Title	Views on safety demonstration and systems engineering for digital I&C
Author(s)	Valkonen, Janne; Tommila, Teemu; Alanen, Jarmo; Linnosmaa, Joonas; Varkoi, Timo
Citation	39th Enlarged Halden Programme Group Meeting, EHPG 2016, 8 - 13 May 2016, Fornebu, Norway
Date	2016
Rights	Institute for Energy Technology. This article may be downloaded for personal use only.

MTO-4.3: Views on Safety Demonstration and Systems Engineering for Digital I&C

Janne Valkonen, Teemu Tommila, Jarmo Alanen, Joonas Linnosmaa
VTT Technical research centre of Finland Ltd
firstname.lastname@vtt.fi

Timo Varkoi
Finnish Software Measurement Association - FiSMA
timo.varkoi@fisma.fi

Abstract

Designing and licensing a nuclear power plant and qualification of its subsystems and components is a challenging task involving several stakeholders and integrating information from various disciplines. Several recent discussions and workshops have shown that the current practice of justifying safety of nuclear power plant's systems can be improved. There still seems to be considerable confusion concerning the key terminology and the flow of the qualification and licensing processes. Existing standards and regulations provide limited guidance on how the licensee should formulate and communicate a convincing story on the safety of the facility. All this can be made more systematic and transparent by utilising the principles of Systems Engineering and model-based computer tools as the general framework for both engineering and safety assessment. There are several analysis methods for collecting the required evidences for a safety demonstration. These methods range from plant-level safety architectures to detailed I&C functions and from technical solutions to human-machine interactions and safety culture. A standards-based, structured safety demonstration can be seen as a knowledge repository that integrates different disciplines and assessment results into a consistent overall picture of systems and their safety properties.

1. Introduction

The fundamental, repeated question with critical, complex systems is 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? Designing and licensing nuclear power plant I&C (Instrumentation and Control) systems requires involvement of several stakeholders from various disciplines. One of the challenges has been the lack of communication between different engineering disciplines, such as process design, automation design, human factors engineering, and electrical design. By using the principles of Systems Engineering (SE) it is possible to better manage the development of complex systems, such as digital I&C. Systems engineering can be defined as "*an interdisciplinary approach governing the total technical and managerial effort required to transform a set of stakeholder needs, expectations, and constraints into a solution and to support that solution throughout its life cycle"* [3]. To efficiently apply the SE approach in practice, a description of the required SE processes and the enveloping Management System is needed. This can be called a Systems Engineering Management Plan (SEMP).

The nuclear authorities, in most countries, demand for a documented justification of safety. It should be logically unarguable, unbiased, comprehensive, transparent and accessible to all relevant parties. As digital I&C systems are nowadays commonplace in new nuclear power plants and modernisations of old ones, qualification of safety critical software has become an issue. As stated by a group of regulatory experts [1], the assessment of software cannot be limited to

verification of the end product, i.e. the computer code. For a trustworthy safety demonstration, also other factors, such as the quality of the development processes, organisations, and methods are needed. Unfortunately, existing standards provide limited guidance on the assessment of these factors.

This paper first describes some of the challenges in designing and licensing complex, critical systems. Secondly, Systems Engineering based approach for designing and qualifying system is introduced. After that the key concepts on the terminology related to safety demonstration is provided by using the Finnish nuclear regulatory regime as the main reference. The last part of the paper concerns approaches and methods that can be used for providing evidence for safety demonstration.

2. Systems Engineering Approach on Systems Design and Qualification

2.1 What Is Systems Engineering

The International Council on Systems Engineering (INCOSE) characterises Systems Engineering (SE) as an “interdisciplinary approach and means to enable the realization of successful systems”. In SE, a system is understood as a combination of interacting elements organised to achieve their stated purposes. System elements can be, e.g., hardware, software, humans, procedures, facilities or materials [3]. These systems are man-made for a purpose. They are successful if they fulfil the actual needs of their stakeholders in the intended environment. So, satisfying written requirements may 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 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, such as requirements definition, solution synthesis and analysis, modelling and documentation, testing and configuration management. SE focuses on technical processes but also defines supporting activities like project management and organisational processes.

SE is more or less what nuclear I&C designers are doing. However, that is 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 [3]. It establishes a framework for the system life cycle 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 processes are applicable throughout the life cycle for managing and performing the life cycle activities. 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 life cycle processes used within an organisation or a project. The standard is intended to help an organisation establish its processes; projects provide products and services; suppliers and acquirers agree on working processes; and to serve as a process reference model (PRM) in process assessments.

The standard is not specific for any area of industry. For example, it doesn’t explicitly describe the activities of safety justification and licensing in regulated domains. Implementation of the standard

typically involves selecting, extending and tailoring the predefined processes for the purposes of the domain, organisation or project. A suggestion for its adaptation to nuclear I&C has been made in [4].

2.2 Model-based Systems Engineering

ISO/IEC/IEEE 42010 [5] defines a model *as follows: "M is a model of S if M can be used to answer questions about S."* In this sense, all typical engineering work products (artefacts) that specify or describe a system are models. Because not all systems engineering is model-based, we use the definition by INCOSE for model-based systems engineering: "*Model-based systems engineering (MBSE) is the formalized application of modelling to support system requirements, design, analysis, verification and validation [activities] beginning in the conceptual design phase and continuing throughout development and later life cycle phases.*" [6]

The difference to traditional SE is in the use of formalised or semi-formalised, machine readable models or virtual engineering artefacts instead of word processing documents to describe the system-under-study. This does not mean that documents are not used in MBSE, but it means that MBSE is based on formalised or semi-formalised models instead of documents. As a consequence, the role of documents changes: in MBSE, documents are a means to present information (including models) instead of being containers of information. This fact encourages using automatic or semi-automatic document generation, which is not possible in traditional SE. Moreover, MBSE provides the means to manage systems engineering artefacts so that all partners have a consistent and up to date view of the system-of-interest. This way SE helps avoid documents chaos.

2.3 Systems Engineering Management Plan

INCOSE [7] defines Systems Engineering Management Plan (SEMP) as "*structured information describing how the systems engineering effort, in the form of tailored processes and activities, for one or more life cycle stages, will be managed and conducted in the organization*". The main contents of SEMP is thus the identification and definition of the SE processes, but it also outlines the Management System [8] context; it identifies the system-of-interest, its context and its life cycle model and the project context; and it describes the stakeholders and their needs (most of them expressed in regulations and standards). For example, the Finnish regulatory guide on nuclear safety YVL A.3 "Management system for a nuclear facility" sets requirements for planning, implementation, maintenance, assessment and improvement of the management system. It also defines responsibilities of the management and sets requirements for developing and managing the processes of the management system.

Each project shall create a SEMP of its own; the project plan is accompanied by the SEMP. A common SEMP template can be provided within the Management System. A proposal for a SEMP table of contents is provided below. As stated above, Chapter 8 of the SEMP in Table 1 is in the core of the plan. The majority of SE processes can be obtained from ISO/IEC/IEEE 15288, but tailoring is anticipated and additional processes are needed, such as the qualification process in nuclear applications.

Table 1. Proposal for SEMP table of contents [3].

1. Introduction to the SEMP 2. System and system context identification 3. Description of the Management System 3.1. Policy statements 3.2. Organisations, roles, responsibilities and competences 3.3. Safety management and safety culture 3.4. Quality management and culture of quality 3.5. Training 3.6. Infrastructure (Facilities, buildings, workspaces and associated utilities; Process tools and equipment; Supporting services; Work environment) 4. Management system context 4.1. Organisation's history context 4.2. Cultural context	4.3. Ecological context 4.4. Economic context 4.5. Legal context 4.6. Political context 4.7. Societal context 4.8. Technological context 4.9. Partner context 5. Project context 6. Stakeholders and their needs, applicable documents 7. Life cycle model 8. Systems Engineering processes 9. References Appendix A: Glossary Appendix B: Process and System documents master index

A SE process consists of activities, and activities consist of tasks; a process has inputs and outputs. It is controlled by regulations and process constraints and supported by enabling mechanisms, such as tools, human resources, facilities and services. ISO/IEC/IEEE 15288 defines a process constructs model that is enhanced in [3] as depicted in Figure 1. With such a powerful information model SE processes can be defined in an unambiguous way and managed on a database-oriented IT platform. The structured data storage provides well identified artefacts (such as the outcomes and their corresponding information items) and trace links between the artefacts. This facilitates project management and collaboration, but especially process assessment and thus safety demonstration.

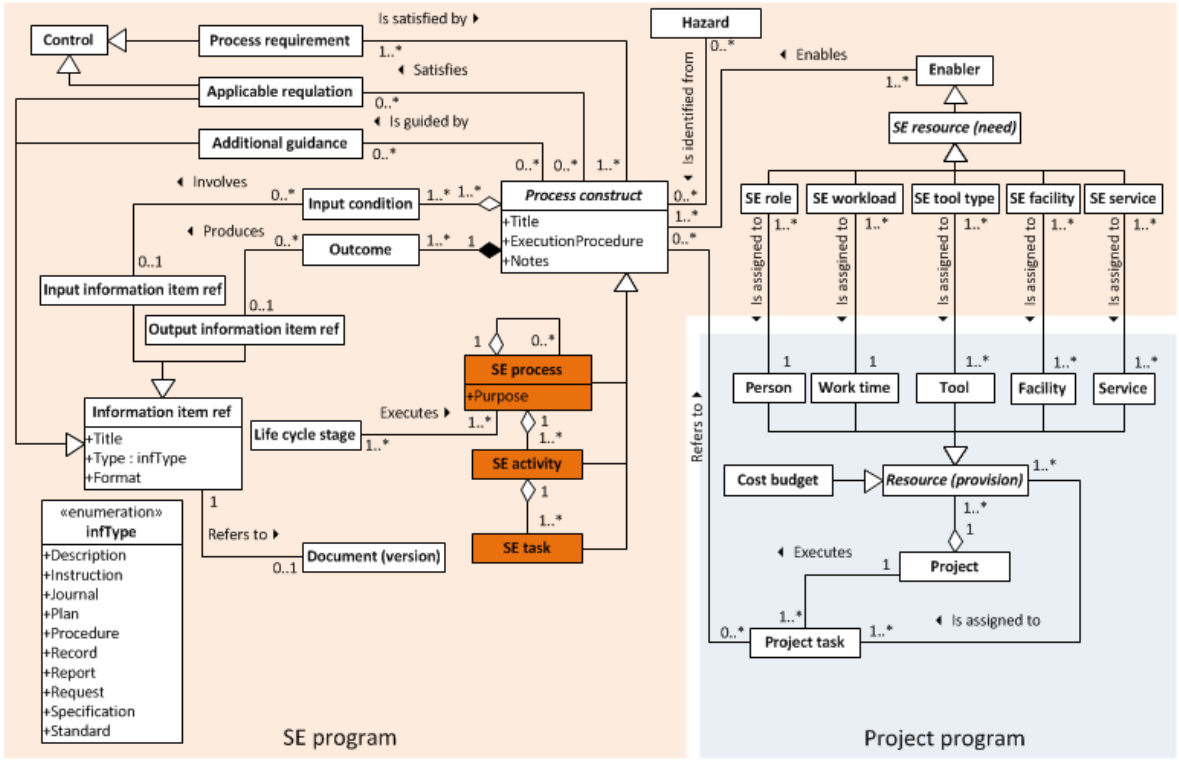

Figure 1. Enhanced process constructs model. Also the main project artefacts are added to illustrate the interface between the SE program and project program [3]. (The figure does not provide all attributes of the SE process -model element; see [3] for the complete list of attributes.)

The main function of a SEMP is to ensure the quality of engineering effort. For a safety demonstration, the SEMP is relevant because it orchestrates the technical processes (e.g. system requirements definition and architecture definition processes) and the qualification activities such that a consistent safety case can be supplied using the verification and validation (V&V) artefacts produced during the V&V activities.

3. Considerations on Safety Demonstration and Licensing

3.1 Key Concepts

Definitions and interpretations of the terminology related to safety justification vary from country to country in the nuclear area. This has always been one of the challenges in large newbuilds and renewal projects where several nationalities work together and mainly communicating with their second or third language. When we add limited knowledge of disciplines other than one's own, misunderstandings are almost inevitable. Common understanding of domain-specific concepts and the meaning behind words is critical for successful communication. This Section presents authors' views on the terminology related to safety demonstration and licensing of nuclear I&C systems.

3.1.1 Safety Demonstration

Herein the term *safety demonstration* is defined according to the safety critical task force's common position in [1]: "*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. The definition also says that a safety demonstration should have a clear structure, e.g. textual, tabular or graphical as depicted in Figure 2.

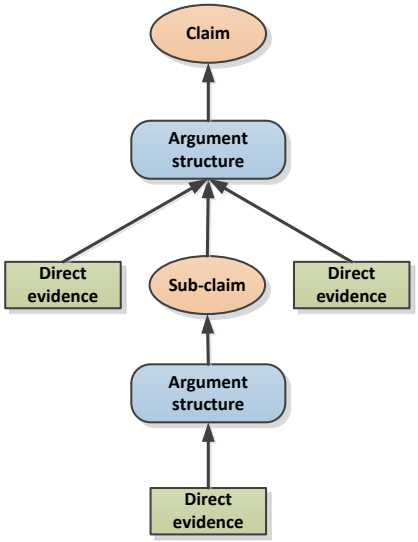

Figure 2. Claim-argument-evidence structure of a safety demonstration.

Sometimes safety demonstration is mixed with or used as a synonym to 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 3). As such, it is more than just claims, arguments and evidences including, for example system description, testing reports, hazards, failure modes and effects analysis results etc. (see [10]). The term safety justification is used as a common language expression for safety cases and safety demonstrations in general.

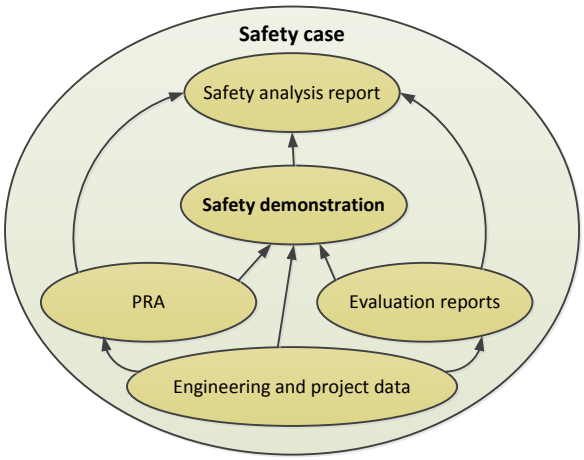

Figure 3. Position of safety demonstration in the overall safety justification material [14].

Similar to [1], the international standard ISO 15026 ISO/IEC 15026 Systems and Software Engineering—Systems and Software Assurance defines the generic *assurance case* as a "*reasoned, auditable artefact created that supports the contention that its top-level claim (or set of claims), is satisfied*" (see section 3.2 below). Depending on its focus, an assurance case can be called a safety case, dependability case, etc. So, the nuclear safety demonstration above is actually a safety case in ISO terms. To emphasise the formal character of safety case and to make

a distinction to our wider interpretation above, we use the expression “structured safety case” for an ISO assurance case.

When looking, for example, at the Finnish Regulatory Guides on nuclear safety (YVL), it becomes clear that some sort of justification is required for decisions having potential safety impacts. Reasons and rationale are key elements of transparency and traceability. Therefore, justifications should be explicit and well written. Common position [1] 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.

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 [12].

3.1.2 Licensing and Qualification of I&C

The term licensing may also be a bit confusing. In the Finnish practice, 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.

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 [11] 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.

Even if expressions like “licensing digital I&C” can be found in the literature, the Finnish regulatory guides (YVL) use the term *qualification* on system and component level. Qualification refers to a process of demonstrating the ability to fulfil specified requirements. As it can be interpreted, qualification is about “demonstrating safety to an official party” (the regulator) and therefore carried out by the license applicant together with its contractors. However, the license applicant carries the ultimate responsibility for safety, demonstrating it and preparing qualification documentation. 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.

In contrast to definitions presented above, e.g. [13] defines 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, in other countries than Finland, the term qualification is used only on component level instead of a system and equipment level.

3.2 Relevant Standards

International standards provide a solid basis to develop models for many engineering disciplines, including systems engineering and safety demonstration. International standards are well-known and widely accepted presentations of state-of-the-art knowledge in their domains. They aim to provide consistent terminology and compatibility between the standards. Main difficulty in using standards is to identify the most useful ones to be applied. This Section provides a short description of the standards relevant to safety justification of I&C systems.

The standard *ISO/IEC/IEEE 15288:2015 Systems and software engineering - System life cycle processes* defines systems engineering processes that apply to the full life of systems, whether performed by system suppliers or the organisation acquiring or using the system.

The *ISO/IEC 24748 Systems and software engineering - Life cycle management* standard has six parts. It provides guidance for the application and management of the system and software life cycle processes, including specific part on applying the 15288 standard, i.e. *Part 2: Guide to the application of ISO/IEC/IEEE 15288 (System life cycle processes)*. The detailed definitions and recommendations for Systems Engineering Management Plan (SEMP) (more in Section 2.3) are in *Part 4: Systems engineering planning* that will be published in 2016.

The 15288 standard refers to *ISO/IEC 15026 Systems and Software Engineering—Systems and Software Assurance* for system and software assurance guidance. The 15026 standard consists of four parts: Part 1: Concepts and vocabulary, Part 2: Assurance case, Part 3: System integrity levels, Part 4: Assurance in the life cycle.

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. A safety demonstration (as an artefact) is a specialisation of the assurance case.

In addition, a model that builds on the 15026 standard is the *OMG Structured Assurance Case Metamodel (SACM)* [9]. SACM defines a metamodel for representing structured assurance cases to enable information exchange related to systems assurance. SACM defines object models for Structured Assurance Case, Argumentation, and Evidence using class diagrams to support tool development for systems assurance.

3.3 Tools

As 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 assurance for justifying the safety of a system or a process. Safety demonstration is a well-structured assurance case, just focusing on the safety aspect of the system. The practical way of presenting all this often large and complex material is using a software tool.

Tools for creating assurance cases are available [10]. 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 stand-alone software tools focused on creating safety cases. Such tools support creation and management of structured assurance case, often by using a specific notation such as Goal Structuring Notation (GSN) or Claims-Arguments-Evidence (CAE), while following the definition of assurance case given by ISO 15026 or OMG's SACM.

Assurance case tools offer features that help the end user gather and prepare a structured safety demonstration. One clear benefit is visually, or in some cases by using hierarchical text, linking the evidence to the supported claims, with argumentation giving the reasoning in between. This helps in representing the justification behind claims and related evidence in a way that is easier for all stakeholders to follow. Software tools can also help reducing the amount of free text descriptions and justifications, and provide the possibility to use more controlled language for expressing arguments. Of course, the tool only gives the possibility of doing this, but in the end it is up to the user to write a good safety demonstration.

Managing a complex assurance cases in tool environment is a challenging process that requires support from standards and the notation used [16]. However, existing assurance case tools are not considered ready for a large scale safety justification just yet. They do not have the features yet to manage large plant or system level assurance case without becoming too complex or difficult to follow, they will get complicated and disordered, and no real solution is given to current practice. Tools available right now are best for component and sub-system level assurance cases. Another major problem is the lack of reusable building blocks, which would help users developing cases in a more efficient and systematic manner. [15]

4. Methods for Providing Evidence for Safety Demonstration

As explained above, the ultimate goal of a safety demonstration is to build trust in the safety of a system. Since safety is an emergent property resulting from interactions of all system elements, several engineering disciplines must be assessed to get a good picture of the overall safety performance. When I&C systems are considered, interfaces to external actors like human operators and process systems are important. In case of complex systems, such as programmable I&C, testing the implementation is not enough, but assessments of both solutions and working practices must be performed and evidence collected throughout the life cycle. All this means that many kinds of assessment methods are needed for a comprehensive safety demonstration. This section gives examples of methods and tools studied in the Finnish SAFIR programmes on nuclear safety [22].

4.1 I&C Architecture Analysis

In common language, “architecture” refers to the way in which the components of a system are organised and integrated. Architecture is described according to several viewpoints each expressing specific concerns of the stakeholders. A distinction can be made between functional architecture (organisation of functions) and physical architecture (organisation of system elements). In nuclear power, *I&C architecture* is understood as organisational structure of all I&C systems of the plant, while *I&C system architecture* is related to one system. As a high-level description, an I&C architecture specification should cover interactions with and physical links to relevant external actors. For example, the idea of Concept of Operations (ConOps) used in Systems Engineering works as a boundary object in collaboration of various user groups and engineering disciplines [7].

So, architectures tie together many aspects and include critical decisions made early in the design process. In particular, I&C architecture plays an important role in the plant-level Defence-in-Depth (DiD) solution. Therefore, improvements would be needed in related terminology, representations and design methods. Since DiD is required by the regulators, the fulfilment of their requirements must be demonstrated. So, there is a need for efficient assessment methods. Today, there are a few approaches for evaluating Diversity and Defence in Depth (D3) capabilities. While progress has been made in using probabilistic methods, the approaches are mostly deterministic [18]. Due to the amount of information and complex dependencies, model-based software tools will be needed to assess DiD and I&C architectures. For example, the Functional Failure Identification and Propagation (FFIP) framework is a risk assessment method that, when combined with failure models and simulation, can be used to identify unintended fault propagation paths crossing system and discipline boundaries [18].

4.2 Model Checking

Model checking is a formal, computer-assisted verification method that can exhaustively prove that a certain type of model of a (software or hardware) system fulfils stated properties. A model checker is a software tool that is used to verify that no model state or execution violates a property. Properties can take the form of liveness (“a good thing always happens”) or safety properties (“a bad thing never happens”). If a model execution contrary to a stated property is found, it is returned as a counterexample (error trace), the analysis of which can then reveal a design error. What sets model checking apart from more conventional methods is the exhaustive analysis (all possible scenarios are taken into account), and particularly the ability to evaluate safety properties, both of which are practically impossible if verification is only based on testing, for example.

In the nuclear domain, model checking has mostly been used for functional verification of I&C application software [25]. However, also methodologies for modelling hardware failures have been developed [26] that allows the verification of plant-level properties under various failure assumptions, which has previously been difficult.

4.3 Probabilistic Safety Assessment

There are two basic types of safety analysis approaches used in nuclear power: deterministic safety analysis (e.g. FMEA) and Probabilistic Safety Assessment (PSA). In addition to estimating accident probabilities, PSA is best suited for determining the safety significance of various plant items and sensitivities of the estimates to input data uncertainties and as a decision support tool for comparing design alternatives. Traditionally, PSA has an important position in assuring nuclear safety, and new approaches are being sought for to apply it also to software-based systems [23]. However, since many safety aspects, such as safety culture of the development organisation, can’t be easily quantified, PSA alone is not sufficient for a safety demonstration as it understood here. But in any case, PSA provides a framework for organising the analysis data and generates results that can be used as evidence in the integrated safety demonstration. Research efforts are also taken for coupling model checking and PRA for safety analysis of digital I&C systems [24].

4.4 Process Assessment

A novel approach that has been used to provide information for qualification is process assessment. So far, assessments have mainly been applied to evaluate safety related risks in implemented software processes and thus to meet the regulatory needs for development process quality. Process assessments are a cost-efficient way to address also a wider range of systems

engineering processes, and to enable systematic collection of evidence for safety demonstration. For assurance purposes, process assessment methods should be extended to include also safety demonstration and conformity with requirements needs [17]. This requires an approach that integrates product evaluation with process assessment. Process assessment cannot alone provide adequate coverage of regulatory requirements, but can effectively support qualification.

4.5 Systems Usability Case

User interfaces and control room arrangements are essential for the I&C architecture and the overall safety of process control operations. Systems Usability Case [19] is a systemic approach for control room evaluation and it is based on the assurance case idea. It illustrates the multi-disciplinary character of safety demonstration and its step-wise implementation in parallel with the development activities. Usability case also gives an example of how observations and structured argumentation can be used to show whether stated safety requirements have been fulfilled or not. So far, the method has been used for control room validation. It is, however, foreseen that all human factors related safety justification data could be arranged in a "human factors safety case" also including issues related to training and procedure design as well as management structure and practices.

4.6 Safety culture evaluation

Nuclear safety depends on the ability and willingness of an organisation to anticipate, monitor, respond to and to learn from the risks inherent in nuclear power production. These abilities and this willingness are the essence of a good safety culture [20]. Even if culture can't obviously be "engineered" in advance, it is important to create circumstances where it can develop in a natural way. In addition, the emergence of safety culture must be managed and assessed in some way. DISC (Design for Integrated Safety Culture) is a safety culture assessment methodology developed by VTT [20]. The DISC model summarises the criteria of good safety culture and the organisational functions that support its development. Assessment uses multiple data collection methods, such as interviews, questionnaires, document analysis, observations, personnel surveys and group work. The core of the assessment process is to use the observations to evaluate to what degree the organisation fulfils the evaluation criteria.

Safety-critical industries are expected to establish a systematic way of managing safety. So, the operational and maintenance organisations in a nuclear facility are natural targets for safety culture assessment. However, many activities are not carried out by the operating company itself but by a network of actors consisting of e.g. subcontractor companies and their workers [21]. In particular, large investment projects involve great complexity and uncertainty, multiple stakeholders and ambiguity. Therefore, assessment of the safety culture, and other capabilities, of the participants and the supply chain as whole should be part of Systems Engineering Management Plan introduced in Section 2.3.

5. Conclusions

This paper has discussed safety justification in the context of digital I&C in nuclear power plants. The goal has been to contribute to the ongoing debate on related terminology and the role of safety demonstration in licensing digital I&C. Systems Engineering principles and their applications on model-based computer tools are seen as the general framework for both engineering and safety assessment. Moreover, interpretations of terms, such as safety demonstration and qualification,

are suggested mainly based on the Finnish practices. Starting from the overall assumption that more rigour in reasoning would lead to better readability and traceability of safety assessments, this paper presents results of ongoing standardisation and tool development that can make structured safety demonstrations feasible in practice. Moreover, examples analysis methods for collecting the required evidences are described. Due to the emergent nature of system safety and multi-disciplinary character of Systems Engineering, many types of analysis methods are necessary ranging from plant-level safety architectures to detailed I&C functions and from technical solutions to human-machine interactions and safety culture. A standards-based, structured safety demonstration is seen as a knowledge repository that integrates different disciplines and assessment results into a consistent overall picture of systems and their safety properties.

6. References

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

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

[3] ISO/IEC/IEEE 15288, Systems and software engineering - System life cycle processes, 2015

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

[5] ISO/IEC/IEEE 42010. 2011. Systems and software engineering – Architecture description. Geneva: International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) and New York: Institute of Electrical and Electronics Engineers (IEEE). 37 p.

[6] Friedental, S., Griego, R. & Simpson, M. 2007. INCOSE Model Based Systems Engineering (MBSE) Initiative. INCOSE2007, San Diego, June 24-29 2007. A presentation. 29 p.

[7] INCOSE. 2015. Systems Engineering Handbook – A guide for system life cycle processes and activities. Fourth edition. San Diego: International Council on Systems Engineering (INCOSE). 290 p.

[8] IAEA. 2006. The Management System for Facilities and Activities. GS-R-3. Vienna: International Atomic Energy Agency (IAEA). 27 p.

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

[10] 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

[11] 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.

[12] 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.

[13] 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.

[14] Valkonen, J., Tommila, T., Linnosmaa, J., Varkoi, T., Safety demonstration of nuclear I&C - an introduction, Research Report : VTT-R-00167-16, 2016, VTT, 38 p

[15] Linnosmaa, J. 2016. Structured safety case tools for nuclear facility automation. Master's Thesis. Tampere University of Technology. To be published in 2016.

[16] Kelly, T. 2003. Managing complex safety cases. In: Redmill, F., Anderson, T. (eds.) Current Issues in Safety-Critical Systems, pp. 99–115. Springer, London (2003)

[17] Varkoi, T. & Nevalainen, R. Extending SPICE for Safety Focused Systems Engineering Process Assessment. R.V. O'Connor et al. (Eds.): EuroSPI 2015, CCIS 543, pp. 1–13, 2015.

[18] Tommila, T., & Papakonstantinou, N., Challenges in Defence in Depth and I&C architectures. Research Report VTT-R-00090-16, VTT, 60 p.

[19] Laarni, J., Savioja, P. et al. Conducting multistage HFE validations – constructing Systems Usability Case. ISOFIC/ISSNP 2014, Jeju, Korea, August 24~28, 2014, 10 p.

[20] Oedewald, P., Gotcheva, N., Viitanen, K. & Wahlström, M. Safety culture and organisational resilience in the nuclear industry throughout the different lifecycle phases. VTT Technology 222, May 2015, 128 p.

[21] Oedewald, P. & Gotcheva, N. Safety culture and subcontractor network governance in a complexsafety critical project. Reliability Engineering and System Safety 141 (2015), pp. 106–114.

[22] The Finnish Research Programme on Nuclear Power Plant Safety 2015 – 2018, SAFIR2018. http://safir2018.vtt.fi/

[23] Holmberg, J.-E., Bäckström, O., Tyrväinen, T., Analysis and modelling of software in probabilistic safety assessment. International Journal of Nuclear Safety and Simulation. IECNSS, 2015, vol. 5, 4, ss. 310-319

[24] Björkman, K., Lahtinen, J., Tyrväinen, T., Holmberg, J.-E., Coupling model checking and PRA for safety analysis of digital I&C systems, International Topical Meeting on Probabilistic Safety Assessment and Analysis, PSA 2015, 26 - 30 April 2015, Sun Valley, ID, USA, American Nuclear Society, ss. 384-392

[25] Pakonen, A., Valkonen, J., Matinaho, S., Hartikainen, M., Model checking of I&C software in the Loviisa NPP automation renewal project. Automaatio XXI, 17 - 18.3.2015, Helsinki, Finland, Finnish Society of Automation

[26] Lahtinen, J., Hardware failure modelling methodology for model checking. Espoo, VTT. 35 p. Research report; VTT-R-00213-14, 2014