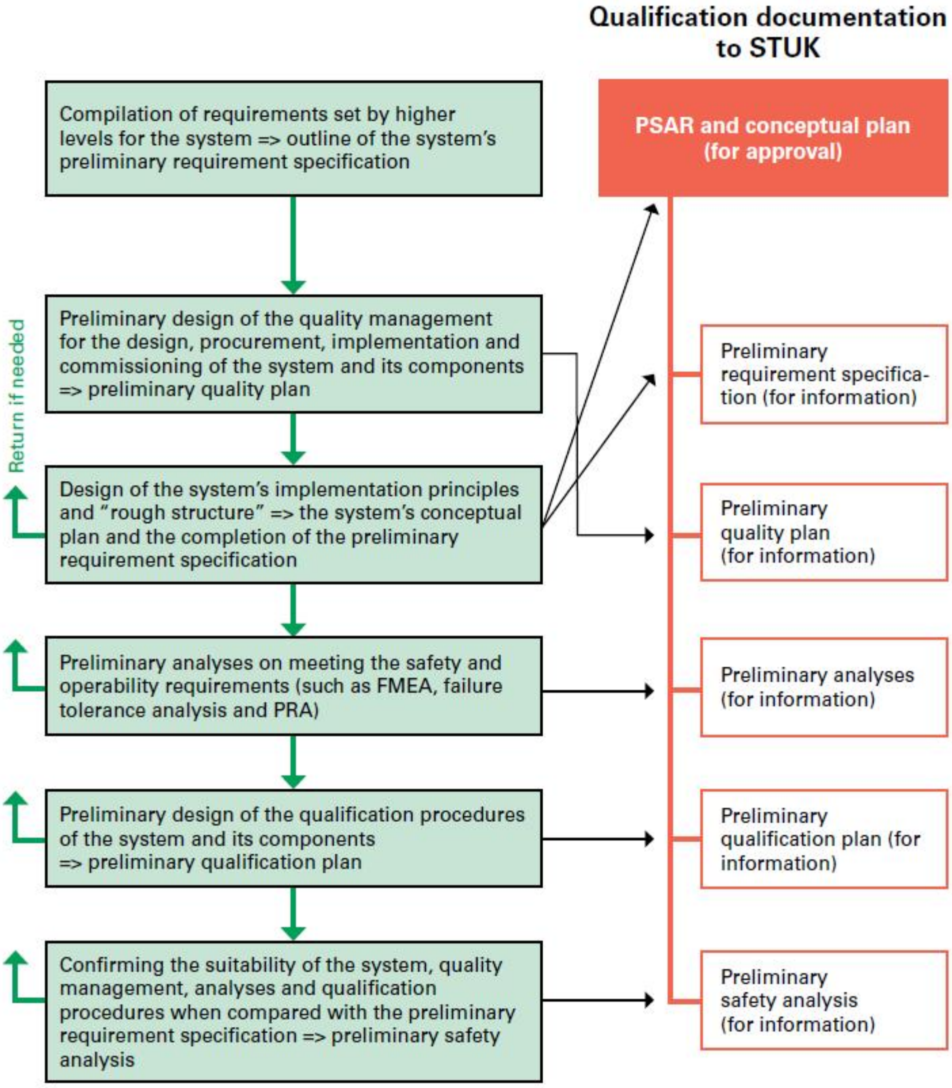

Qualification documentation to STUK
PSAR and conceptual plan (for approval)
Compilation of requirements set by higher levels for the system => outline of the system's preliminary requirement specification
Preliminary design of the quality management for the design, procurement, implementation and commissioning of the system and its components => preliminary quality plan
Design of the system's implementation principles and "rough structure" => the system's conceptual plan and the completion of the preliminary requirement specification
Preliminary analyses on meeting the safety and operability requirements (such as FMEA, failure tolerance analysis and PRA)
Preliminary design of the qualification procedures of the system and its components => preliminary qualification plan
Confirming the suitability of the system, quality management, analyses and qualification procedures when compared with the preliminary requirement specification => preliminary safety analysis
Return if needed
Preliminary requirement specification (for information)
Preliminary quality plan (for information)
Preliminary analyses (for information)
Preliminary qualification plan (for information)
Preliminary safety analysis (for information)

Figure 5. Example of how the design process relates to the preliminary safety report or conceptual plan (YVL E.7 2013).

3.2 Systems engineering and safety demonstration

In the workshops of SAUNA project, it has been discussed whether nuclear industry, especially instrumentation and control area, should pay more attention to Systems Engineering (SE) and how nuclear I&C projects could benefit from systems engineering processes.

The International Council on Systems Engineering (INCOSE, http://www.incose.org) characterises Systems Engineering as an interdisciplinary approach and means to enable the realization of successful systems. In SE, a system is understood as combination of interacting elements organized to achieve their stated purposes. System elements can be, e.g., hardware, software, humans, procedures, facilities or materials (adapted from ISO 15288). These systems are man-made and exist in the real world. They are successful in the sense that they fulfil the actual needs of their stakeholders in the intended environment. Satisfying written requirements may, however, not be enough. SE considers whole systems in their operating environment including their goals and requirements, physical system elements, operation and maintenance processes, as well as the work items (materials, data, etc.) and tools. Therefore, SE involves multiple engineering disciplines and user groups. SE is a systematic and managed but still flexible and iterative approach to engineering. It covers all life cycle stages and all relevant activities like requirements definition, solution synthesis and analysis, modelling and documentation, testing and configuration management. SE focuses on technical processes but is linked to supporting activities like project management and organisational processes.

SE is more or less what nuclear I&C designers are doing. However, that may be done by following long-lived traditions and tied up by regulatory requirements and practices. As often said, there might be lessons to learn from other critical domains. One useful starting point is the well-known standard ISO/IEC/IEEE 15288:2015 *Systems and software engineering – System life cycle processes* (Figure 6). It establishes a common framework for describing the life cycle of systems and defines a set of processes, activities and tasks and associated terminology from an engineering viewpoint. These processes can be applied at any level in the hierarchy of a system's structure. Selected sets of the processes can be applied throughout the life cycle for managing and performing the stages of a system's life cycle. This is accomplished through the involvement of all stakeholders, with the ultimate goal of achieving customer satisfaction.

Standard 15288 also provides processes that support the definition, control and improvement of the system life cycle processes used within an organization or a project. The standard is intended to be used to help an organization to establish its processes; projects to provide products and services; supplier and acquirers to develop agreements on processes and activities; and to serve as a process reference model (PRM) in process assessments.

A system may be configured with one or more of the following system elements: hardware, software, data, humans, processes (e.g., processes for providing service to users), procedures (e.g., operator instructions), facilities, materials and naturally occurring entities. As viewed by the user, they are thought of as products or services.

The implementation of the standard typically involves selecting, extending and tailoring the predefined processes for the purposes of the organization or project. The standard is not specific for any area of industry which makes it generic. For example, it doesn’t explicitly describe the activities of safety justification and licensing in regulated domains. However, a suggestion for its adaptation to nuclear I&C has been made in the SAUNA project by Alanen and Salminen (2016).

It can now be asked what role qualification has in systems engineering and which processes in ISO/IEC/IEEE 15288 support the development of a safety demonstration. ISO/IEC/IEEE 15288 defines four process groups: Agreement processes, Organisational Project-Enabling Processes, Technical Management Processes and Technical Processes (Figure 6).

The Quality Management Process (belonging to the Organizational and Project Enabling Processes group) goes hand in hand together with Quality Assurance Process (Technical Management Processes group). It should be noted that in ISO/IEC/IEEE 15288, quality characteristics include safety, security, reliability and availability, which are among the key features whose presence is to be justified in nuclear systems. While the Quality Assurance Process focuses on providing confidence that quality requirements will be fulfilled, the Quality Management Process acts on higher level planning, defining, assessing, and managing activities. These two processes contain several aspects that are included in the safety demonstration as defined in PLANS (Planning Safety Demonstration) project that is linked to SAFIR programme and funded by the Nordic Nuclear Safety Research forum (NKS, http://www.nks.org/).

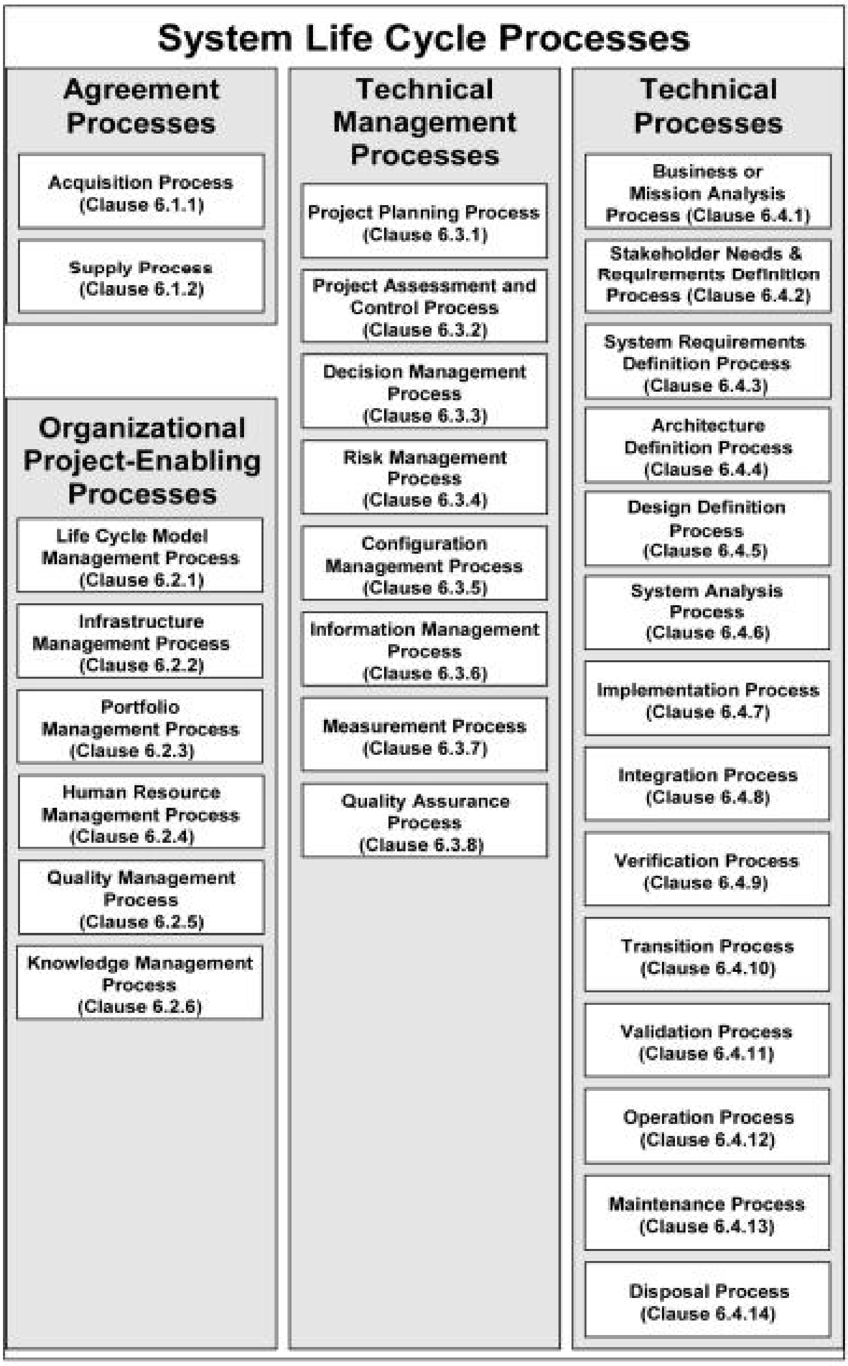

System Life Cycle Processes
Agreement Processes
Acquisition Process (Clause 6.1.1)
Supply Process (Clause 6.1.2)
Organizational Project-Enabling Processes
Life Cycle Model Management Process (Clause 6.2.1)
Infrastructure Management Process (Clause 6.2.2)
Portfolio Management Process (Clause 6.2.3)
Human Resource Management Process (Clause 6.2.4)
Quality Management Process (Clause 6.2.5)
Knowledge Management Process (Clause 6.2.6)
Technical Management Processes
Project Planning Process (Clause 6.3.1)
Project Assessment and Control Process (Clause 6.3.2)
Decision Management Process (Clause 6.3.3)
Risk Management Process (Clause 6.3.4)
Configuration Management Process (Clause 6.3.5)
Information Management Process (Clause 6.3.6)
Measurement Process (Clause 6.3.7)
Quality Assurance Process (Clause 6.3.8)
Technical Processes
Business or Mission Analysis Process (Clause 6.4.1)
Stakeholder Needs & Requirements Definition Process (Clause 6.4.2)
System Requirements Definition Process (Clause 6.4.3)
Architecture Definition Process (Clause 6.4.4)
Design Definition Process (Clause 6.4.5)
System Analysis Process (Clause 6.4.6)
Implementation Process (Clause 6.4.7)
Integration Process (Clause 6.4.8)
Verification Process (Clause 6.4.9)
Transition Process (Clause 6.4.10)
Validation Process (Clause 6.4.11)
Operation Process (Clause 6.4.12)
Maintenance Process (Clause 6.4.13)
Disposal Process (Clause 6.4.14)

Figure 6. System Life Cycle processes in ISO/IEC/IEEE 15288:2015.

The System Analysis Process aims to provide a rigorous basis of data and information for technical understanding to aid decision-making across the life cycle of the system under consideration. It includes utilization of various methodologies, such as mathematical analysis, modelling, simulation, experimentation, to analyse technical performance, system behaviour, feasibility, affordability, critical quality characteristics, technical risks, etc. of a system.

In addition to System Analysis Process, two interesting processes with technical nature are the Verification Process and the Validation Process. Verification Process aims at providing objective evidence that a system or a system element fulfils its specified requirements and characteristics. Validation process provides objective evidence that the system, when in use, fulfils its business or mission objectives and stakeholder requirements, achieving its intended use in its intended operational environment. Configuration Management Process (belonging to Technical Management Processes group) is about managing and controlling system elements and configurations over the life cycle of a system. When looked from an organisational viewpoint, negotiations and communication with the regulator can also be placed under the title Agreement processes (as suggested in Alanen & Salminen 2016).

As safety demonstration gathers results and input from several disciplines and activities, it is difficult or even impossible to state that some of the processes of IEC 15288 would be totally out of scope. However, the processes mentioned above have the biggest contribution to successful I&C qualification.

3.3 On the qualification process

Obtaining a common understanding of the design and qualification process is not straightforward, partly because there are many kinds of applications and projects and partly due to the differences and weaknesses in the terms used. This section discusses some basic concepts and their interpretation in the context of I&C systems and their qualification.

The behaviour of technical systems is usually specified in terms of *functions* (see Tommila & Alanen 2015). *Activities* are a more natural approach for describing human organisations. Activities transform inputs into outputs, for example to new or updated artefacts or states-of-affairs. Activities are enabled by various mechanisms and controlled by constraints (Figure 7).

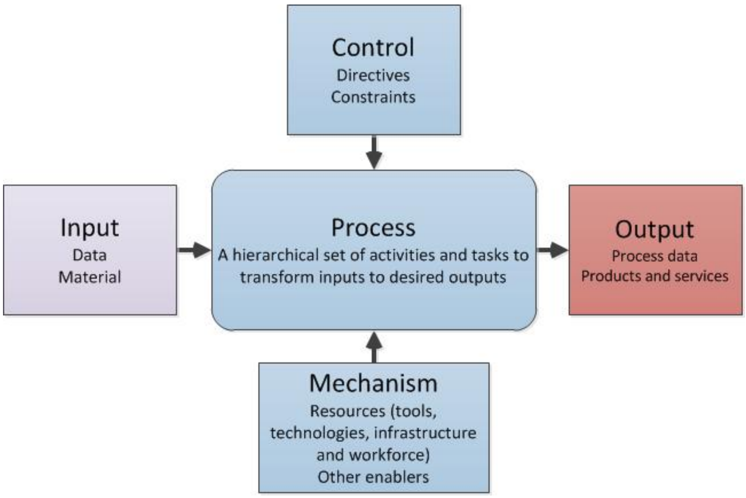

Control
Directives
Constraints
Input
Data
Material
Process
A hierarchical set of activities and tasks to transform inputs to desired outputs
Output
Process data
Products and services
Mechanism
Resources (tools, technologies, infrastructure and workforce)
Other enablers

Figure 7. An approach to structure descriptions of processes and activities (Alanen & Salminen 2016).

Chains of interrelated activities can be called *processes*. In fact, the development of any complex system requires a large network of concrete activities carried out by several organisations over a long time period. Activities are repeated, performed by several participants and used in several processes. Therefore, when we try to define the overall “processes” related to nuclear I&C, we actually speak about *process views* that are selected from the network of all activities for a purpose and according to a specific viewpoint (ISO/IEC/IEEE 15288 2015, ISO/IEC 15026-1 2013).

The definition of an activity focuses on causal relations rather than on timing. In fact, Systems Engineering is necessarily iterative, and activities can be distributed over a long time period and several life-cycle phases and also be performed several times during a project. For project management, the efforts must be organised as consecutive *life-cycle phases* separated by decision gates, *milestones.* A *life-cycle model* describes this work plan on a general level. Unfortunately, a well-founded and commonly accepted life-cycle model for nuclear I&C systems is hard to find. Work towards this direction is going on in the SAUNA project (Alanen & Salminen 2016).

YVL (E.7) uses the ISO definition for *qualification* as a process to demonstrate the ability to fulfil specified requirements (corresponds to the qualification process of the ISO 9000 standard). This is quite similar to *validation* that shall refer to confirmation, through the provision of objective evidence, that the requirements for a specific intended use or application have been fulfilled (also derived from (ISO 9000). Our interpretation is that qualification is a subtype of validation. The difference is that qualification aims to demonstrate safety to an external and in some sense "official" party, which in our case is the regulatory authority. So, in the context of nuclear I&C the term qualification can be interpreted in the following way:

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.

As discussed earlier in Section 2.1, *safety demonstration* is understood as a set of information, i.e. as an artefact or a set of artefacts. According to the definition in (Common position 2014), it has, in principle, a clear structure of claims, arguments and evidences. The actual presentation can, however, have various formats. So, safety demonstration represents the final reasoning needed for safety justification. In the current practice, this information is supposed to be found in a "safety assessment/analysis", i.e. the licence applicant's own assessment on how the system and the participating organisations satisfy the safety and quality requirements.

The expression "qualification documentation" also refers to all kinds of information sent to the regulator for approval or for information. As such, qualification documentation loosely corresponds to our definition of safety case, even if some parts of the safety case may be intended for in-house use only. Some examples from YVL E.7 (2013, Summary of documents to be submitted to STUK at different phases) are:

- Preliminary and final suitability analysis and appendices, e.g.
    - requirement specification, and its evaluation report in safety class 2
    - description of the component and its manufacturer
    - information and plans concerning type approvals and tests
    - summary of the results of factory tests
    - qualification results, and independent review of their acceptability
- Quality plan
- Test plans and schedules for factory acceptance tests and commissioning
- Deviation report of deviations observed during the commissioning inspection.

Having said that qualification is a subtype of validation, we make the observation that an I&C system is validated not only against regulatory safety requirements but also against the operational requirements (cost, availability, functionality, maintainability) of the plant owner itself. Consequently, the qualification documentation is part of a larger "V&V documentation". Only part of all this material is relevant to the regulator.

A *qualification plan* shall be prepared and implemented for the system to guide the qualification process. According to YVL B.1 (2013), a qualification plan shall present the data generated in the quality assurance stages, the external assessments, tests and analyses to be used, the documentation to be produced and submitted for regulatory review and a qualification roadmap complete with estimated timetables and dependencies. So, qualification plan seems to correspond to the term *safety (demonstration) plan* in (Elforsk 2013).

The definition of qualification implies that the license applicant and its suppliers have the main responsibility in producing the safety demonstration and its background material, i.e. the safety case. However, there should be an ongoing dialogue with the regulator right from the beginning. In addition, the regulator, possibly with the help of a technical support organisation (TSO), reviews the submitted material, requests clarifications or modifications and makes decisions on approval of design solutions and documentation. Therefore, we consider also the regulator as a participant in the qualification process.

Processes and activities are carried out by physical resources, such as organisations, persons and tools. Each of them has a specific *role* with respect to an activity and its outcomes. In an actual project, roles are allocated to individual persons and participating organisations. When the principle of Defence in Depth (DiD, see Tommila & Papakonstantinou 2016) is applied to the design organisation, there is a need for several independent and diverse organisational layers to protect against design errors. Definitions of relevant roles, e.g. in terms of work content and required competencies and independence, are necessary for a comprehensive description of the qualification process and actual qualification planning. These roles can be classified in several dimensions, e.g. according to the nature of the doing or the responsible organisation. This is a possible topic for further research, where existing literature (e.g. Shear 1996, http://sebokwiki.org/wiki/Roles_and_Competencies) can be adapted to our domain. A taxonomy of systems engineering roles in nuclear I&C might include, for example, following roles:

- Manager: Guides organisations and people in achieving agreed goals
  - Project manager
  - Safety manager
- Developer: Produces the technical and organisational solutions
  - Requirements engineer
  - System architect
  - Designer
- Assessor: Evaluates the results produced by other roles
  - Verifier/validator
  - Reviewer
  - Tester
  - Qualifier
  - Certifier
  - Inspector
  - Approver
- Regulator: Legal authority that oversights system design, construction and operation
  - Nuclear safety
  - Environment
  - Occupational safety and health

It should be noted that these general roles are named so that they are independent of the performing organisation. For example, there can be applicant's assessors, third party assessors and regulator's assessors involved in an I&C project.

As shown in Figure 8, activities related to permitting power plants and their systems are carried out in several organisations. Typically activities can be divided into planning and execution, of course complemented with progress monitoring, assessment and feedback loops. As qualification is a process carried out by the regulatory body and the license applicant, it is a network of activities carried out in several organisations. According to the Defence in Depth principle there are independent “defence lines” in the supply chain. While design solutions are produced by designers and suppliers, the results must be assessed (e.g. reviewed and tested) by sufficiently independent teams. In a similar fashion, when V&V results are used as evidence in a safety justification, they must be independently interpreted and evaluated by the qualification team. Finally also the qualification results should be critically evaluated, e.g. by a third party assessor (see Kelly 2007).

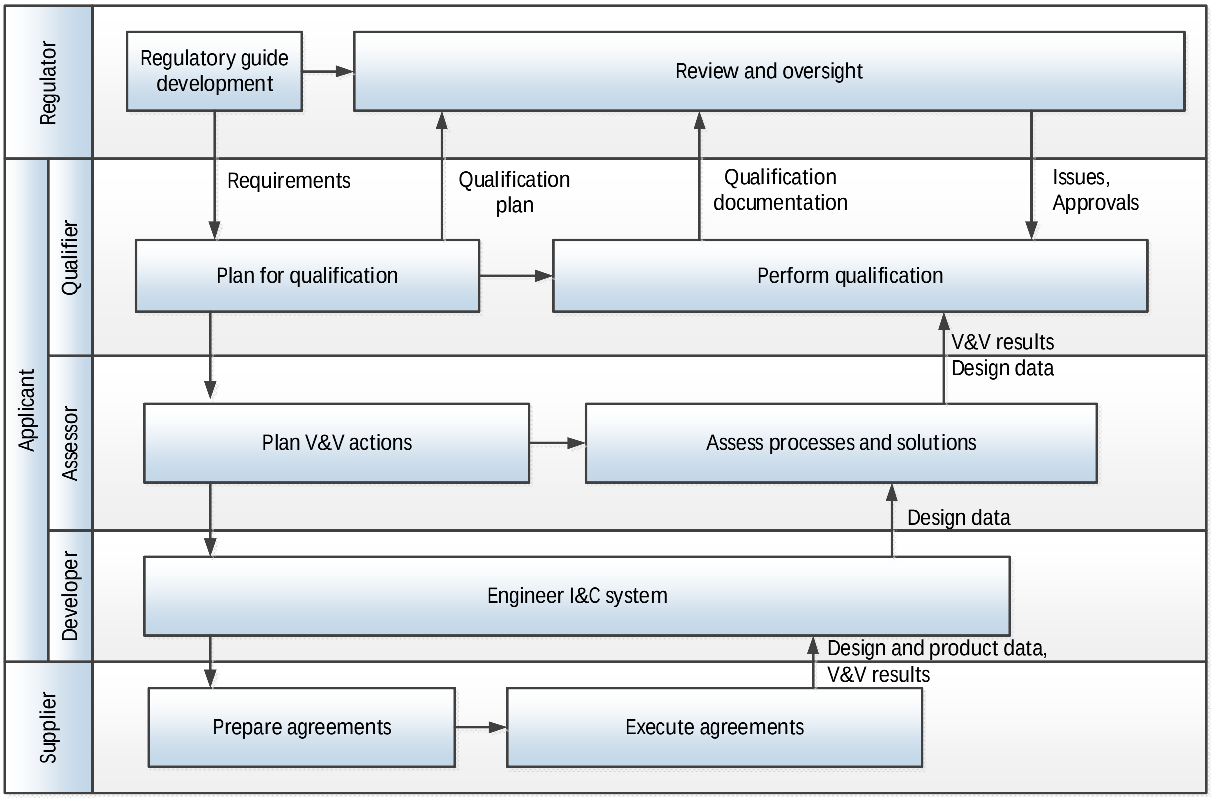


Figure 8. Overview of activities and organisations in I&C qualification.

In general, qualification is a process that takes regulatory requirements and expectations and design and V&V documentation as its inputs and prepares a safety justification. There are different ways to divide the qualification process into activities and concrete tasks. Due to the iterative character of design and the definition of an “activity” as a transformation not tied to the time-line, the most natural basis for decomposition is the purpose and content of an activity. Then activities can be chained according to their causal relationships, i.e. to information (and other) flows between them. So, the main activities in qualification might be outlined as follows:

- Plan for qualification (-> qualification plan)
    - Identify regulatory requirements and expectations
    - Identify applicable standards and guidelines
    - Define overall qualification strategy
    - Define claim-argument structure and required evidences
    - Define qualification activities, resources and schedule

- Perform safety justification (-> safety demonstration/”safety analysis”)
    - Identify and record necessary evidences
    - Evaluate evidences (request for additional V&V if necessary)
    - Derive and argument truth of claims
- Assess qualification results (-> assessment results)
    - Define assessment criteria and approach
    - Perform assessment
- Obtain regulatory approval (-> change requests, requests for clarification)
    - Agree about actions and schedule (e.g. regulatory inspections at site)
    - Submit qualification documentation
    - Manage decisions and track open issues

Figure 9 shows the main qualification activities and information flows in the format introduced above in Figure 7. Please note that this presentation describes the progression of time only implicitly.

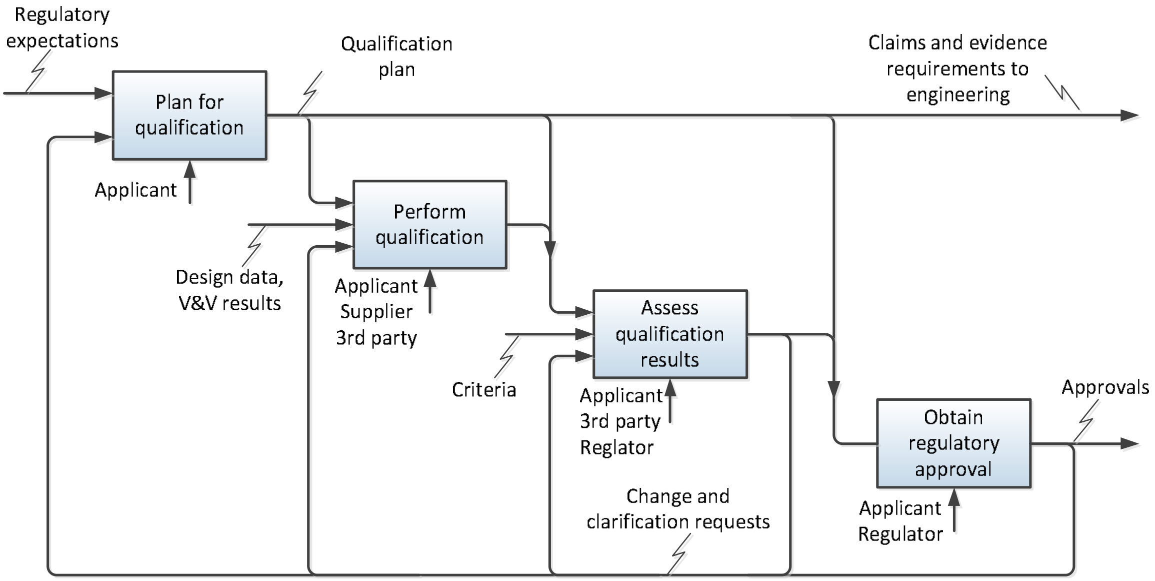


Figure 9. A decomposition of qualification into activities.

To sum up the discussion above, Figure 10 illustrates some of the main concepts as an informal mind map. Definitions of key terms can be found in Appendix A.

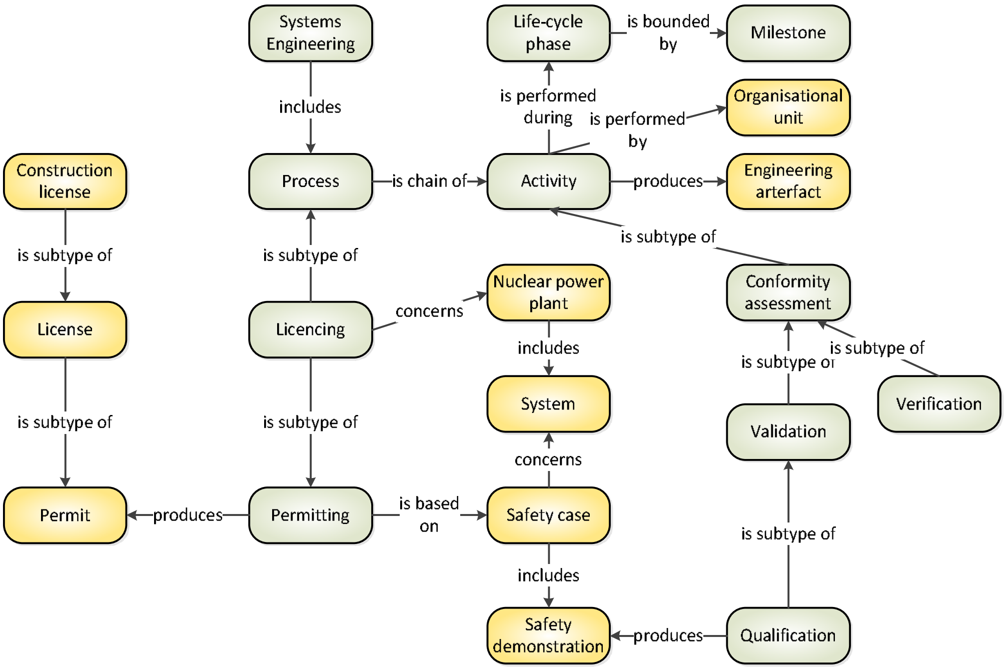


Figure 10. Some concepts related to the system life-cycle.

4. Standards and tools

As examples of ongoing international activities relevant for safety demonstration this chapter provides insight to the applicable systems and software engineering and assurance standards and their development phases. Each standard is briefly described with emphasis on its purpose and possible use for safety demonstration and qualification.

First, the standard ISO/IEC/IEEE 15288 on system life cycle processes is presented together with several supporting standards. Next, the main assurance standard ISO/IEC 15026 and the assurance case information model by OMG are introduced in Section 4.2. Finally, available software tools are reviewed in Section 4.3.

4.1 System life cycle related standards

4.1.1 ISO/IEC/IEEE 15288 Systems and software engineering - System life cycle processes

As said earlier, qualification is part of Systems Engineering and linked to many other technical and management activities. Therefore, Systems Engineering processes must be understood as the context of qualification. Systems Engineering and the standard ISO/IEC/IEEE 15288 were introduced in above Section 3.2 along with a figure of system life cycle processes (Figure 6). This section gives a more detailed description of the standard.

The standard ISO/IEC/IEEE 15288:2015 applies to the full life cycle of systems, including conception, development, production, utilization, support and retirement of systems, and to the acquisition and supply of systems, whether performed internally or externally to an organization. The life cycle processes of this standard can be applied concurrently, iteratively and recursively to a system and incrementally to its elements. The standard does not prescribe a specific system life cycle model, development methodology, method, model or technique. The users of 15288 are responsible for selecting a life cycle model for the project and mapping the described processes, activities, and tasks into that model. The parties are also responsible for selecting and applying appropriate methodologies, methods, models and techniques suitable for the project.

The standard is compatible with the quality management system provided by ISO 9001, the service management system provided by ISO/IEC 20000-1, and the information security management system provided by ISO/IEC 27000.

The 15288 groups the activities that can be performed during the life cycle of a system into four process groups: Agreement Processes; Organizational Project-Enabling Processes; Technical Management Processes; and Technical Processes. Each life cycle process is described in terms of its purpose and outcomes. Activities and tasks that need to be performed to achieve the outcomes are defined. The four process groups and 30 processes are illustrated in Figure 6.

The current version of the standard was published in May 2015 and it has reached wide acceptance throughout the industry and other standardization bodies. Therefore, it can be expected to stay stable for at least the next five years until the systematic review date.

4.1.2 ISO/IEC/IEEE 15289 Systems and software engineering - Content of life-cycle information products (documentation)

The ISO/IEC/IEEE 15289:2015 standard provides requirements for identifying and planning the specific information items (information products, documentation) to be developed and revised during systems and software life cycles and service processes. It specifies the purpose and content of all identified systems and software data records and life-cycle information items, as well as records and information items for information technology service management. The information item contents are defined according to generic document types (description, plan, policy, procedure, report, request, and specification) and the specific purpose of the document. For simplicity of reference, each information item is described as if it were published as a separate document. However, information items may be unpublished but available in a repository for reference, divided into separate documents or volumes, or combined with other information items into one document. 15289 is based on the life-cycle processes specified in ISO/IEC 12207 and 15288, and the service management processes specified in ISO/IEC 20000. Currently, the standard is under review to accommodate the changes in the 15288 latest revision.

4.1.3 ISO/IEC 24748 Systems and software engineering - Life cycle management

The 24748 standard is a multipart standard with six parts. It provides guidance for the application of the system and software life cycle processes.

ISO/IEC TR 24748-1:2010 Systems and software engineering - Life cycle management - Part 1: Guide for life cycle management

Part 1 provides information on life cycle concepts and descriptions of the purposes and outcomes of representative life cycle stages. It also illustrates the use of a life cycle model for systems in the context of ISO/IEC/IEEE 15288. In addition, it provides detailed discussion and advice on adapting a life cycle model for use in a specific project and organizational environment. It further provides guidance on life cycle model use by domains, disciplines and specialties. This standard is under review and to be published next as a draft IS.

ISO/IEC TR 24748-2:2011 Systems and software engineering - Life cycle management - Part 2: Guide to the application of ISO/IEC/IEEE 15288 (System life cycle processes)

Part 2 addresses system, life cycle, process, organizational, project, and adaptation concepts, principally through reference to Part 1 and 15288. It also gives guidance on applying the 15288 standard from the aspects of strategy, planning, application in organizations, and application on projects. The standard is under review and will be published next as a Technical Specification (TS).

ISO/IEC TR 24748-3:2011 Systems and software engineering - Life cycle management - Part 3: Guide to the application of ISO/IEC 12207 (Software life cycle processes)

Part 3 is a guide for the application of ISO/IEC 12207:2008. It addresses system, life cycle, process, organizational, project, and adaptation concepts, principally through reference to Part 1 and 12207. It gives guidance on applying the 12207 standard from the aspects of strategy, planning, application in organizations, and application on projects. The standard is under review and will be published as a Technical Specification (TS), similar to Part 2.

ISO/IEC/IEEE FDIS 24748-4 Systems and software engineering - Life cycle management - Part 4: Systems engineering planning

Part 4 provides guidance for the execution of the 15288 processes that are required for planning and managing a project to implement a significant systems engineering effort. It also provides normative definition of the content and recommendations for the format of the related information item, the project's Systems Engineering Management Plan (SEMP).

This standard replaces the former ISO/IEC 26702:2007 (IEEE Std 1220-2005), Systems engineering - Application and management of the systems engineering process. Next, the standard goes to ballot for an International Standard that should be published in 2016.

ISO/IEC/IEEE CD 24748-5 Systems and software engineering - Life cycle management - Part 5: Software development planning

Part 5 focuses on the processes required for successful planning and management of the project's software development effort and for development of the software development plan (SDP) as a vehicle for representing a project's application of software life cycle processes. The SDP is a top level technical planning document for a project which addresses technical management processes established by three principal sources (the project’s contract, applicable organizational processes, and the software development project team) as necessary to successfully accomplish the software development related tasks of the project. The standard is under development and the next step is a Draft International Standard ballot (DIS).

ISO/IEC/IEEE PDTS 24748-6 Systems and software engineering - Life cycle management - Part 6: System integration engineering

Part 6 describes the integration engineering activities dealing with planning, performing, managing the integration of a system, including the related activities of other technical processes, in particular verification and validation processes. These are real practices in industry, i.e., the integration of a system is technically engineered and managed as a project (included in the system development project). Although these practices are performed, they are not formalized in a standard today. This standard facilitates the use of the 15288 Integration process. The standard is under development and is planned to be published as a Technical Specification late 2016.

4.2 Assurance standards and models

4.2.1 ISO/IEC 15026 Systems and Software Engineering—Systems and Software Assurance

ISO/IEC 15026 Systems and software assurance standards use a specific definition for assurance as being grounds for justified confidence. The appropriate valid arguments and evidence to establish a rational basis for justified confidence in the relevant claims about the system’s properties need to be made. These properties may include aspects like future costs, behaviour, and consequences. Throughout the life cycle, adequate grounds need to exist for justifying decisions related to ensuring the design and production of an adequate system and to be able to place reliance on that system. The 15288 standard refers to 15026 for system and software assurance guidance, particularly in the Technical Processes.

The on-going renewal of 15026 aims to unify the concepts related to integrity levels with other international standards, especially IEC 61508 and ISO 26262. The set of 15026 standards consists of four parts.

The assurance case is relevant to some extent in all parts. Part 2 concentrates on the contents and structure of the assurance case. Part 3 relates integrity levels to their role in assurance cases, and Part 4 provides details on integrating the assurance case into the system life cycle processes.

ISO/IEC 15026-1:2013 Part 1: Concepts and vocabulary

Part 1 defines assurance-related terms and establishes an organized set of concepts and their relationships. It provides information to users of the subsequent parts of ISO/IEC 15026, including the use of each part and the combined use of multiple parts.

Part 1 is to be updated whenever other parts change their vocabulary. Currently, a corrigenda caused by 15026-3 revision is being prepared.

ISO/IEC 15026-2:2011 Part 2: Assurance case

Part 2 specifies minimum requirements for the structure and contents of an assurance case to improve the consistency and comparability of assurance cases and to facilitate stakeholder communications, engineering decisions, and other uses of assurance cases.

An assurance case includes a top-level claim for a property of a system or product (or set of claims), systematic argumentation regarding this claim, and the evidence and explicit assumptions that underlie this argumentation. Arguing through multiple levels of subordinate claims, this structured argumentation connects the top-level claim to the evidence and assumptions.

Assurance cases are generally developed to support claims in areas such as safety, reliability, maintainability, human factors, operability, and security, although these assurance cases are often called by more specific names, e.g. safety case or reliability and maintainability (R&M) case.

The purpose of an assurance case is to improve assurance communications by informing stakeholders' decision-making and supplying grounds for needed stakeholder confidence. The most common use of an assurance case is to provide assurance about system properties to parties not closely involved in the system's technical development processes. Such parties may be involved in the system's certification or regulation, acquisition, or audit. Usually, an assurance case addresses the reasons to expect and confirm successful production of the system, including the possibilities and risks identified as difficulties or obstacles to developing and sustaining that system.

Part 2 waits for the systematic review cycle in 2016; no major changes are expected.

ISO/IEC 15026-3:FDIS Part 3: System integrity levels

Part 3 specifies the concept of integrity levels with corresponding integrity level requirements that are required to show the achievement of the integrity level. It places requirements on and recommends methods for defining and using integrity levels and their corresponding integrity level requirements. It covers systems, software products, and their elements, as well as relevant external dependences. One important use of integrity levels is by suppliers and acquirers in agreements; for example, to aid in assuring safety, financial, or security characteristics of a delivered system or product.

Part 3 of ISO/IEC 15026 first establishes an integrity level framework. The remainder of the standard covers defining integrity levels, using integrity levels, determining system or product integrity levels using risk analyses, assigning system element integrity levels, meeting integrity level requirements using evidence, and agreements and approvals involving authorities.

Part 3 has just passed its final draft (FDIS) ballot and is expected to be published in 2016.

ISO/IEC 15026-4:2012 Part 4: Assurance in the life cycle

Part 4 gives guidance and recommendations for conducting selected processes, activities and tasks for systems and software products requiring assurance claims for properties selected for special attention, called critical properties. It specifies a property-independent list of processes, activities and tasks to achieve the claim and show the achievement of the claim.

Part 4 provides a 15288-type process view for systems and software assurance by providing a statement of purpose and a set of outcomes suitable for systems and software assurance. A process view includes a statement of purpose and outcomes, but does not include activities and tasks. Instead, the description includes guidance and recommendations explaining how the outcomes can be achieved by employing the activities and tasks of the various processes in ISO/IEC 15288 and ISO/IEC 12207 (Software life cycle processes).

Part 4 will be updated and a working draft is currently in preparation.

4.2.2 OMG Structured Assurance Case metamodel

The Object Management Group (OMG) has specified a set of metamodels to enable information exchange related to systems assurance. The models provide a tool-oriented approach and use ISO/IEC 15026 as a normative reference. The focus is on software-intensive systems.

OMG Structured Assurance Case Metamodel (SACM) Version 1.1 (Jul. 2015)

The specification defines a metamodel for representing structured assurance cases. In this specification, Assurance Case is a set of auditable claims, arguments, and evidence created to support the claim that a defined system/service will satisfy the particular requirements. Assurance case is a document that facilitates information exchange between suppliers and acquirers, and between the operator and regulator, where the knowledge related to the safety and security of the system is communicated in a clear and defendable way. Assurance case represents the scope of the system, the operational context, the claims, the safety and/or security arguments, along with the corresponding evidence.

Systems Assurance is the process of building clear, comprehensive, and defensible arguments regarding the safety and security properties of systems. The vital element of Systems Assurance is that it makes clear and well-defined claims about the safety and security of systems. Certain claims are supported through reasoning. Reasoning is expressed by explicit annotated links between claims, where one or more claims (called sub-claims) when combined provide inferential support to a larger claim. Certain associations between claims and subclaims are justified. Justification explains the selection of argument strategy Claims are propositions which are expressed by statements in some natural language. The degree of precision in formulation of the claims may contribute to the comprehensiveness of an assurance case. The context is important to communicate the scope of the claim, and to clarify the language used by the claim by providing necessary definition and explanations. Context involves assumptions made about the system and its environment. Explicit statement of the assumptions contributes to the comprehensiveness of the argument. Argumentation flow between claims is structured to facilitate communication of the entire assurance case.

The specification also defines a metamodel for representing structured arguments. A convincing and valid argument that a system meets its assurance requirements is at the heart of an assurance case, which also may contain extensive references to evidence. The Argumentation Metamodel facilitates projects by allowing them to effectively and succinctly communicate in a structured way how their systems and services are meeting their assurance requirements. The scope of the Argumentation Metamodel is therefore to allow the interchange of structured arguments between diverse tools by different vendors. Each Argumentation Metamodel instance represents the argument that is being asserted by the stakeholder that is offering the argument for consideration.

Additionally, the specification provides a metamodel for collecting, developing, evaluating, communicating, and managing Evidence (referred to as the SACM Evidence Metamodel). Specifically, this Evidence Metamodel does all of the following:

- Identifies the main factors that determine the evidence collection process.
- Identifies the main factors that determine the evaluation of evidence.
- Identifies and defines the elements of evidence.
- Defines a common interchange format to facilitate the exchange of information between different Software Assurance tools and services.

The SACM Evidence Metamodel defines a catalogue of elements for constructing and interchanging precise statements related to evidence in support of various assurance efforts. This specification facilitates development of a new type of Assurance tools related to assurance of safety and security of software-intensive systems, and automation of the processes of regulatory compliance and risk assessments.

The SACM Evidence Metamodel provides the basis for logical design of easily-constructed tools for storing, managing, cross-referencing, evaluating, and reporting the elements of evidence during assurance efforts.

4.2.3 Assurance case components

Assurance case components are described both in the ISO/IEC 15026 Part 2 and the OMG SACM specification. Part 2 gives a mathematically oriented recursive definition of the set of assurance cases, while the SACM provides a more tool-oriented metamodel for assurance cases. In general, an assurance case consists of claims, arguments, evidence, justifications, and assumptions.

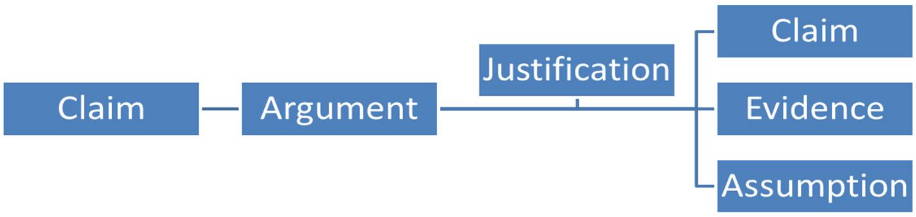


Figure 11. Assurance case components

ISO/IEC 15026 Part sets requirements for the assurance case components:

a) The components of an assurance case shall be unambiguous, identifiable, and accessible.
b) Each component shall be uniquely identified and shall be able to have its origin identified, its history ascertained, and its integrity assured.

c) For each component, the component's contents, the information related to it, and the other components with which it has relationships shall be identifiable and accessible.
d) An assurance case shall contain the auxiliary contents that ISO/IEC 15289 requires for this type of documentation.

Additionally, there are requirements for the structure of an assurance case:

a) An assurance case shall have one or more top-level claims that are the ultimate goals of its argumentation.
b) An argument shall be supported by one or more claims, evidence, or assumptions.
c) A claim shall be supported either by just one argument, or by one or more claims, evidence, or assumptions.
d) A claim, argument, evidence, or assumption shall not support itself either directly or indirectly.

The OMG SACM defines object models for Structured Assurance Case, Argumentation, and Evidence using class diagrams. An example below shows the root object of an assurance case, the AssuranceCase element.

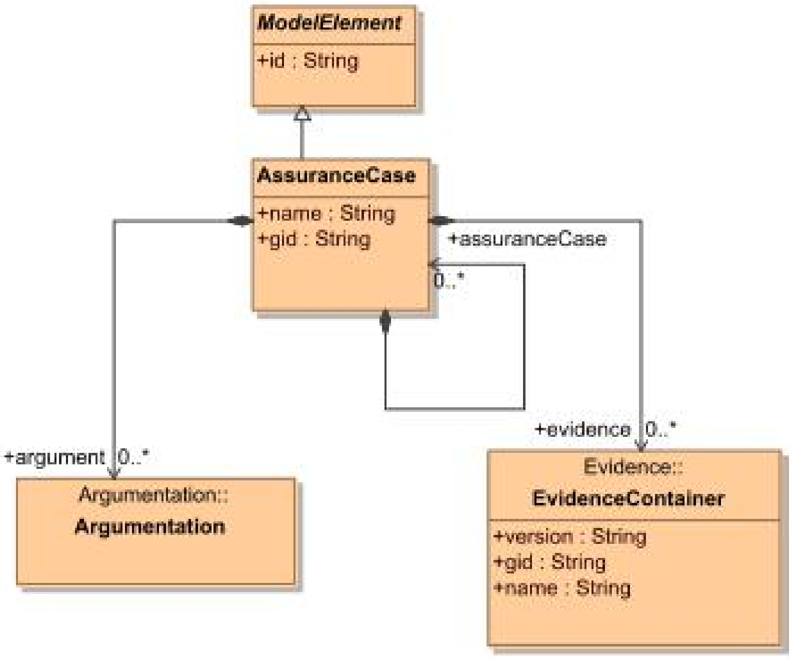


Figure 12. AssuranceCase element

The OMG SACM metamodels are aimed to standardize the structure and format of data in the tools used to support assurance cases. This facilitates information exchange between the tools.

4.3 Software tools

The safety demonstration process in complex projects, such as constructing a nuclear power plant, produces a considerable number of safety related documents. Like mentioned previously, the safety justification should be logically unarguable, unbiased, comprehensive, transparent and accessible to all relevant parties. All this brings forth challenges for creating a safety demonstration artefact which complies with the requirements. Thus, an emerging trend in many safety critical areas is to use structured safety cases for justifying the safety of a system or a process. The only practical way of presenting all this material and creating a safety demonstration in a structured way is using a software tool which supports creation of structured safety cases.

Fortunately, tools for creating structured safety cases are available (Linnosmaa 2016). First these tools were mostly add-ons or plugins for popular modelling tools such as MS Visio or Eclipse, but at the moment there are also available stand-alone software tools which are just focused on creating safety/assurance cases. Figure 13 and Figure 14 below are examples of such tools; Assurance and Safety Case Environment ASCE by company called Adelard and Astah GSN by Change Vision Inc. Safety case tools support creation and management of structured safety cases, often by using a recognised notation such as Goal Structuring Notation (GSN) or Claims-Arguments-Evidence (CAE). Goal Structuring Notation even has its own community standard which is being updated to meet the growing requirements.

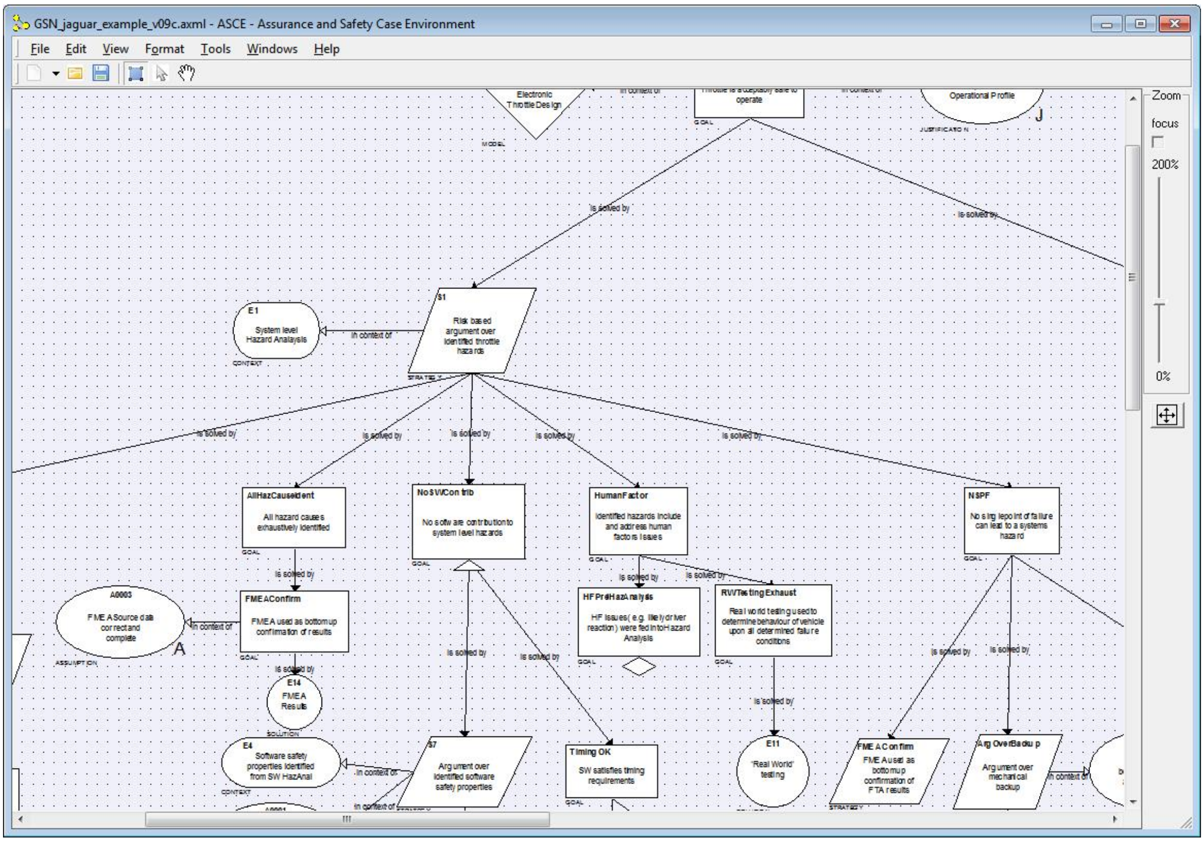

GSN_jaguar_example_v09c.axml - ASCE - Assurance and Safety Case Environment
File
Edit
View
Format
Tools
Windows
Help
Zoom
focus
200%
0%
Electronic Throttle Design
MODEL
in context of
operate
GOAL
Operational Profile
J
JUSTIFICATION
is solved by
E1
System level Hazard Analaysis
CONTEXT
in context of
S1
Risk based argument over identified throttle hazards
STRATEGY
AllHazCauseIdent
All hazard causes exhaustively identified
GOAL
NoSWContrib
No software contribution to system level hazards
HumanFactor
Identified hazards include and address human factors issues
NSPF
No single point of failure can lead to a systems hazard
A0003
FMEA Source data correct and complete
A
ASSUMPTION
FMEAConfirm
FMEA used as bottomup confirmation of results
HFPreHazAnalysis
HF issues(e.g. likely driver reaction) were fed into Hazard Analysis
RWTestingExhaust
Real world testing used to determine behaviour of vehicle upon all determined failure conditions
E14
FMEA Results
SOLUTION
E4
Software safety properties identified from SW HazAnal
S7
Argument over identified software safety properties
Timing OK
SW satisfies timing requirements
E11
'Real World' testing
FMEAConfirm
FMEA used as bottomup confirmation of FTA results
STRATEGY
Arg OverBackup
Argument over mechanical backup

Figure 13. Safety case using CAE notation done with ASCE.

Safety case or assurance case tools offer features which help the end user gathering and preparing a structured safety case. One clear benefit is visually, or in some cases using hierarchical text (Figure 15), linking the evidence to the supported claims, with justified argumentation giving the reasoning in between. This helps representing the arguments and the justification behind claims and related evidence in a way it is easier for all stakeholders to follow and understand. Software tool can also provide the potential for reducing the amount of free text and the possibility to use more controlled language for expressing the argument. Of course the tool only gives the possibility of doing this, but in the end it is up to the user to write the safety case and actually make it a good safety demonstration.

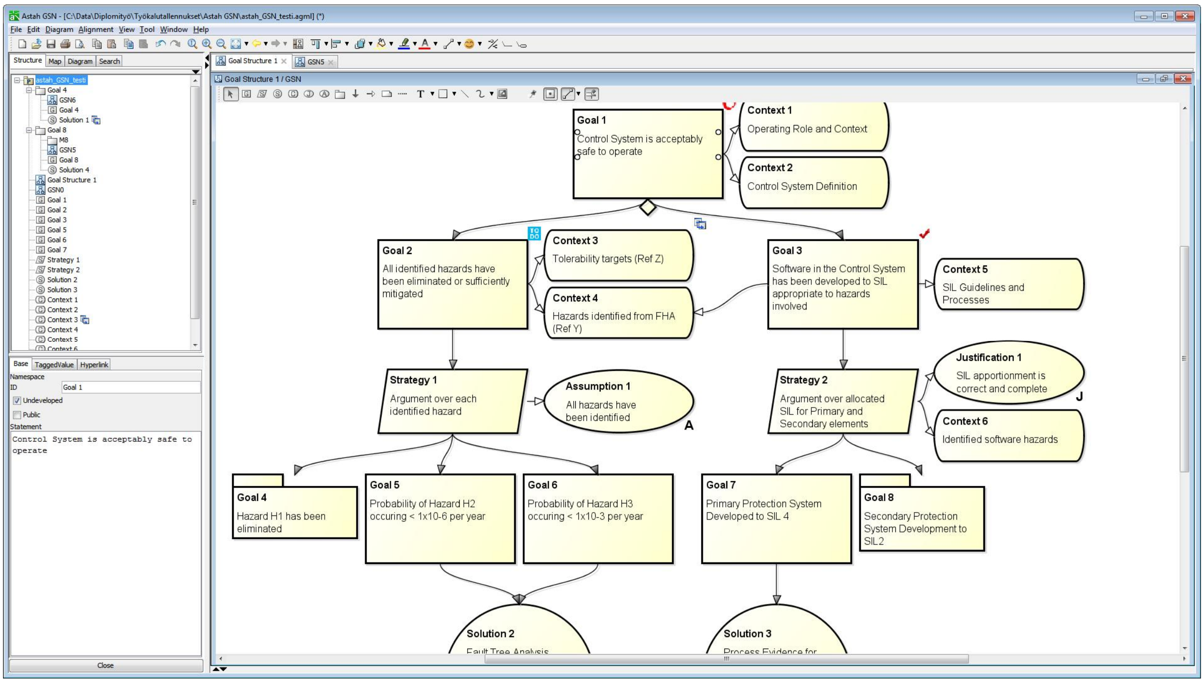
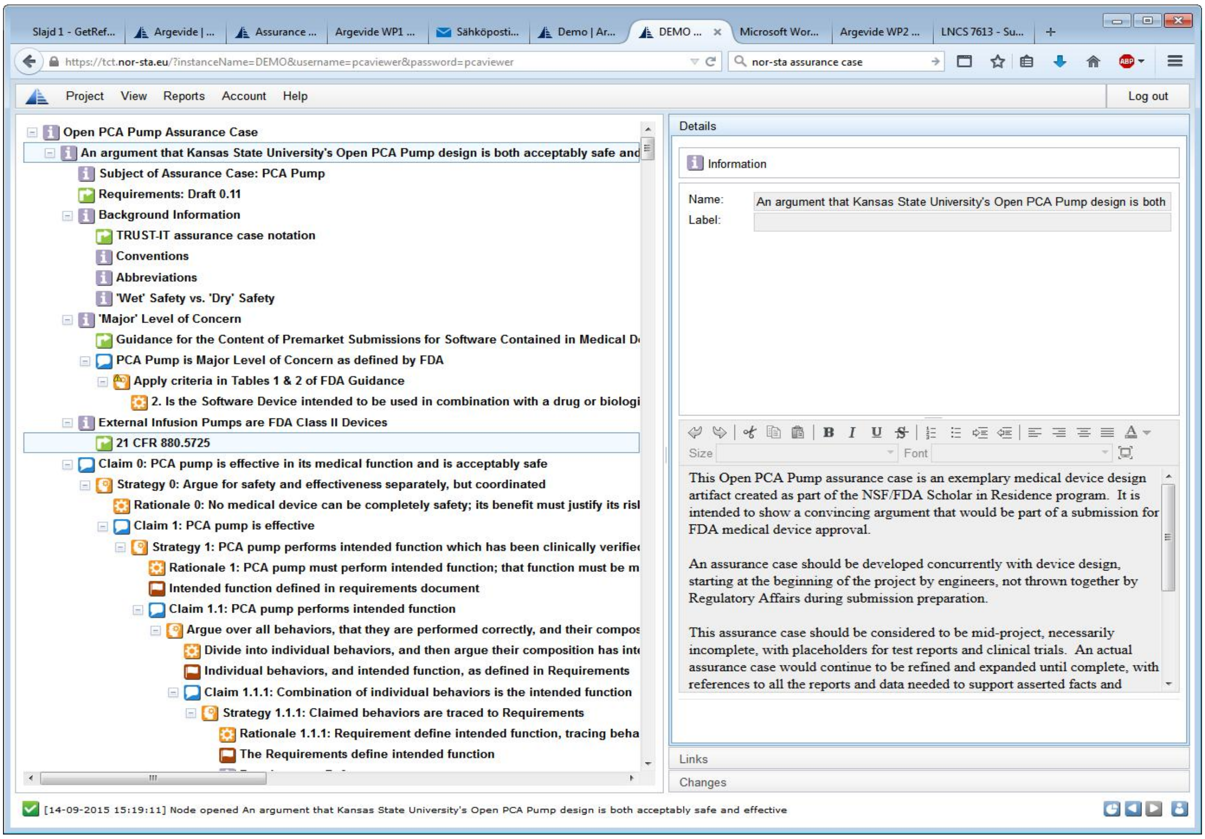

Astah GSN - [C:\Data\Diplomityö\Työkalutallennukset\Astah GSN\astah_GSN_testi.agml] (*)
File Edit Diagram Alignment View Tool Window Help
Goal Structure 1
GSN5
Goal Structure 1 / GSN
Goal 1
Control System is acceptably safe to operate
Context 1
Operating Role and Context
Context 2
Control System Definition
Goal 2
All identified hazards have been eliminated or sufficiently mitigated
Context 3
Tolerability targets (Ref Z)
Context 4
Hazards identified from FHA (Ref Y)
Goal 3
Software in the Control System has been developed to SIL appropriate to hazards involved
Context 5
SIL Guidelines and Processes
Strategy 1
Argument over each identified hazard
Assumption 1
All hazards have been identified
A
Strategy 2
Argument over allocated SIL for Primary and Secondary elements
Justification 1
SIL apportionment is correct and complete
J
Context 6
Identified software hazards
Goal 4
Hazard H1 has been eliminated
Goal 5
Probability of Hazard H2 occuring < 1x10-6 per year
Goal 6
Probability of Hazard H3 occuring < 1x10-3 per year
Goal 7
Primary Protection System Developed to SIL 4
Goal 8
Secondary Protection System Development to SIL2
Solution 2
Fault Tree Analysis
Solution 3
Process Evidence for
Base
TaggedValue
Hyperlink
Namespace
ID
Goal 1
Undeveloped
Public
Statement
Control System is acceptably safe to operate
Close

Figure 14. Safety case done with GSN notation in Astah GSN.



Open PCA Pump Assurance Case
An argument that Kansas State University's Open PCA Pump design is both acceptably safe and
Subject of Assurance Case: PCA Pump
Requirements: Draft 0.11
Background Information
TRUST-IT assurance case notation
Conventions
Abbreviations
'Wet' Safety vs. 'Dry' Safety
'Major' Level of Concern
Guidance for the Content of Premarket Submissions for Software Contained in Medical De
PCA Pump is Major Level of Concern as defined by FDA
Apply criteria in Tables 1 & 2 of FDA Guidance
2. Is the Software Device intended to be used in combination with a drug or biologi
External Infusion Pumps are FDA Class II Devices
21 CFR 880.5725
Claim 0: PCA pump is effective in its medical function and is acceptably safe
Strategy 0: Argue for safety and effectiveness separately, but coordinated
Rationale 0: No medical device can be completely safety; its benefit must justify its risl
Claim 1: PCA pump is effective
Strategy 1: PCA pump performs intended function which has been clinically verifiec
Rationale 1: PCA pump must perform intended function; that function must be m
Intended function defined in requirements document
Claim 1.1: PCA pump performs intended function
Argue over all behaviors, that they are performed correctly, and their compos
Divide into individual behaviors, and then argue their composition has inte
Individual behaviors, and intended function, as defined in Requirements
Claim 1.1.1: Combination of individual behaviors is the intended function
Strategy 1.1.1: Claimed behaviors are traced to Requirements
Rationale 1.1.1: Requirement define intended function, tracing beha
The Requirements define intended function

Name: An argument that Kansas State University's Open PCA Pump design is both
Label:

This Open PCA Pump assurance case is an exemplary medical device design artifact created as part of the NSF/FDA Scholar in Residence program. It is intended to show a convincing argument that would be part of a submission for FDA medical device approval.

An assurance case should be developed concurrently with device design, starting at the beginning of the project by engineers, not thrown together by Regulatory Affairs during submission preparation.

This assurance case should be considered to be mid-project, necessarily incomplete, with placeholders for test reports and clinical trials. An actual assurance case would continue to be refined and expanded until complete, with references to all the reports and data needed to support asserted facts and

```
[14-09-2015 15:19:11] Node opened An argument that Kansas State University's Open PCA Pump design is both acceptably safe and effective
```

Figure 15 Hierarchical text based tool by NOR-STA (Argevide).

However, preparing a safety case gets more difficult when the system-of-interest is large and so the visual structures will become more complex. Currently, this is somehow being managed by dividing bigger safety cases into sub-cases (modules), maybe even to component level. In future, safety case could be compiled out of predeveloped modules, which are done by different teams in-house or third parties (suppliers, TSOs). Tools could give the benefit of better configuration management possibilities for keeping the safety artefacts up-to-date and accessible in case the system is affected by a modification which will require changes to safety justification.

According to STUK, the appearance of the safety demonstration is free, as long as it is understandable and satisfies all the relevant requirements from YVL guides. STUK is moving towards of electronic submission of qualification and licencing material. Software tools could be a way of automating the development of safety assessment reports, if they could generate the correct type of documents or export data in suitable formats. At the moment, the tools evaluated in (Linnosmaa 2016) have a limited ability to do so.

As mentioned previously, the safety demonstration should be understood as an artefact, a set of documents related to safety of a specific system. A proper tool offers a way to combine these documents to a single hypertext document, with links straight to referred evidence, justification or technical detail artefact whenever it is mentioned in the safety demonstration or otherwise needed for inspection. This obviously reduces the time and effort put to assembling and reviewing the safety case, as well as the length and complexity of the following document.

However, safety case tools are not to be considered ready to use on a large scale safety justification just yet. While they could possess the future possibility for proper SE integration, at the moment they are still too lightweight for heavy industrial use. They do not have the features yet to manage large plant or system level safety cases without becoming too complex or difficult to follow. Tools available right now are best for constructing component and sub-system level safety cases, which will have fewer sub-claims under the top-claim and thus need less evidence and modules to be adequate and still accessible. It is not just a tool problem either; the standards, guidelines and notations do not offer enough support for whole system level safety cases with large numbers of modules and subcases with references to each other. It will get complicated and disordered, and no real solution is given to current practice. Other major problem is the lack of pre-existing building blocks (libraries), which would help users developing cases in a more rigorous and systematic manner. However, work is done towards making safety case tools able to handle large systems as well (Denney & Pai 2015; Netkachova et al. 2015). A further problem includes the absence of critical evaluation of linked evidence, which is given in OMG's Evidence metamodel. Most tools are missing full support for other critical standards as well (ISO 15026, SACM), but current view is that they are developing into that direction. So, developing and communicating the safety demonstration with computer-based tools could definitely be a step forward. Another step would be connecting safety case tools as part of SE environment for better integration with the rest of the system design and management processes.

5. Summary and conclusions

In this research report we have discussed the principles of safety justification of nuclear power plants with the focus on instrumentation control systems and the Finnish regulatory practices. Worldwide, in many regulated domains safety justification follows the “structured assurance case” approach and explicit argumentation. According to our understanding derived from literature, discussions and limited samples of real-world documentation, nuclear power (at least in Finland) applies less formal, traditional practices in safety justification. We expect, however, that structured safety assurance methods and tools are useful also in nuclear power, for example due to the complexity and multi-disciplinary character of digital automation. As an indication of this trend, a group of European regulatory experts has defined the term “safety demonstration” as a set of arguments and evidences which support a set of claims on the safety of a system (Common position document).

According to our review, there is both a need for more efficient confidence building practices and possibilities to solve the problems. For example, experiences from other critical domains, existing international standards and ongoing development of information models and tools can be used as a starting point. These practical solutions should, of course, be adapted to the current practices with a stepwise approach. In general, safety engineering and assurance is tightly connected to other system development and project management activities. Therefore, the qualification process producing the safety demonstration of an I&C system should be integral part of the overall Systems Engineering approach for nuclear I&C.

On the basis of this summary it is possible to identify three main directions for further research. Firstly, the qualification process of I&C systems (and equipment) should be refined covering, for example, terminology, activities, phases, documents and participant roles in various types of I&C projects. This should be done in the wider context of systems engineering reference models. Secondly, practical guidance should be provided for organising the qualification documentation and for presenting the reasoning behind safety claims in understandable, unarguable and traceable ways. Thirdly, differences between the qualification practices and procedures of the existing plants and the newbuilds should be identified and recognised to provide focused and tailored guidance for each purpose.

For all these goals, it would be important to discuss with industrial practitioners, to have access to real-world sample documents and to test the ideas with application examples.

References

Alanen, J. & Salminen, K. 2016. Systems Engineering Management Plan template - V1. Research report VTT-R-00153-16, 81 p. + app. 12 p.

Common position 2014. Licensing of safety critical software for nuclear reactors - Common position of seven European nuclear regulators and authorised technical support organisations.

Denney, E & Ganesh, P. 2015. Towards a Formal Basis for Modular Safety Cases. SAFECOMP 2015, LNCS 9337, pp. 328–343.

Elforsk 2013. Safety Demonstration Plan Guide A general guide to Safety Demonstration with focus on digital I&C in Nuclear Power Plant modernization and new build projects. Elforsk rapport 13:86, 63 p.

Greenwell, W. 2006. A taxonomy of fallacies in system safety arguments. Proceedings of the 2006 International System Safety Conference.

Hauge, A., Karpati, P. & Katta, V. 2014. Summary of the 2014 Expert Workshop on Safety Demonstration and Justification of Digital Instrumentation and Control Systems in Nuclear Power Plants. HWR 1113, OECD Halden Reactor Project, 38 p.

IAEA 2010. Licensing Process for Nuclear Installations. Specific Safety Guide No. SSG-12, 80 p.

IEC 61513 2011. Nuclear power plants - Instrumentation and control important to safety - General requirement for systems.

Kelly, T. 2007 Reviewing assurance arguments-a step-by-step approach. Workshop on Assurance Cases for Security-The Metrics Challenge, Dependable Systems and Networks (DSN), 5 p.

Leveson, N. 2011. The Use of Safety Cases in Certification and Regulation. Journal of System Safety, vol. 47, no. 6, November-December 2011, 9 p.

Linnosmaa, J. 2016. Structured Safety Case Tools for Nuclear Facility Automation. Master's Thesis. Tampere University of Technology. To be published in 2016.

Netkachova, K; Netkachov, O & Bloomfield, R. 2015. Tool Support for Assurance Case Building Blocks. SAFECOMP 2015 Workshops, LNCS 9338, pp. 62–71.

NUREG-0800 2011. Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition. United States Nuclear Regulatory Commission (NRC), available at: http://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr0800/.

OMG 2015. Structured Assurance Case Metamodel (SACM), version 1.1. Object Management Group (OMG), 176 p. Available at: http://www.omg.org/spec/SACM.

ONR 2013. The purpose, scope, and content of safety cases. Office for Nuclear Regulation (ONR, an agency of HSE), guide NS-TAST-GD-051 rev. 3, 26 p. Available at: http://www.onr.org.uk/operational/tech_asst_guides/ns-tast-gd-051.pdf

ONR 2014. Right First Time Safety Cases: How to Write a Usable Safety Case, Issue 1, March 2014, UK Nuclear Safety Case Forum Guide.

Raetzke, C., & Micklinghoff, M. 2006. Existing nuclear power plants and new safety requirements - an international survey, A description of the legal situation and of the regulatory practice in eight countries and in Germany. Germany: Heymanns.

STUK 2015a. Regulatory oversight of nuclear safety in Finland - Annual report 2014. STUK-B 191, 166 p. Available at: http://www.julkari.fi/bitstream/handle/10024/126384/stuk-b191.pdf.

STUK 2015b. Definitions used in the YVL guides. MS Excel file, 2015-07-15, available at: http://www.stuk.fi/saannosto/stukin-viranomaisohjeet/ydinturvallisuusohjeet. Retrieved 27.10.2015.

STUK 2010. Finnish report on nuclear safety - Finnish 5th national report as referred to in Article 5 of the Convention on Nuclear Safety. STUK-B 120, 86 p.

Tommila, T., Savioja, P. & Valkonen, J. 2014. Role of requirements in safety demonstrations Version 2, 31.1.2014. SAFIR 2014 programme, Working report of the SAREMAN project, 49 p.

Toulmin 1958. S. E. Toulmin “The Uses of Argument” Cambridge University Press, 1958.

WNA 2015. Licensing and Project Development of New Nuclear Plants. World Nuclear Association, Licensing & Permitting Task Force, report No. 2015/005, 44 p.

YVL A.1 2013. Regulatory oversight of safety in the use of nuclear energy. The Radiation and Nuclear Safety Authority (STUK), 22 November 2013, 43 p.

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 A: Glossary

This appendix explains the meaning of a selection of key terms used in this report. Most of them have been taken from relevant standards and guidelines. In some cases, however, slightly modified or even new definitions (indicated by an asterisk) are suggested for use in licensing nuclear I&C systems. The work with terminology will be continued in the forthcoming projects.

For interested readers it is probably worthwhile to know about these freely available collections of definitions:

- Software and Systems Engineering Vocabulary (SEVOCAB): http://pascal.computer.org
- IEC's Online Electrotechnical Vocabulary (Electropedia): http://www.electropedia.org
- STUK Glossary: Definitions used in the YVL guides, https://ohjeisto.stuk.fi/YVL/YVL-maaritelmat.xls (STUK 2015b)

Approved organisation: An organisation approved by the regulatory authority (STUK), for example a manufacturer, laboratory, testing body or inspection organisation. (*, inspired by STUK 2015b)

Argument (perustelu): The reason why the truth of a claim is or can be deduced from the specified evidence (modified from ISO/IEC 15026-2 2011, p. 3).

> Note: An argument shall have an associated justification for the validity or merit of its method (ISO/IEC 15026-2 2011).
>
> Note: A body of information presented with the intention to establish one or more claims through the presentation of related supporting claims, evidence, and contextual information (OMG 2015).

Assumption (oletus): A statement expected to be true without further justification.

> Note: Some assumptions are inherently true given their context and role within the assurance case. Some others are rather claims not fully warranted by evidence. Such assumptions should have a reason and an indication of the uncertainty regarding the truth of the assumption. They should be few in number and have low uncertainty or a weak impact on the argumentation. (ISO 15026-2 2011)
>
> Note: A claim is called an assumption if it appears in an assurance case as evidence. Such evidence is a proposition without any reason why it is true. (ISO 15026-2 2011)

Assurance: Grounds for justified confidence that a claim has been or will be achieved (ISO/IEC 150126-1 2013).

> Note: In general, assurance should be independent and unbiased. Therefore, it would be more correct to re-write the definition as"… whether a claim has been or will…".

Assurance case: 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 claim(s) (ISO/IEC 150126-1 2013).

> Note: Examples of the components of an assurance case are claims, arguments, evidence and assumptions. Assurance cases can be defined recursively. For example, a lower-level assurance case can be used as a claim at a higher level (see ISO/IEC 15026-2 2011).

Auditing (auditointi): A systematic, independent and documented process to objectively evaluate the audit evidence obtained to determine the extent to which the agreed auditing criteria are met (STUK 2015b/YVL A.1, SE VOCAB).

> Note: This definition is very generic and close to conformity assessment. In investment projects, auditing often refers to determining whether a supplier or service provider can meet the customer's requirements.

Claim (väite, väittämä): True-false *statement* about the limitations on the values of an unambiguously defined property — called the claim's property — and limitations on the uncertainty of the property's values falling within these limitations during the claim's duration of applicability under stated conditions (ISO/IEC 15026-1 2013).

Conformity assessment (vaatimustenmukaisuuden arviointi): Demonstration that the requirements relating to a product, process, system, person or body are fulfilled (STUK 2015b).

Evidence (todistusaineisto): Information or object used by an argument to show that a claim holds (modified from ISO/IEC 15026-2 2011).

> Note: Evidence is a fact, a piece of information (datum), an object, a claim or an (lower-level) assurance case. Evidence can already exist, be newly created or collected, or be planned for the future. (ISO/IEC 15026-2 2011)

Inspection (tarkastus): Examination of components or structures and related designs and processes as well as the verification of their conformity to requirements in terms of the requirements presented in STUK's decisions, the YVL Guides and the design bases (STUK 2015b).

Justification (oikeutus, perustelu): In this report, justification is used as a general term referring to a satisfactory reason or explanation for doing something or for something existing. (*)

> Note: In an structured assurance case, the justification of claim is a reason why the claim has been chosen (see ISO/IEC 15026-2 2011).

Licence (lisenssi): A legal document issued by the *regulatory body* granting authorisation to perform specified activities related to a facility or activity. Licence is a product of the authorisation process. (IAEA 2007)

> Note: The terms 'licence', 'authorisation' and 'permit' are considered to be synonymous; authorisation may take different forms, such as certification, granting of a permit, agreement, consent, regulatory approval depending on the governmental and regulatory framework of the particular State (IAEA 2010).

Licence applicant (luvanhakija): A person or organisation who applies to a regulatory body for authorisation to establish a nuclear installation, or parts of a nuclear installation, or to undertake specified activities (IAEA 2010).

Licensee (luvanhaltija): The holder (person or organisation) of a current *licence* having overall responsibility for a facility or activity (IAEA 2007).

> Note: Licensee shall refer to the holder of a licence entitling to the use of nuclear energy. The use of nuclear energy refers to the operations laid down in Sections 2(1) and 2(2) of the Nuclear Energy Act. (STUK 2015b)

Licensee's in-house inspection organisation (luvanhaltijan omatarkastuslaitos): Licensee's separate inspection unit, the position of which is arranged in compliance with the type B requirements of ISO/IEC EN 17020, the operations of which meet the specific requirements laid down by STUK, and which STUK has approved to carry out inspection tasks pertaining to the pressure equipment, steel and concrete structures and mechanical components of a nuclear facility in the form of in-house control by the licensee. (STUK 2015b)

Licensing (lisensiointi, luvitus): Authorisation process applied for nuclear installations. It includes all authorisation processes and generally covers a particular stage of the lifetime of a nuclear installation. (adapted from IAEA 2010)

> Note: In general, licensing applies to the whole nuclear facility.
>
> Note: The main participant roles are the *regulatory body* and the *licence applicant*.
>
> Note: The public should be given an opportunity to present their views during certain steps of the licensing process, where appropriate (IAEA 2010).

Note: Also *permitting* used as a synonym of licensing.

Plan (suunnitelma): Information item that presents a systematic course of action for achieving a declared purpose, including when, how, and by whom specific activities are to be performed (SE VOCAB).

Note: Quality plan is a document setting out the specific quality practices, resources and sequence of activities relevant to a particular product, project or contract (IEC 61513 2011).

Note: Qualification plan, see safety demonstration plan

Note: Configuration management plan is a description of the configuration management processes and related instructions, responsibilities and resources (YVL B.1 2013).

Note: Conceptual design plan corresponds to a Preliminary Safety Analysis Report and quality management plan concerning a planned system modification (see YVL B.1 2013). So, it is actually not a “plan” as defined above.

Qualification (kelpoistus, pätevöinti): The process of determining by comparison to the criteria set by the society whether an organisation, person or technical system is suitable for its intended tasks. (Tommila & Alanen 2015)

Note: This definition tries to express the general idea that qualification is about obtaining acceptance from an official or legal body, in our case from the regulatory body.

Note: For personnel, qualification refers to a demonstrated ability to apply knowledge and skills (STUK 2015b).

Note: A process to demonstrate the ability to fulfil specified requirements (YVL B.1 and E.7 2013). IEC 61513 (2011) defines qualification as the process of determining whether a system or component is suitable for operational use. IAEA (2007) defines this term as the generation and maintenance of evidence to ensure that equipment will operate on demand, under specified service conditions, to meet system performance requirements.

Note: Other definitions from the Software and Systems Engineering vocabulary (SE VOCAB): (1) process of demonstrating whether an entity is capable of fulfilling specified requirements; (2) the process of determining whether a system or component is suitable for operational use.

Regulator: The *regulatory body* and/or authorised technical support organisation acting on behalf of its authority (Common position 2014).

Regulatory body: An authority or a system of authorities designated by the government of a State as having legal authority for conducting the regulatory process, including issuing authorisations, and thereby regulating nuclear, radiation, radioactive waste and transport safety (IAEA 2007).

Requirement (vaatimus): A *statement* that translates or expresses a need and its associated constraints and conditions (ISO/IEC 150126-1 2013).

Safety (analysis) report (turvallisuusseloste): An artefact submitted to the regulator in the construction license application stage (Preliminary Safety Analysis Report, PSAR) or in the operation license application stage (Final Safety Analysis Report, FSAR). PSAR shall include general design and safety principles of the nuclear facility, a description of the operation of the facility, a description of the behaviour of the facility during accidents. FSAR shall provide an overview of the principles applied in the design of the entire plant and in the design of each system contained in the plant. (YVL B.1)

Safety case: An *assurance case* focusing on safety aspects. (*)

Note: A collection of arguments and evidence in support of the safety of a facility or activity (IAEA 2007).

Note: Safety case (turvallisuusperustelu) refers to documentation for demonstrating compliance with the long-term safety requirements (STUK 2015b/YVL D.5).

Note: A nuclear safety case is a set of documents that describe the radiological hazards in terms of a site or facility (or part of it) and modes of operation and the measures that prevent or mitigate against harm being incurred. The safety case should provide a coherent demonstration that relevant standards have been met and that risks to persons have been reduced to as low as reasonably practicable (see ONR 2013).

Safety demonstration (turvallisuusperustelu): 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 (Common position 2014).

Note: Safety cannot be discussed and shown to exist without using accurate descriptions of the system architecture, of the hardware and software design of the system behaviour and of its interactions with the environment (Common position 2014).

Safety (demonstration) plan: A plan, which identifies how the *safety demonstration* is to be achieved; more precisely, a plan which identifies the types of evidence that will be used, and how and when this evidence shall be produced. A safety plan is not necessarily a specific document. (Common position 2014, Elforsk 2013)

Statement (toteamus): A broad term referring to an expression (proposition) by a stakeholder of a past, current or future state-of-affairs. (modified from Tommila & Alanen 2015)

Note: Depending on its communicative intent, a statement is interpreted as a fact, claim, assumption, requirement, etc.

Structured safety case: A safety case based on a defined (formal) information model of claims, arguments, evidences, etc. (*)

Suitability analysis/assessment (soveltuvuusarvio): A suitability analysis shows whether a component or product (e.g. instrument, process controller, electrical equipment or cable) is suitable for its intended use in the specified operating environment. (*)

Note: For fire protection, a suitability assessment presents how well a fire protection system meets the requirements placed on it and how the licensee has verified conformity. The suitability assessment also lists changes to the approved documents and their effect on the suitability and acceptability of the system in question. (STUK 2015b/YVL B.8)

Note: Preliminary suitability analysis shall be used by the licensee to verify that a component is suitable for its intended location of use on the basis of its rated values. The qualification of the component is also inspected and designed. After the preliminary suitability analysis the requirement specification of the component is verified, and the procurement of the component may be started, if necessary. (STUK 2015b/YVL E.7)

Note: Final suitability analysis refers to the licensee’s assessment to demonstrate (validate) that a component meets its rated values (YVL E.7 2013).

Testing (testaus): 'Testing shall refer to determining one or more characteristics of an object evaluated for conformity to requirements STUK 2015b).