Title	Demonstrating and argumenting safety of I&C systems - challenges and recent experiences
Author(s)	Valkonen, Janne; Tommila, Teemu; Linnosmaa, Joonas; Karpati, Peter; Katta, Vikash
Citation	10th International Topical Meeting on Nuclear Plant Instrumentation, Control and Human Machine Interface Technologies, NPIC & HMIT 2017, 11 - 15 June, 2017, San Francisco, CA, USA, pages 568-580
Date	2017
Rights	Copyright 2017 by the American Nuclear Society, LaGrange Park, Illinois

DEMONSTRATING AND ARGUMENTING SAFETY OF I&C SYSTEMS – CHALLENGES AND RECENT EXPERIENCES

Janne Valkonen, Teemu Tommila, Joonas Linnosmaa
VTT Technical Research Centre of Finland Ltd
P.O.Box 1000, FI-02044 VTT, Finland
firstname.lastname@vtt.fi

Peter Karpati, Vikash Katta
OECD Halden Reactor Project, Institute for Energy Technology
P.O. Box 173, NO-1751 Halden, Norway
firstname.lastname@ife.no

ABSTRACT

Nuclear licensees are required to submit a documented justification of the safety of the plant and its systems to the local regulatory body. Developing this documentation is a hard task and requires a lot of effort from several stakeholders. It should be understandable, transparent, convincing and complete. Observations from the current practice indicate that the nuclear power industry would benefit from more structured, systematic and harmonized practices in engineering instrumentation and control (I&C) systems and justifying their safety. This paper describes recently recognized challenges in demonstrating the safety of digital I&C systems and suggests possible ways to solve them. Some of the proposed solutions are light improvements in the everyday documentation practices, working methods and utilization of computerized support tools, while others would involve fundamental changes in the design and documentation philosophy that are more demanding to implement.

Key Words: safety demonstration, model-based systems engineering, safety argumentation, nuclear I&C

1. INTRODUCTION

Nuclear power plants are large-scale and long-term investments with specific risk potential. Therefore, their reliability and safety are important both for the industry and the society. Use of nuclear power is controlled by national regulations and international standards. Responsible utilities are required to submit a justification of the safety of the plant and its systems – a "safety demonstration" – to the local regulatory body.

The fundamental questions are, is the plant sufficiently safe and is it reasonable to rely on its safety demonstration. Because of the complexity of nuclear power plants and the emergent nature of safety, these questions are hard to answer. In particular, digital instrumentation and control (I&C) systems have turned out to be a challenge. Partly, it is due to their interdisciplinary role as a link between several plant systems, human operators and engineering disciplines. The complexity and failure mechanisms of software have introduced additional difficulties in safety analysis and demonstration.

Developing an understandable, transparent, convincing and complete safety demonstration in a cost-effective way is a difficult task, especially in the context of complex systems and varying regulatory environment. From the viewpoint of safety authorities, submittals of licensing documentation for regulatory review and approval could have more explicit argumentation, better traceability and clearer structure. From the licensee viewpoint, it has been a problem to collect and understand a complete set of requirements and to demonstrate compliance to them. Therefore, we can come to the conclusion that the nuclear power industry would benefit from more structured, systematic and harmonized practices in engineering I&C systems and justifying their safety. Possible

solutions can be found, for example, from other safety-critical domains, Systems Engineering (SE) principles and standards.

In the following, we discuss challenges in demonstrating the safety of I&C systems and suggest possible ways to solve them. The challenges are authors' interpretations summarized mainly from discussions with safety authorities and licensee organizations. The rest of this paper is organized as follows: As a background, Section 2 describes some related activities in authors' organizations. Section 3 gives an introduction to the subject and justifies the need of better safety demonstrations. The identified challenges are described in Section 4 and possible solutions in Section 5. Section 6 concludes the paper with discussion on possible future work.

2. BACKGROUND

VTT Technical Research Centre of Finland Ltd (VTT) has been working with nuclear I&C and safety assurance for a long time in several international and national projects. The publicly funded nuclear research in Finland is mostly organized under the National Nuclear Safety Research Programme (SAFIR, http://safir2018.vtt.fi/). In SAFIR, VTT has performed several studies on safety demonstration, system qualification and licensing, model-based systems engineering and probabilistic risk assessment of I&C systems (see e.g. [1,2,3,4,5]). The EU FP7 project HARMONICS (Harmonised Assessment of Reliability of Modern Nuclear I&C Software) addressed software verification & validation, software safety justification, and quantitative evaluation of software reliability [6].

The Institute for Energy Technology, Norway (IFE) is running the OECD Halden Reactor Project (HRP) and has performed several investigations related to safety demonstration and justification during the last few years. To understand the state of practice and challenges in safety demonstration and licensing of digital I&C systems, the HRP has performed interviews of nuclear regulators in a number of countries [7]. HRP has also performed an exploratory case study based on real nuclear power plant submittal documents to better understand the challenges of reviewing safety demonstration and give recommendations on how to improve the documentation [8,9].

A joint Nordic undertaking called PLANS (Planning safety demonstration) was carried out in 2015 by IFE, VTT, Solvina AB, and the Swedish Radiation Safety Authority (SSM). The PLANS project was building on the Safety Demonstration Plan Guide [10] that gives recommendations for planning and performing safety justification in modernization and newbuild projects including digital I&C systems. The PLANS project had close interaction with end users (licensees, regulators, consultants) and addressed some of the challenges of safety justification, e.g. the knowledge gap in understanding what a safety demonstration is and how it should be accomplished.

3. NEED OF BETTER SAFETY DEMONSTRATIONS

In regulated areas, 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. In fact, with the increasing complexity of systems there is a need to shift the traditional approach centered around anticipated events and single component failures towards an overall safety concept that could better handle (intended and unintended) dependencies and unexpected (external) events.

Building confidence in that the system can be trusted on, not only by their developers and owners but also by the society and public, is a hard task requiring lots of effort and documentation. Also the regulator spends typically person years to review the I&C systems of a nuclear power plant (newbuild or modernization) [11]. Therefore, a safety justification should be well organized, logically unarguable, unbiased, comprehensive, transparent and accessible to all relevant parties. A plan should be defined in advance to identify what kind of information, methods, resources and argument strategies will be used.

With the increasing amount of regulation and safety challenges there has been growing interest in structured safety justification approaches [12,13]. This can be seen also in the nuclear domain, even if the associated terminology is still rather unestablished. For example, in the UK, safety is typically justified with "safety cases". In addition, the Task Force on Safety Critical Software (TF-SCS) [14] has defined the term *safety demonstration* as "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" (See Figure 1). Even if this looks rather formal, a safety demonstration may or may not use the structured safety case presentation. Furthermore, some guidance exists for planning its preparation [10].

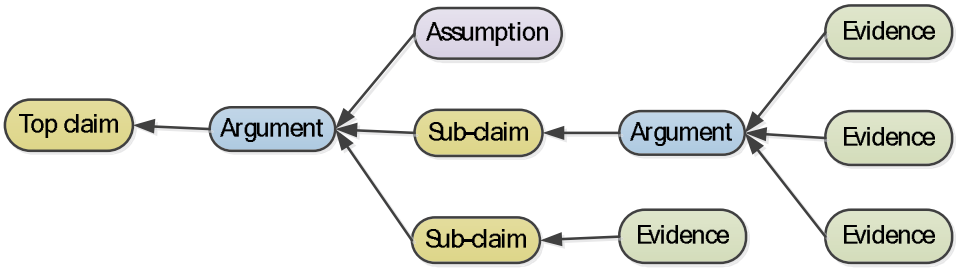

Figure 1. Claim, arguments and evidence structure adapted from [14, 16].

Figure 2 illustrates our understanding of the structure of licensing material. The term *safety case* is used here as an overall term referring to a totality of the safety argumentation and all the supporting material. As such, it is more than just the structured safety demonstration including, for example, the system descriptions, test reports and risk analysis results used as evidence (see [15]). Preliminary and final Safety Analysis Reports (SAR) are typically descriptive summary documents that contain limited amount of explicit safety justification. In our interpretation, safety demonstration as defined in [14] is an artefact stored in databases or in human-readable documents. *Structured safety case* is a special application of the (structured) *assurance case* [16] focusing on safety and based on a defined information model of claims, arguments and evidences. The word justification is used here as a general term. So, safety cases and safety demonstrations are its specializations.

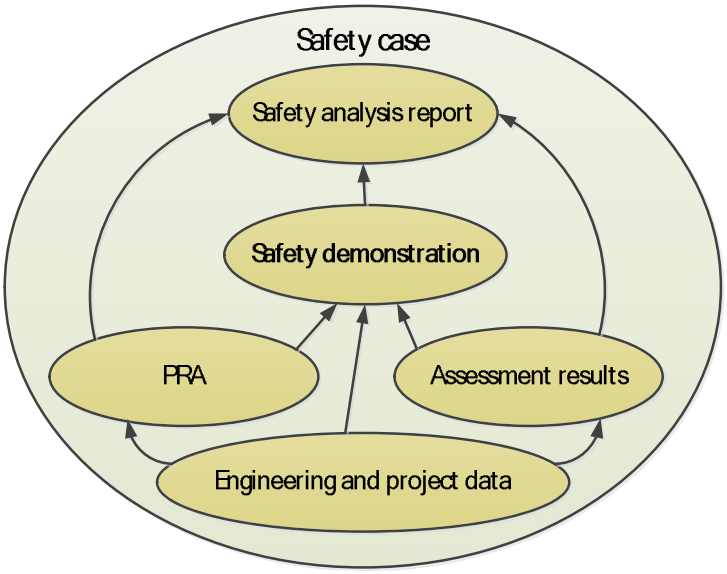

Figure 2. Position of safety demonstration in the overall safety justification material [1].

Safety demonstration applies, e.g., to I&C systems, components and their development processes. Accordingly, there are several terms related to obtaining regulatory acceptance. For example, in the Finnish practice, licensing applies only to the whole nuclear power plant. In the

context of I&C, qualification (of systems and components) refers to a process to demonstrate the ability to fulfil specified requirements. So, the process of developing a safety demonstration 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 or qualification planning. However, the terminology related to qualification activities, stakeholder responsibilities and required engineering artefacts in various situations (e.g. newbuilds and I&C renewals) is currently not quite clear and would benefit from shared reference models [2]. For example, [9] differentiates between three main aspects of safety demonstration: the argumentation, the documentation and the process aspects, which is a broader consideration of safety demonstration than given in the Common position [14].

In the sections below we discuss the challenges experienced in I&C qualification and ponder what kind of solutions would be available for improving the current practices.

4. CHALLENGES

This Section describes some challenges of safety demonstration that have been identified in interviews and co-operation with nuclear safety authorities and licensee organizations. The challenges listed here are partly based on the interviews of safety authorities reported in [7] and partly on the discussions with authorities and licensee organizations organized in 2016 as part of HRP's Safety Demonstration project and VTT's efforts in the SAUNA project (Integrated safety assessment and justification of nuclear power plant) in the SAFIR2018 research program. The challenges described below are authors' interpretations of the confidential interviews and discussions with experts.

Terminology

Similarly to safety classification schemes and regulatory requirements, the technical terminology differs country by country in the nuclear area. Also the terms in international standards often have differences and may leave space for interpretations (see e.g. www.electropedia.org for examples). This has always been a challenge in large newbuild and modernization projects and possibly will be also in the future despite harmonization efforts. As this is increasingly recognized in global projects and computer-based tools are increasingly used, there are better chances to minimize problems and misunderstandings related to terminology.

Communication

The review by IFE [17] raises up the differences in working cultures between experts from different countries. There are also "invisible barriers" between different engineering disciplines and parts of an organization, which concretize in the form of difficulties in understanding the interrelations between the work done in different teams and with other systems. Lack of communication is especially harmful for I&C systems because they are in central role having interfaces with several other systems and typically appear as black boxes for other systems.

Requirements

Most problems in developing and demonstrating safety of nuclear systems originate from wrong or incomplete requirements [17]. From regulators' viewpoint, this means the challenge of defining, writing, and communicating the regulatory requirements to the licensees, system suppliers and their support organizations. Also the regulators could be more precise and consistent with the decisions they make and what they require, which would facilitate the licensing activities.

From license holders' and also system suppliers' viewpoint, it is challenging to derive a coherent set of system and safety requirements as a solid foundation for design, testing, manufacturing, installation and safety justification. More attention could be paid to validation of requirements to

ensure that they are correct and complete. However, it is sometimes not enough to consider just the explicitly given requirements in the safety demonstration.

If the requirements are incomplete or vaguely formulated, it is impossible to communicate what the system should do, and also to verify that the developed system has the desired properties. In many cases, I&C system's functional requirements have been defined on too high level meaning that the system's behavior in rare and unexpected situations, such as unplanned system reboot, unexpected operator behavior, or effect of faulty signals, is not unambiguously defined. This makes the full scale utilization of, e.g., formal verification methods difficult. For example, model checking is dependent on exact formal representation of the system behavior (see e.g. [4]).

Traceability

Traceability between the higher and lower level requirements, as well as between the requirements and the produced evidence (test results, analyses, certificates, expert judgement) is vital for understanding the system behavior in detail, and to be able to convince oneself and also the external evaluators or a safety authority that the system is as stated and it has the desired properties. Designing and constructing systems so that there exists traceability between requirements, design, V&V, and implementation, and maintaining it while the design evolves and changes, is a big challenge. In some nuclear construction projects, traceability is maintained on document level and in others on more detailed requirements level. There are also examples where requirements traceability is maintained on requirement level only in systems with high safety significance, while lower safety significance systems have weaker traceability, e.g., document traceability.

The more detailed traceability is used, the easier it is to see the effects of changes, to justify the decisions made and to ensure that requirements have been correctly implemented. However, one of the challenges is the large effort needed to collect and record all the traceability information in manageable format, especially in the old power plants where the requirements may not be well documented and no strong traceability links exist.

Lack of personnel with multidisciplinary experience

Challenging nuclear projects need plenty of experts with deep knowledge on specific topics, but also experienced people having good overall understanding on plant and its requirements. It has been recognized in several cases that typically there are high quality experts with deep technical understanding within each discipline, but there are not so many people who fully understand in detail the overall system concepts and interrelations between different disciplines. This may lead to several other challenges described below and creates barriers between different disciplines.

Scattered information, fragmented documentation

Because a nuclear power plant is a complex system of systems applying several technologies, the requirements are scattered in several discipline-specific documents (like standards and regulatory guides). This concerns especially multidisciplinary systems, such I&C systems, that include e.g. electronics, automation, mechanics and human factors. It is challenging to develop and validate a coherent set of requirements for such systems.

In some cases, the same challenge applies also to the design documentation. In a bit provocative example, the design organization provides system level documentation for the licensee, who reviews and treats the documents without further information about their relationship with the interfacing systems and the overall plant architecture. This may lead to problems in later phases in the system life cycle.

Lack of detailed guidance in standards

Many standards and regulations are rather discipline-specific and there are not so many interdisciplinary documents available. In addition to being discipline-specific, many standards are

written for a certain scope as well as many nuclear regulatory guides. Some high level guides exist (such as IAEA safety guides) but typically they are not very helpful for detailed design.

Also [17] reports criticism against standards because they do not offer adequate guidance e.g. on how to achieve or implement a requirement or they lack guidance for new technologies. Sometimes the lack of details in standards is because of allowing application freedom for their users. This is understandable and, in principle, a good practice, but it leaves room for interpretation and may cause confusion.

Hierarchical design of I&C architecture

Typically, there are at least two I&C platforms involved in NPPs, one for operational I&C and another for safety I&C. They must satisfy many requirements concerning, e.g., independence and diversity. One of the challenges is to be able to develop and freeze the fundamental I&C architecture early enough. After that, system specific requirements can be derived based on the architecture level decisions. If design decisions affecting the overall I&C architecture and Defense in Depth concept are made separately on system level, there is chance that designers make faulty assumptions on the interfaces. That may lead to a situation where different I&C systems function correctly according to their own specifications, but their data exchange and mutual coordination fail. This challenge is related to the lack of communication and poor coordination of work in the design organization. So, it is important to have generalists in the team to look after the big picture, interfaces and links to other disciplines.

Documenting requirements and design principles over the life cycle

Inadequate documentation of design principles and system requirements poses challenges to system testing, test planning and most importantly to maintenance of systems. The planned 60+ year operating periods for newbuilds mean that I&C systems will have to be renewed a few times. Recent nuclear projects have got a lot of publicity for cost overruns and years of delays [18,19,20,21]. In most cases, the reasons are related to poorly defined or misunderstood requirements, inadequate system design, incomplete justification of safety, and difficulties in understanding the design decisions made tens of years ago. For example, the experiences of some recent I&C renewal and maintenance projects have shown that there have been big challenges in finding the requirements and design principles for original systems. This has caused delays, extra cost and also some confusing

situations related to the operation of I&C systems because of wrongly understood / interpreted original requirements.

Safety argumentation

Writing a safety argument can be also challenging. For example, the case study presented in [9] revealed many problems in a real safety demonstration document submitted to a regulator:

- Ambiguities coming from the use of natural language
  - Weak claims (e.g. proposition that only "suggests" some relevance with the claim)
  - Ambiguous references (e.g. target of word "this")
  - Unclear type of safety argument element (e.g. claim or context)
  - Ambiguity introduced through conjunctions like "and" and "or"
- Missing or hidden information
  - Implicit claims
  - Using an example instead of logically demonstrating the truth of a claim
  - Unclear relation of claims to the status of source documents (e.g. concept or validated specification)
- Missing structure of the safety arguments, partial arguments
  - Missing links between argument elements (e.g. implied through order and structure of the sentences, context or expected domain knowledge)
  - Missing links between hazard and solution (what hazards are eliminated by a solution)

To summarize the challenges described above that are based on our discussions with safety assurance and justification experts, the weaknesses identified above were specific occurrences of more general problems experienced in the safety assurance research community. Some of the challenges are caused by the inevitable difficulty of assuring safety of complex systems, while others are rather related to practical issues, such as working practices and training, large amount of information, variations in standardization and regulatory practices, and difficulties in communication between organizations and engineering disciplines.

5. POSSIBLE SOLUTIONS

The previous section described a set of identified challenges of safety justification. This section suggests possible solutions that could provide improvements to the current situation, either in the short term or in the long run. Thus, the simplest solutions are improvements in the documentation practices and "everyday" working methods. They could be embedded in the organizations' practices along with ongoing projects, step by step. On the other hand, the implementation of conceptual, organization wide changes, e.g. in the design or documentation philosophy, will require remarkable efforts and possibly also pilot projects to allow a smooth transition. It is evident that this would also require extensive utilization of computerized tools to support the new working processes.

Document and information management

Design documentation, safety analysis and V&V results, safety demonstrations, as well as the underlying regulations and standards, are a knowledge asset that must be communicated and maintained throughout the system life cycle. The solutions available today include, for example, good practices of technical writing and drawing, document and configuration management systems and design and plant databases. Irrespective of any formal structure for safety argumentation, these

methods can be applied for preparing better safety demonstrations. In particular, we can see the following opportunities for short-term improvements:

- learn to write understandable and unambiguous requirements, claims and arguments by using agreed terminology and recommended sentence structures
- provide guidance in good argumentation principles and avoidance of typical flaws in reasoning
- where practical, make use of tabular or graphical presentations of claim-argument-evidence type of relationships and traceability
- agree document templates (scope and structure) to be used in the whole project organization
- clarify the requirements for and role of explicit safety demonstration documents (and organizations) in the overall safety case.

Harmonization and standardization

The development of nuclear facilities is controlled by a large number of regulations and standards. Especially for digital I&C systems, they provide only limited guidance for regulatory and safety assessment. Licensing approaches are determined independently and with only limited information exchange [14]. The uncertainties and variability, besides the amount of information, have resulted in difficulties faced by vendors and utilities in achieving regulatory approval, especially for those operating in multiple countries [22].

As stated in the NUGENIA roadmap [23], there is a need for further harmonization and standardization. Already now there are many international and national groups sharing information and exploring opportunities for convergence of requirements and practices. For example, [14] gives guidance that licensees can follow to achieve an adequate safety demonstration of software-based I&C. Due to different traditions and complexity of the issues, harmonization takes time and effort. However, it is necessary and must be continued, also concerning safety demonstration by sharing best practices in the nuclear domain and in other critical areas.

Harmonization of terminology across the nuclear industry seems to be impossible due to differences in languages and national regulations. Thus, each project should write its own vocabulary and agree on the used terminology among the relevant stakeholders. Still, there is potential for misunderstandings but as long as the challenge is recognized, people can pay more attention to it and ask for clarifications when they notice possibility of confusion.

Besides harmonization, standardization bodies are moving towards electronic publication. Open-source standard development, online databases, modularization and formalization can be seen as solutions to the challenges of standard development and use. With distributed intelligence, internet and semantic technologies, “smart” standards and regulations can lead to a new way of engineering safety-critical products and applications. For example, relevant requirements can be found and fetched easily and used for defining system requirements, assessment criteria and claims in a safety demonstration.

Systems Engineering principles

Safety is an emergent property that requires seamless and resilient co-operation of all system elements. Therefore, a systematic and multi-disciplinary approach is needed. By definition of International Council on Systems Engineering, (INCOSE), Systems Engineering (SE) is one answer to that need. SE principles and related standards and guidelines can provide an overall framework also for the design of nuclear I&C. Of course, they need to be adapted to the specific requirements of nuclear power, for example in the form of reference models for design (e.g. [22]), safety management and licensing [2].

While SE is mostly concerned with the principles, artefacts and activities of engineering design, it should be seen in the wider context of the life cycle processes as defined, e.g., in [12]. Therefore,

SE is closely related to and partly overlapping with project management. For comprehensive safety demonstration, both systems and product and their development processes and organizations need to be assessed. So, we should have a consistent set of concepts, documents and models that link together technical I&C and safety engineering, project management and operation and maintenance processes.

Assurance case approach

A safety justification should be easily understandable, transparent, traceable, complete and logically flawless. It should also have a clear, modular structure that enables its efficient maintenance and allocation of responsibilities in the project organization and supply chain. Traditional documentation practices don't support these goals very well. More structure is needed to do that.

In fact, arguments have always been used - informally - to communicate reasoning and to persuade stakeholders (SACM). Also the idea of explicit, logics-based argumentation has been around for a while [25], and has been developed further by the research community (e.g. [24]). The ideas have been applied in many critical domains as structured safety cases. The way this is done has changed over the years, in response to major accidents and changes to the technology and economic environment [26]. This has led to international standardization of system assurance [16].

The goal of the structured *assurance case* approach is to improve the quality of reasoning and to facilitate stakeholder communications. An assurance case includes one or more top-level claims for properties of a system, argumentation regarding truth of the claims, and evidence and assumptions used as the basis of the argumentation [16]. Multiple levels of sub-claims and argumentation connect the top-level claims to the evidence. Assurance cases usually concern properties such as safety, human factors, and security. Accordingly, they are often called a safety case, usability case, security case, etc. As can be seen, the definition of *safety demonstration* by the nuclear regulatory experts above [14] is basically an assurance case, even though it is not required to apply the structured format.

On a more technical level, the Object Management Group (OMG) has worked for years to develop the Structured Assurance Case Metamodel (SACM) on the basis of ISO/IEC 15026, the Goal Structuring Notation (GSN) out of the University of York, the efforts of the Open Platform for EvolutioNary Certification of Safety-critical Systems (OPENCOSS), and some other work from the OMG [13]. The goal is to make system assurance more practical by providing a basis for tool support and exchange of assurance-related information. Already today, there are a number of safety case tools on the market [27], even if they don't necessarily support the OMG metamodel.

With this said we conclude that the structured assurance case approach would be useful in nuclear power, for example in the assessment of engineering artefacts, organizations and working processes, suitability analysis of equipment and components, system and plant level safety assessments, and in assessment of safety demonstrations themselves [1]. Safety cases provide a tool for data and knowledge management and for integrating diverse evidences from various disciplines. They also support communication and shared understanding among stakeholders and, if properly modularized, help in work allocation among service providers and manufacturers. A well-structured and transparent safety case reveals implicit assumptions and judgements and makes the review by the regulator easier, thus paving the way to a smoother and faster licensing.

There are benefits but also challenges in structured safety cases. The industry is often concerned about additional cost and paper work caused by a new approach. Safety cases may also drift away from everyday system operation and stakeholders, which can limit both their quality and usefulness. Development of safety cases requires trained personnel, defined working practices and tools. Even if these problems apply to any approach selected, the feasibility of structured assurances cases in nuclear I&C needs further studies. While experiences in other domains can help, a stepwise strategy would be necessary in the adaption of the principles to the existing nuclear practices. For example, learning to write more understandable natural language claims and arguments (cf. requirements) and

developing more structured (e.g. tabular) and modular document templates would be a good mid-term goal.

While being internally traceable, an assurance case/safety demonstration should be also linked to all relevant engineering artefacts used, for example, as evidence. This includes system specifications, project and V&V plans, V&V results, etc. In other words, an assurance case can't be planned and implemented afterwards or separately from the normal engineering work. In MBSE this means that the model-based assurance case is integrated with system models and project models. Such a solution would provide several opportunities, for example related to application specific terms and change management. In particular, MBSE would make it possible to determine the argument structure and truth value of some claims automatically.

Model-based approaches

One attractive solution is to move from documents based design and safety justification towards Model-Based Systems Engineering (MBSE). It can be defined as 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 [28]. Models can be used to guide designers in their work, and to enable design automation and computer-assisted system analysis, such as formal verification (e.g. model checking) and simulation-assisted I&C testing. Moreover, structured models help to link I&C specifications and PRA models.

Especially in preparing a safety demonstration, model-based analysis tools provide means to generate high-quality evidence. In particular, the structured assurance case described above is also a "model", which creates the opportunity to integrate the safety demonstration and models of I&C systems and their design processes. For example, automatic generation of assurance cases based on a formal Architecture Description Language (ADL) has been reported in [29]. According to [30] assurance cases generated in such way are expectedly more rigorous than manually constructed assurance cases. [30] states that the lack of integration with and limited traceability to design artefacts can undermine confidence in the assurance case. The paper describes a model-based approach, which allows integration between assurance case, design and process models and metamodels compliant with the Structured Assurance Case Metamodel (SACM) by OMG. These two approaches are attempts to automatically generate assurance cases for security of safety-critical software-based systems. Despite being of limited size and outside nuclear, these examples are an indication that similar approaches could be investigated also within nuclear industry. Based on a quick literature review, similar work has not been performed in large scale in nuclear sector so far.

6. CONCLUSIONS AND PLANS FOR FUTURE WORK

The design and construction of nuclear power plants is controlled by a large number of standards and regulations. Especially for digital I&C systems, they provide only limited guidance for preparing safety demonstrations, which appears to be difficult for various reasons. This paper discusses those challenges and presents possible solutions for improving the current state of affairs. The presented ideas are based on several interviews and discussions with safety experts working for the nuclear licensee companies and safety authorities.

Two main categories of challenges can be identified: The first is the inevitable difficulty of assuring safety of complex systems, and the other one is related to more practical issues, such as working practices and training, large amount of information, variations in standardization and regulatory practices, and difficulties in communication between organizations and engineering disciplines.

The suggested solutions in this paper include improvements in the documentation practices and "everyday" working methods that could be embedded along with the ongoing projects. More demanding and harder-to-implement solutions, such as increased utilization of model-based approaches and computerized tools, would require, in many cases, organization wide changes to the

design or documentation philosophy. Research efforts and pilot projects would be in role to allow smooth transition.

The challenges and potential solutions for safety justification evolve over time. Thus, the intention of the authors is to update the knowledge base of safety justification practices, challenges and tools on a regular basis with all stakeholders in the nuclear field and the research community. The plan is to organize the information about the most impactful topics into a set of guidelines called Safety Demonstration Framework and update it according feedback and new developments. Performing case studies on real, relatively recent submittals of licensing documentation offers also relevant feedback and experience, and thus our plan is to continue that series of work as well. Software tools will certainly play an important role in transition to model-based, structured ways of preparing safety demonstration. Investigating the tools for, e.g., formalizing requirements and modelling and analysing I&C architecture and its Defence in Depth capabilities, will be an important future activity. Also following the development and evaluating the existing tools used to support safety justification provides possibilities to envision new tools to fill the gaps of the current ones.

7. ACKNOWLEDGMENTS

This work has been supported by the SAUNA project (Integrated safety assessment and justification of nuclear power plant automation) in the context of the SAFIR2018 programme (The Finnish Research Programme on Nuclear Power Plant Safety 2015–2018), and the OECD Halden Reactor Project's Safety Demonstration activity.

8. REFERENCES

1. Valkonen, Janne; Tommila, Teemu; Alanen, Jarmo; Linnosmaa, Joonas; Varkoi, Timo, Views on safety demonstration and systems engineering for digital I&C, 39th Enlarged Halden Programme Group Meeting, EHPG 2016, 8 - 13 May 2016, Oslo, Norway. Institute for Energy Technology (2016), 13 p.
2. Alanen, Jarmo; Tommila, Teemu. 2016. A reference model for the NPP I&C qualification process and safety demonstration data, VTT. 43 p. + app. 21 p. Research Report; VTT-R-00478-16
3. Tommila, Teemu; Alanen, Jarmo. 2015. Conceptual model for safety requirements specification and management in nuclear power plants. Espoo, VTT. 120 p. + app. 26 p. VTT Technology; 238, ISBN 978-951-38-8365-2
4. Pakonen, A., Valkonen, J., Matinaho, S., Hartikainen, M., 2014. Model checking for licensing support in the Finnish nuclear industry. International Symposium on Future I&C for Nuclear Power Plants, ISOFIC 2014, 24 - 28 August 2014, Jeju Island, Republic of Korea, Korean Nuclear Society. 9 p. http://www.vtt.fi/inf/julkaisut/muut/2014/ISOFIC_2014_Pakonen_et_al_FINAL.pdf
5. Authén, Stefan; Bäckström, Ola; Holmberg, Jan-Erik; Porthin, Markus; Tyrväinen, Tero. 2016. Modelling of DIgital I&C, MODIG - Interim report 2015, Nordic nuclear safety research. 85 p. NKS-R reports; NKS-361, ISBN 978-87-7893-445-1, http://www.nks.org/scripts/getdocument.php?file=111010213493819
6. Valkonen, Janne; Guerra, S.; Bloomfield, R.; Thuy, N.; Märtz, J.; Liwång, B.; Hämäläinen, Jari. 2014. HARMONICS: EU FP7 Project on the Reliability and Safety Assessment of Modern Nuclear I&C Software. International Symposium on Future I&C for Nuclear Power Plants (ISOFIC 2014), Jeju Island, Repulic of Korea, 24 - 28 August 2014, Korean Nuclear Society
7. P. Karpati, A. A. Hauge, V. Katta, and C. Raspotnig, "Safety Demonstration and Justification of DI&C Systems in NPPs – Elicitation Interviews with Regulators", HWR-1112, OECD Halden Reactor Project, 2014a

8. P. Karpati, C. Raspotnig, V. Katta, and A. A. Hauge, “Safety Demonstration and Justification of DI&C Systems in NPPs – Future Directions”, HWR-1139, OECD Halden Reactor Project, 2014b
9. P. Karpati, K. C. Attwood, S. Nair, V. Katta, and C. Raspotnig, “Extracting the safety argument from an interim safety demonstration – A case study from the nuclear field (Part 1: Argument comprehension)”, HWR-1149, OECD Halden Reactor Project, 2016.
10. Elforsk 2013. Safety Demonstration Plan Guide A general guide to Safety Demonstration with focus on digital I&C in Nuclear Power Plant modernization and newbuild projects. Elforsk rapport 13:86, 63 p.
11. NEA/CNRA/R(2014)7, CNRA Working Group on the Regulation of New Reactors, Report of the Survey on the Design Review of New Reactor Applications, Volume 1, Instrumentation and Control, June 2014
12. ISO/IEC 15288: 2015. System Life Cycle Processes.
13. OMG 2015. Structured Assurance Case Metamodel (SACM) Version 2.0.
14. Common position 2014. Licensing of safety critical software for nuclear reactors - Common position of seven European nuclear regulators and authorised technical support organisations.
15. 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
16. ISO/IEC 15026-2:2015, Systems and software engineering – Systems and software assurance – Part 2: Assurance case
17. P. Karpati, A. A. Hauge, V. Katta, and C. Raspotnig, Safety demonstration challenges and recommendations in the nuclear field, Safety and Reliability of Complex Engineered Systems, ESREL 2015, Edited by Luca Podofillini, Bruno Sudret, Bozidar Stojadinovic, Enrico Zio, and Wolfgang Kröger, CRC Press 2015, Pages 3791–3799, Print ISBN: 978-1-138-02879-1, eBook ISBN: 978-1-315-64841-5, DOI: 10.1201/b19094-497
18. WNA 2016. Nuclear Power in Finland. World Nuclear Association, registered in England and Wales, number 01215741. June 2016. http://www.world-nuclear.org/information-library/country-profiles/countries-a-f/finland.aspx
19. FT 2016. Financial Times, EDF’s French nuclear plant faces years of further delay, March 20, 2016, Kiran Stacey and Tom Burgis, http://www.ft.com/cms/s/0/73d62552-ec65-11e5-bb79-2303682345c8.html#axzz4IKbEPSHp
20. NEI 2014, Nuclear Engineering International, Oskarshamn 2 upgrade and modernization delayed, 24 June 2014, Progressive Media Group Limited, http://www.neimagazine.com/news/newsoskarshamn-2-upgrade-and-modernization-delayed-4300849
21. PEI 2013, Power Engineering International, Oskarshamn 3: How not to prepare a power uprate, 02/01/2011, Volume 19, Issue 2, http://www.powerengineeringint.com/articles/print/volume-19/issue-2/features/oskarshamn-3-how-not-to-prepare-a-power-uprate.html
22. EPRI 2014. Principles and Approaches for Developing Overall Instrumentation and Control Architectures that Support Acceptance in Multiple International Regulatory Environments. Electric Power Research Institute, Inc. (EPRI), technical report 3002002953, 366 p.

23. NUGENIA Roadmap 2013, Nuclear Generation II & III Association, http://s538600174.onlinehome.fr/nugenia/wp-content/uploads/2014/02/NUGENIA_roadmap.pdf
24. Kelly, T. P. 1998. Arguing Safety – a Systematic Approach to Managing Safety Cases. 341 p. PhD Thesis, University of York, September 1998.
25. S. Toulmin, "The Uses of Argument", Cambridge, University Press, 1958.
26. Health Foundation 2012. Using safety cases in industry and healthcare. A pragmatic review of the use of safety cases in safety-critical industries – lessons and prerequisites for their application in healthcare.
27. Linnosmaa, J. 2016. Structured Safety Case Tools for Nuclear Facility Automation. Master's Thesis. Tampere University of Technology, 68 p.
28. 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.
29. R. Hawkins, I. Habli, D. Kolovos, R. Paige, T. Kelly, Weaving an Assurance Case from Design: A Model-Based Approach, IEEE 16th International Symposium on High Assurance Systems Engineering (HASE), 8-10 Jan. 2015, DOI: 10.1109/HASE.2015.25
30. A. Gacek, J. Backes, D. Cofer, K. Slind and M. Whalen, Resolute: an assurance case language for architecture models, in the Proceedings of the 2014 ACM SIGAda annual conference on High integrity language technology, Pages 19-28, Portland, Oregon, USA — October 18 - 21, 2014 , ACM New York, NY, USA, 2014, ISBN: 978-1-4503-3217-0, http://dx.doi.org/10.1145/2663171.2663177.