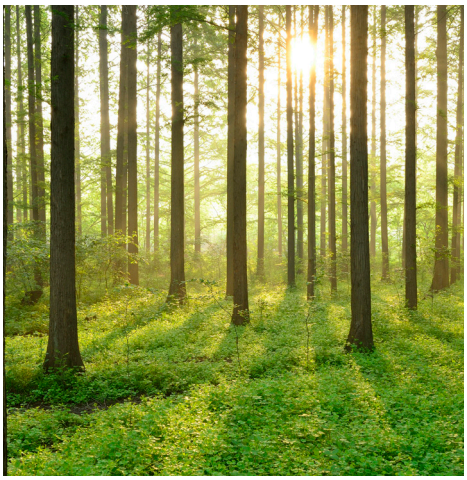
SAFETY DEMONSTRATION PLANNING FOR DIGITAL I&C PROJECTS

REPORT 2016:267



ENSRIC

Energiforsk

Safety Demonstration Planning for Digital I&C Projects

Challenges, Future Directions and Improving Guidance

VIKASH KATTA, INSTITUTE FOR ENERGY TECHNOLOGY, NORWAY
PONTUS RYD, SOLVINA AB, SWEDEN
JANNE VALKONEN, VTT TECHNICAL RESEARCH CENTRE OF FINLAND LTD, FINLAND

ISBN 978-91-7673-267-0 | © 2016 ENERGIFORSK

Energiforsk AB | Phone: 08-677 25 30 | E-mail: kontakt@energiforsk.se | www.energiforsk.se

Foreword

When safety related instrumentation and control systems in a nuclear power plant are renewed, the licensee has to submit a safety demonstration to document that the change does not affect the safety of the plant in any way. This often results in vast amounts of documentation. There are large differences in current practice in different countries for safety demonstration, as well as some common challenges.

This project has addressed some of these challenges by providing detailed guidance on how to plan and perform safety demonstration for digital instrumentation and control systems in nuclear power plants. A safety demonstration plan guide was developed in a previous project, and is presented in Elforsk reports 13:85 and 13:86. This guide has been further refined in this project.

The activity was carried out with support from ENSRIC, Energiforsk Nuclear Safety Related I&C research program. ENSRIC is focused on safety related I&C systems, processes and methods in the nuclear industry. The three focus areas of the program are:

- LTO of existing analogue platforms
- Asset management of existing digital platforms
- Emerging technologies.

The ENSRIC results are used in the plant development process, including managers, strategic teams, analysts and implementation teams at the NPPs and at the authorities, to contribute to safe and robust I&C systems that promotes low Life Cycle Cost. The program is financed by Vattenfall, Uniper, Fortum, TVO, the Swedish Radiation Safety Authority, Skellefteå Kraft and Karlstad Energi.

NKS-357
ISBN 978-87-7893-441-3

Safety Demonstration Planning for Digital I&C Projects – Challenges, Future Directions and Improving Guidance

Vikash Katta[1]

Pontus Ryd[2]

Janne Valkonen[3]

[1]Institute for Energy Technology, Norway

[2]Solvina AB, Sweden

[3]VTT Technical Research Centre of Finland Ltd, Finland

February 2016

Abstract

Licensee should submit a safety demonstration case and supporting documentation to the regulator describing how safety has been achieved. However, more often, submittals to regulators consist of vast amount of documentation without providing any explicit argumentation on how this documentation supports safety demonstration. There are large differences in current practice in different countries for safety demonstration, as well as some common challenges. The project aims to address some of these challenges by providing detailed guidance on how to plan and perform safety demonstration for Digital Instrumentation and Control (DI&C) systems in Nuclear Power Plants (NPP).
The project elicited the experiences and challenges related to safety demonstration of DI&C facing the NPP industry by organizing industry expert workshops. The experts who participated in the workshop recommended future activities for the project. These future activities reflect the needs of the industry in order to address some of the challenges related to safety demonstration. One need of the industry is the clarification of how to perform safety demonstration and how safety demonstration is related to the existing system engineering process. Another need is a multidisciplinary approach for safety demonstration that should involve personnel from different disciplines (e.g. I&C, safety, management, process) across organisation at the early stages of the project and plan for how to achieve and demonstrate safety.
The project has refined a guide for planning safety demonstration, called Safety Demonstration Plan Guide (SDPG) to address some of the challenges and needs of the industry. As per SDPG, the contents of the safety demonstration can be organised effectively using a set of Safety Subject Areas (SSA). SSA is an aspect of safety and the complete set of SSAs constitute the safety demonstration case. SDPG's refinement involved detailing on some of the SSAs. As a starting point for future work, the project has provided an overview on the topic of system engineering and the role of safety demonstration in the overall systems engineering process.

Key words

Safety demonstration, safety demonstration planning, safety case

NKS-357
ISBN 978-87-7893-441-3
Electronic report, February 2016
NKS Secretariat
P.O. Box 49
DK - 4000 Roskilde, Denmark
Phone +45 4677 4041
www.nks.org
e-mail nks@nks.org

Safety Demonstration Planning for Digital I&C Projects – Challenges, Future Directions and Improving Guidance

Phase I (2015) Report from the NKS-R PLANS activity

(Contract: AFT/NKS-R(15)117/10)

Vikash Katta[1]
Pontus Ryd[2]
Janne Valkonen[3]

[1]Institute for Energy Technology, Norway
[2]Solvina AB, Sweden
[3]VTT Technical Research Centre of Finland Ltd, Finland

Table of contents

Acknowledgements

The work reported in this report is 50% funded by Nordic Nuclear Safety Research (NKS). The rest is funded by the Halden Reactor Project, The Finnish Research Programme on Nuclear Power Plant Safety 2015 - 2018 (SAFIR 2018), and ENSRIC group from Energiforsk. There is a cross-fertilisation of knowledge and results between these projects.

We thank Niclas Larsson, SSM, for his contributions to the project. We thank our colleagues at the Institute for Energy Technology, Solvina, VTT, and SSM for providing input to the project.

NKS conveys its gratitude to all organizations and persons who by means of financial support or contributions in kind have made the work presented in this report possible.

Executive summary

This report presents the activities and the results from the Phase I (2015) of the NKS-R PLANS (Planning Safety Demonstration) project. The aim of the PLANS project is to provide guidance on safety demonstration planning for Digital Instrumentation and Control (DI&C) systems in Nuclear Power Plants (NPP). The project addresses some of the challenges of safety demonstration, e.g. knowledge gap on what a safety demonstration is and how it should be performed, by providing detailed guidance on how stakeholders can plan for safety demonstration. The activities of the project in 2015 resulted in, among other things, organising industry expert workshops to better understand the practices and challenges related to performing safety demonstration and to elicit future directions on improving guidance on how to plan and perform safety demonstration. The activities also included further development of a guide for planning safety demonstration.

With the help of industry expert workshops the project elicited experiences and challenges on safety demonstration from the NPP industry experts, in particular experts from the Nordic NPP end user organisations. It was widely recognised by the experts that there is a lack of awareness of safety demonstration in organisations and there is a lack of information flow between personnel belonging to various disciplines (e.g. I&C and other engineering processes, management, safety) across organisations involved in development and demonstration processes. In addition to the challenges, the project also identified the needs of the industry experts with respect to safety demonstration and their recommendations on how these can be addressed by future activities of PLANS. Some of the recommendations from the experts include proposing a multidisciplinary approach for safety demonstration and planning that involves personnel from different disciplines across organisations at the early stages of the project to plan for how to achieve and demonstrate safety. Experts also suggested that PLANS should consider clarifying the concepts underlying safety demonstration and the role of safety demonstration in the overall (existing) systems engineering process.

PLANS addressed some of the safety demonstration challenges by further developing a guide for planning safety demonstration, called Safety Demonstration Plan Guide (SDPG). Ongoing work on refining SDPG involves detailing an approach to plan for safety demonstration covering the entire development lifecycle and identifying the development artefacts that could be used as evidence to justify the claims on (acceptable) safety of the system. Moreover, the concepts of safety demonstration and how safety demonstration related to systems engineering process are being clarified. The further development of SDPG, as per the project plan, will be carried out over a three years period.

PLANS has established a Nordic network of competence on nuclear DI&C safety demonstration (NordicNSEC), which is a forum for knowledge exchange among experts from multidiscipline. This network is being extended by inviting experts from several end user organisations. PLANS see this network as a medium to increase awareness on demonstration, to discuss experiences in safety demonstration, and to communicate relevant work being performed by the Nordic and international community, including the results from PLANS.

1. Introduction

Digital Instrumentation and Control (DI&C) systems in new nuclear power plants (NPP) and modernisations of existing plants are becoming increasingly complex (Karpati, 2014). I&C is the "nervous system" of the whole plant, and its safety (and quality) demonstration inherently integrates the different systems and components constituting the overall plant. Such integration is by nature multi-disciplinary and therefore calls for a multidisciplinary approach integrated with the overall design and integration efforts. In practice, the interfaces and information flow between the disciplines (I&C, process, mechanical, electrical, etc.) is not good enough. For example, the interface between plant design and I&C design is not clearly described since the scopes and boundaries of the actual systems are often unclearly defined and therefore the completeness of I&C requirements towards plant design cannot be (safety) demonstrated – nor can quality.

More often, submittals to regulators (submittals on the approval of the commissioning of DI&C changes) consist of vast amount of documentation without providing any explicit argumentation or explanation on how this documentation supports safety demonstration. Moreover, safety demonstration tends to focus on one (snapshot) of safety assessment report and not the entire lifecycle. In a series of interviews with nuclear regulators from different countries (Karpati, 2014), a widely mentioned issue is that important information (e.g., argument and evidence) is often not properly structured in submittals to regulators, or the information is not presented at the appropriate abstraction level. The same issues were also pointed out by the experts participating in a workshop on safety demonstration challenges with DI&C systems (Hauge et al., 2014). During the workshop, the lack of guidance to the industry on how to organise information or evidence was identified as one of the causes leading to such issues. As an example of the lack of guidance, it was stated during the workshop (Hauge et al., 2014) that "in the 2004 version of IEEE 1012, there is a requirement to perform hazard analysis, but there are no requirements for the upper level I&C systems for computer system hazard analysis. In this sense, it is difficult for the industry to use the guidance in standards for organising evidences when there is no guidance on mapping hazards with properties of the computer system. The mapping should be explicitly defined and given as guidance to the industry." (Hauge et al., 2014) To solve this issue, guidance should be provided on safety demonstration planning of what kind of evidence should be produced in each stage of the development process. The guidance should also address how to organise the evidences in a logical manner. However, current guidance on how to achieve safe DI&C systems within the nuclear domain does not clearly describe how safety demonstration should be planned and realised. In this sense, there is a lack of information providing detailed guidance on how to effectively and efficiently plan for and demonstrate safety.

The PLANS (Planning Safety Demonstration) project was started with the objective of improving guidance on safety demonstration planning for DI&C systems in NPPs on selected topics. This report presents the work performed under the PLANS project for the year 2015. The work being carried out in PLANS is in collaboration with other projects being carried out at project member organisations, in particular the Halden Reactor Project (The Halden Reactor Project, 2015), SAFIR 2018 (SAFIR, 2015), and ENSRIC group (ENSRIC, 2015) from Energiforsk (Energiforsk, 2015). The PLANS project originates in the Halden Reactor Project (HRP) coordinated by the Institute for Energy Technology (IFE), in whose frame the participating partners cooperated before and established their common goals for improvements in the Nordic nuclear industry for the PLANS project. PLANS is embedded to the Finnish Research Programme on Nuclear Power Plant Safety, SAFIR2018. This enables

efficient communication with the Finnish NPP stakeholders and gives additional forum to distribute project's results and get concrete input to the research topics addressed in PLANS.

2. Glossary

The terms used in this report are defined here. For additional terminology on safety systems engineering and demonstration refer to (Bel V et al., 2014; Axenborg, 2013; U.S. Nuclear Regulatory Commission, 2015).

Assumption

Definition: "A premise that is taken for granted, i.e., not validated. Often, It is taken for granted implicitly." (U.S. Nuclear Regulatory Commission, 2015)

Claim

Definition: "A true-false statement about the value of a defined property of a system." (U.S. Nuclear Regulatory Commission, 2015)

Similar terms: Assertion, Goal, Proposition

Context

Definition: "A basic Argument Element Type representing factors which might have influence on the subject referred to by the Argument Element to which it is attached. Contexts can be attached to claims or evidence. A *Context for a Claim* includes facts, information, or observations which are necessary to establish the truth of the claim, or references to information referred to in the claim. A *Context for Evidence* is likely to contain an assertion (which may need to be established by further argument) regarding the trustworthiness or correctness of the evidence, or an explanation of the evidence or some feature of the evidence. Context should always linked to an Argument Element, otherwise it is superfluous." (Karpati, To be published)

Note: "Argument Element Type: It determines the role of an Argument Element in the Argument. The basic Element Types in an Argument are: Claim, Context and Evidence." (Karpati, To be published).

Similar terms: Environment, Scope of validity

Evidence

Definition: "A basic Argument Element Type representing artefact containing information, facts or observations presented to underpin a claim." (Karpati, To be published)

Definition: "Data supporting the existence or truth of something." (U.S. Nuclear Regulatory Commission, 2015)

Similar terms: Data, Solution, Ground

Licensee

Definition: "The owner of the Nuclear Power Plant (NPP) is also the owner and responsible for the license for nuclear operation of the plant. In a NPP project perspective the project sponsor is usually the licensee" (Axenborg, 2013).

Regulator

Definition: "The regulatory body and/or authorised technical support organisation acting on behalf of its authority" (Bel V et al., 2014).

Argument

Definition (for Reason): “Argument; a logical sequence or series of statements from a premise to a conclusion (adapted from entry for argument in (Merriam-Webster, 2016)).” (U.S. Nuclear Regulatory Commission, 2015)

Definition: “A collection of Basic Arguments where the conclusions of some Basic Arguments are the premises of others. When used in a strict sense, the Basic Arguments should form a connected directed graph structure which contains exactly one node with outdegree 0 (without any outgoing directed edge) and no cycles.” (Karpati, To be published)

Note: “Basic Argument: Two or more propositions, one of which is the conclusion, the other(s) being direct premise(s) for that conclusion.” (Karpati, To be published).

Similar terms: Reasoning

Safety demonstration

Definition: “The 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” (Bel V et al., 2014).

Definition: “Documents, activities, and theoretical constructs intended to demonstrate that a system meets its safety requirements. There are three main aspects of Safety Demonstration of a system:

- Safety Demonstration as an Intellectual Product: A safety argument supporting a selected set of claims on the sufficient safety of a system in a given environment.
- Safety Demonstration as a Collection of Documents: A collection of documents representing the intellectual product aspect of safety demonstration in a written, assessable form.
- Safety Demonstration as a Process: A process handling the production and lifecycle of the intellectual product and document aspects of safety demonstration.” (Karpati, To be published)

Safety demonstration plan guide

Definition: “A guideline or a document describing an approach for how to plan and perform safety demonstration. The guide supports the development of the safety plan” (Axenborg, 2013).

Safety plan

Definition: “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” (Bel V et al., 2014).

Similar terms: Safety demonstration plan

Safety Subject Area

Definition: “Aspect of safety. The complete set of SSA constitute the Safety Demonstration Case” (Axenborg, 2013).

3. PLANS project

The objective of the PLANS project is to improve guidance on safety demonstration planning for DI&C systems in NPPs by building upon existing guidance and models for safety justification. PLANS achieves this objective by building upon the existing work on safety demonstration, in particular Safety Demonstration Plan Guide (SDPG) (Axenborg, 2013), and develop it further in selected areas perceived as most relevant by Nordic and international experts. In the long term, PLANS intends to define a framework for effective and efficient DI&C safety demonstration planning which can serve as a harmonized foundation between the Nordic countries. The project is planned with 3 phases (I, II, III) that will be performed during the period of 2015-2017. If funded, Phase II and Phase III will continue as planned.

The following are the achievements of the project in 2015. Each of them will be discussed in detail in the next sections.

- Better understanding of the relevant challenges associated with DI&C safety demonstration and how they can be effectively addressed in the early stages of development projects which benefits all concerned stakeholders on a general level. This was achieved by inviting experts from the NPP end user organisations to workshops organised by PLANS, and by eliciting their experiences, including challenges, with safety demonstration. See Section 5 for descriptions on the workshops and the elicited challenges.
- Refining guidance for DI&C safety demonstration planning on selected topics offering better work routine, harmonized practises and cost savings for stakeholders and thus an expected competitive edge for Nordic end user organizations. SDPG was refined according to the input collected from the experts during the PLANS workshops. SDPG is being extended by detailing the guidance on safety subject areas (SSAs) of SDPG. See Section 6 and 7 for further information.
- PLANS has established a Nordic network of competence on nuclear digital I&C safety demonstration (NordicNSEC), which is a forum for knowledge exchange among experts from multidiscipline (NordicNSEC, 2015). See Section 8 for details on NordicNSEC.

Phase II and Phase III will continue to improve guidance in SDPG by progressively seeking input from NPP end user organisations. NordicNSEC network will be maintained and will be strengthened by inviting more experts from Nordic NPP community.

4. Background

4.1. Safety demonstration and planning

Safety demonstration is “the 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” (Bel V et al., 2014). Licensee should submit a safety demonstration case (also referred to safety case, assurance case) and supporting documentation to the regulator describing how (acceptable) safety has been achieved. There are large differences in current practice in different countries for safety demonstration, as well as some common challenges. The practices and challenges have been identified in project members’ earlier work on interviewing nuclear regulators from different countries (Karpati et al., 2014) and through an expert workshop on safety demonstration (Hauge et al., 2014). Some of these challenges were also pointed out by experts during industry workshops organised by PLANS in 2015. It was pointed out by the experts that some of the challenges could be resolved by improving the communication between stakeholders as

early as possible in the project. Stakeholders should plan on how safety will be achieved during the project, how it will be demonstrated, and come to a common understanding. One way to achieve this is to have a safety demonstration plan, which should be produced in the beginning of the project that "shall identify the claims that are made on the system, the types of evidence that are required, the arguments that are applied, and when this evidence shall be produced" (Bel V et al., 2014). It is important that the licensee and supplier plan for safety, and communicate their plans to the safety authority. A thorough planning process at the early stages of the project that includes all stakeholders facilitates a common understanding of how safety will be achieved. However, as mentioned earlier, there is a lack of detailed guidance on how to effectively plan for and demonstrate safety.

4.2. Safety demonstration plan guide

Energiforsk's (former ELFORSK) ENSRIC group recognized the problems with safety demonstration described above and initiated/financed the project on the development of safety demonstration plan guide (SDPG) as a means to address the problems. One of the PLANS project members, Solvina AB, got the mission to develop the guide. SDPG is a "guide for how to plan for and perform demonstration of safety in modernization- and new build projects including digital instrumentation and control (I&C) systems within the nuclear power industry" (Axenborg, 2013). The guide supports the development of a safety demonstration plan.

As described in the guide, safety demonstration should be performed in close cooperation with project development process and safety analysis reporting. Safety demonstration reports provide explicit safety argumentation and references for the specific project relevant subjects that the overall balance of detail in the safety analysis reports is not suitable for. Safety demonstration reports can also provide the description and assessment discussion of a certain issue gathered (for e.g. how independence is considered in I&C architecture), where the corresponding information may be scattered in several bits and pieces in the safety analysis reports, due to format constraints. Figure 1 taken from SDPG shows that safety demonstration supports the project process with overall structure and coordination of information, and provides the needed complementary information to safety reporting as a part of present licensing process. The figure also shows the phases of safety demonstration as used in the guide, namely *Safety Demonstration Planning*; *Qualification of the Overall Project and Product Conceptual Design*; *Qualification of Product Basic Design*; *Qualification of Product Detailed Design including FAT*; *Qualification of Product as Installed and Commissioned including SAT*; *Qualification of Product at One Year of Operation including Outage*.

Performing safety demonstration as recommended by SDPG will result in development of safety demonstration plan (SDP) and safety demonstration reports (SDR). Figure 2 presents a typical life cycle overview diagram highlighting the time wise correlation between the activities of the main project stakeholders (Regulator, Licensee, NPP project and Supplier) and the outputs of the safety demonstration that are SDP and several versions of SDR. While SDP is an output of *Safety Demonstration Planning* phase, versions of SDR are produced during remaining phases of the safety demonstration.

As per the SPDG, a safety demonstration is preferably based on a Safety Demonstration Case (SDC). SDC can be seen as the explicit safety argumentation on how NPP is safe after the implementation of a modernization or new build project. As shown in Figure 3, the contents of the safety demonstration can be organised effectively using a set of Safety Subject Areas (SSA), where each SSA addresses an important aspect of safety. It should be demonstrated

that every SSA is sufficiently addressed by providing arguments and evidences that are assessed for completeness, correctness and consistency (referred to as 3C).

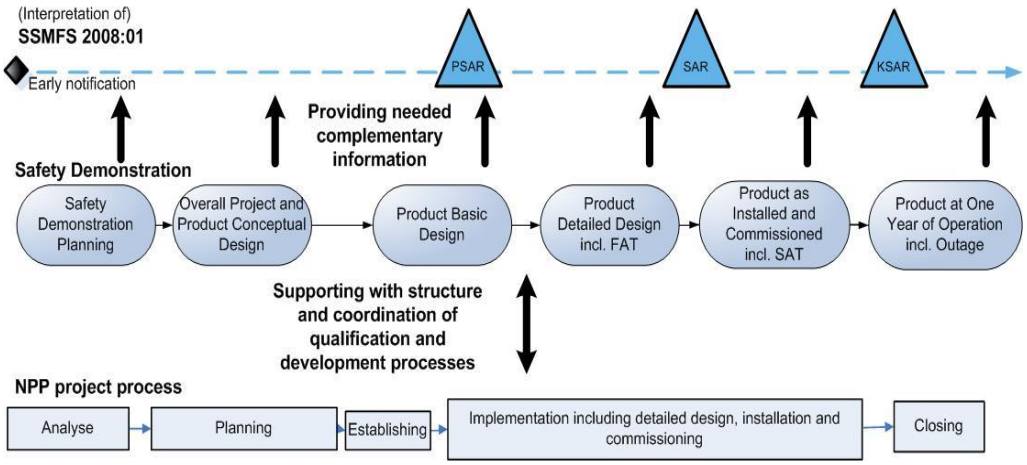


Figure 1. Safety Demonstration supports the development of safety analysis reports (SAR) and the licensing process between the Licensee and the regulator. The reporting of safety as illustrated in the top of the figure is an interpretation of the text in SSMFS 2008:1- Chapter 4, section 2 and General advice to Chap. 4, section 5 (excerpt from (Axenborg, 2013))

SDC is defined early in the project, i.e. in the planning phase of the safety demonstration life cycle, and agreed upon and committed to by all stakeholders involved. For each SSA, scope and purposes are formulated and the demonstration strategy including type of evidence (typically V&V-activities such as reviews, inspections, audits, analysis and tests) to be used should be defined. While SDC is initially defined in the planning phase of the safety demonstration, it is updated in the later phases of safety demonstration as detailed information on evidence is available.

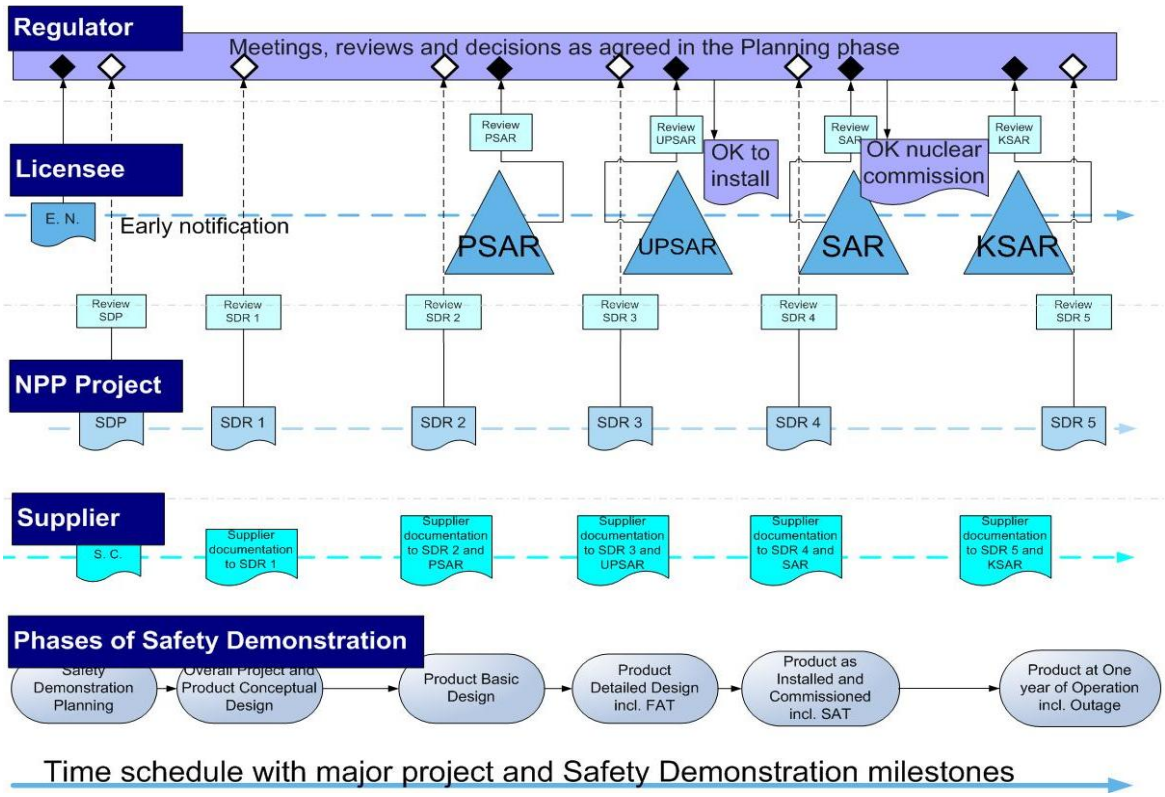


Figure 2. Typical lifecycle overview diagram in a safety demonstration plan (excerpt from (Axenborg, 2013))

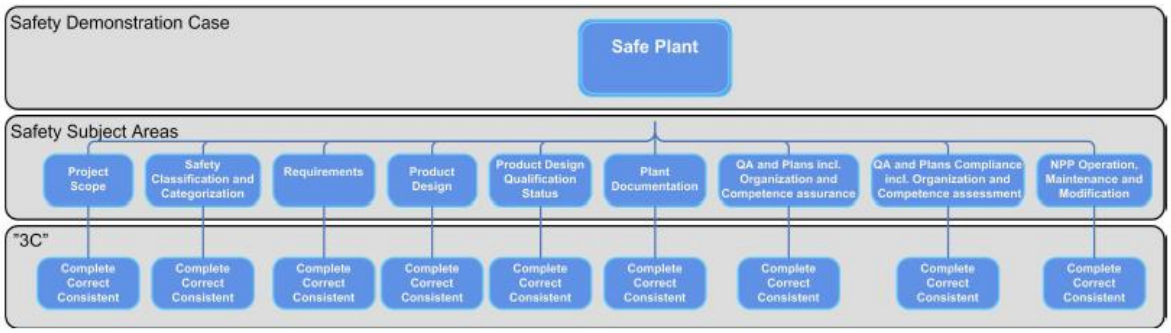


Figure 3. Safety demonstration case and safety subject areas (excerpt from (Axenborg, 2013))

SDPG provides high-level guidance on SSAs including their purpose and scope is defined along with some advice on a strategy to perform the demonstration. SDPG states that safety case methodology is an attractive method to define the scope of the SSAs is to formulate claims or claims hierarchies using a safety case methodology. However, SDPG does not provide a detailed strategy on what type of claims and evidence should be collected and how they should be organised together to demonstrate 3C for each of the SSAs.

5. PLANS Workshops

PLANS organised two workshops as its main activities in 2015. The aim of organising the workshops was three fold: involve NPP end user organisations in the project, increase awareness on safety demonstration, disseminate PLANS results and collect feedback from the NPP community. With the help of participation of experts from the end user organisations in PLANS workshops, the project is able to interface with the ongoing new builds and I&C modernisation projects in Nordic countries.

5.1. Industry expert workshop

PLANS have organised an industry expert workshop on *Safety demonstration and planning in Nordic NPP digital I&C projects*. The workshop was hosted by SSM at their premises in Stockholm on 12/05/2015. The objective of the workshop was to bring together Nordic experts in safety demonstration from the NPP licensee and supplier organisations to actively seek their expertise. The presentations and discussions during the workshop focused on the practises, challenges and possible solutions related to safety demonstration. The participants discussed how safety demonstration planning at the early stages of the project can address several of the challenges related to safety demonstration.

The workshop had 20 participants representing the following organisations: ELE Engineering AB, Fortum, IFE, OKG, Ringhals, Solvina, SSM, STUK, TVO, VTT and ÅF. A representative from NKS has also participated. Most of the participants had expertise in instrumentation and control (I&C). There were also participants with expertise in other areas such as human factors.

There were three presentations from the NPP utility organisations - Fortum, OKG and Ringhals - that gave an overview of the practises and experiences with safety demonstration in their respective organisations. Then, participants contributed to brainstorming sessions by discussing the important challenges facing the industry in regards to safety demonstration. The workshop concluded with participants pointing the future directions the PLANS project should take in order to better contribute to the safety demonstration needs of the industry. Findings from the workshop are presented in Section 5.3 and Section 5.4.

5.2. Joint workshop

PLANS project partners gave presentations on the ongoing work on improving guidance on safety demonstration planning, especially on safety demonstration plan guide. These presentations focused around the following topics, which were the suggested future directions/activities by the participants of an earlier PLANS workshop conducted in May 2015. In addition to presentations from PLANS project partners, the workshop had six presentations on practical experiences, research and standardisation activities in safety demonstration. The workshop also had a brainstorming session on safety demonstration and future activities for PLANS.

5.3. Challenges of safety demonstration

A brainstorming session was conducted during PLANS workshop in May 2015. The participants were asked to discuss the experiences and possible challenges related to safety demonstration facing the NPP industry. The participants were organised into three groups and each group was asked to elicit challenges of safety demonstration. Thereafter, each group was asked to prioritise the most important challenge and propose possible solutions to address the challenge. The following are the three most important topics selected by the groups.

1. *Knowledge gap across organisations as well as within departments of an organisation.*

Currently, there is a knowledge gap between the experts involved in system development and demonstration. The knowledge gap within safety demonstration is for example in terms of: what is a safety demonstration, what constitutes (claims, evidences, documentation) safety demonstration, how to perform safety demonstration, what are the advantages and cost-benefits of creating and maintaining safety demonstration.

The experts involved in a project are from different disciplines (I&C and other engineering disciplines, management, safety & security, assessor etc.) and from different organisations (utility, vendors and regulator). There should be better communication and common understanding between the experts both within the organisation and across organisations. Regulator should be involved at the early stages of the project and should be informed continuously so that there is a common understanding on safety demonstration and the required documentation as a part of it. Moreover, the management should be committed to safety demonstration.

One way to improve the knowledge gap and to increase awareness is having a safety demonstration plan. The plan should cover the complete lifecycle describing what is required for safety demonstration during different phases of lifecycle. In addition, right people from different disciplines should be involved during planning. The contents of the plan should be clearly described and the plan should focus on important (safety) areas of the project. Note that the focus (safety) areas will vary from project to project and will vary over time, and the plan should consider this.

2. *Multidisciplinary approach incorporating boundaries and interfaces between various disciplines.*

The interfaces and information flow between the disciplines (I&C, process, mechanical, electrical, etc.) is not good enough. For example, the interface between plant design and I&C design is not clearly described since the scopes and boundaries of the actual systems are often unclearly defined and therefore the completeness of I&C requirements towards plant design

cannot not be (safety) demonstrated – nor can quality. Safety demonstration tends to focus on one (snapshot) of safety assessment report and not the entire lifecycle.

Integrating safety demonstration with design/development process is way to bridge the gaps (knowledge, etc.). This will enable, for example, justification of design decisions made, the status of the safety demonstration during the project. The safety demonstration plan should be multidisciplinary and should show the interfaces and information flow between the disciplines. There should be a good configuration and change management, with tool support, for the whole plant and all the changes have to be reviewed by all the relevant departments.

3. Better understanding of safety demonstration and its cost-benefits.

The concepts of safety demonstration should be made clear and understandable. There is confusion among the experts on the difference or relation between safety demonstration and other processes or activities such as design, licensing and qualification. The management should understand the safety and cost benefits of safety demonstration being integrated in the normal project and design process.

The terminology and syntax of safety demonstration should be clarified. The documentation structure of safety demonstration should be exemplified by using templates, etc.

5.4. Future directions for PLANS

During the PLANS workshop in May 2015 the participants were asked to suggest the future directions for the PLANS project. The future directions are the tasks or activities that could be performed by the project in order to better contribute to the NPP industry in addressing safety demonstration challenges. The future directions reflect the participants' opinions during brainstorming session. The following are the topics proposed by the participants.

1. Define how safety demonstration fits with systems engineering.

The PLANS project could look into describing how safety demonstration fits with the existing systems engineering processes. This will improve the awareness on safety demonstration among experts who are involved at the different stages of systems engineering. For example, the project could investigate on how safety demonstration fits with the systems engineering processes described in the ISO/IEC 15288, and this could be documented in the safety demonstration plan guide.

In addition, the relation between safety demonstration plan and other plans (e.g. qualification plan, project plan) should be made clear.

2. Define terminology for the concepts of safety demonstration.

The project could define terminology and syntax for concepts underlying safety demonstration.

3. *Examples describing how to apply safety demonstration plan guide.*

The project could provide examples on applying safety demonstration plan guide. This will exemplify the contents of the safety demonstration, for e.g., what is a claim, what is a good argument, how to specify an argument.

4. Multidisciplinary approach covering the overall plant.

Since I&C is the "nervous system" of the whole plant, its safety (and quality) demonstration inherently integrates (and reveal any deficiencies in integration) the different systems and components constituting the overall plant. Such an integration is by nature multi-disciplinary

and therefore calls for a multidisciplinary approach integrated with the overall integration and design efforts. This multidisciplinary approach also needs to integrate to the normal plant project processes for effectiveness.

The project could provide further clarifications and examples in the guide on this, that also strongly interfaces to e.g. item 1 above, but also to items 1-3 discussed under the brainstorming session described in Section 2 above.

5. *Increase the awareness on safety demonstration within the NPP community.*

The project should help the community to bridge the knowledge gap that exists in the personnel from several departments, including management, involved in I&C (and overall plant) projects. One way to do this is to engage the experts from the industry through the Nordic network for nuclear experts on digital I&C safety demonstration. The network will offer a forum of competence and knowledge exchange in the area of safety demonstration. The Nordic network should be extended to include more people with different expertise (human factors, management, etc.), thereby increasing the awareness across disciplines. The project as well as the Nordic network should communicate the results or opinions to other relevant networks or communities (e.g. IEC Nordic TC45, Task Force on safety critical software).

Improvements and clarifications of the "executive summary" of the safety demonstration plan guide ("safety demonstration for dummies") could also assist in this matter.

6. Safety demonstration plan guide – Improving guidance

As stated earlier, refining the safety demonstration plan guide (SDPG) is an ongoing work that will be carried out over three years period. In 2015, SDPG's refinement involves detailing the guidance on some of the safety subject areas (SSAs) of SDPG. In this report, we have listed a set of claims for four SSAs of SDPG, namely *Requirements*, *Product Design*, *Product Design Qualification Status*, *QA and Plans Compliance Including Organization and Competence Assessment*. For each of the claims, relevant evidence and context information that needs to be provided is given. The claims and relevant argument elements provided here are generic and are based on common practises. The claims are high-level and could be further decomposed into sub-claims. The detail and rigor of safety demonstration depends on, among others, the safety significance of the system.

Requirements SSA

- Claim: Applicable requirements (design, standards, work process, competence) are identified.
    - Context: Project scope specification, Requirements specification
    - Evidence: Requirements specification review, QA review, Traceability matrix
- Claim: I&C requirements are traceable to plant level requirements
    - Context: project scope specification, requirements specification
    - Evidence: Traceability matrix
- Claim: I&C requirements are traceable to functional, system design, detailed design requirements.
    - Context: Requirements specification, Design description

        - Evidence: Traceability matrix
    - Claim: All hazardous conditions are identified and are acceptable.
        - Context: Requirements specification, System level hazards
        - Evidence: Hazard log, Hazard analysis report, Hazard analysis report review, Traceability matrix

Product Design SSA

- Claim: Applicable version of product design is identified.
    - Context: Design description, requirement specification
    - Evidence: Design review, CM report
- Claim: Product design is complete and consistent with project scope and requirements.
    - Context: Design description, requirement specification, standards
    - Evidence: Design review, traceability matrix

Product Design Qualification Status SSA

- Claim: Product design implements the project scope and requirements.
    - Context: Design description, Requirements specification, QA and Plans
    - Evidence: V&V records (review, inspection, analysis, tests)

QA and Plans Compliance Including Organization and Competence Assessment SSA

- Claim: Quality assurance program is followed.
    - Context: QA program and associated processes and plans
    - Evidence: Audit

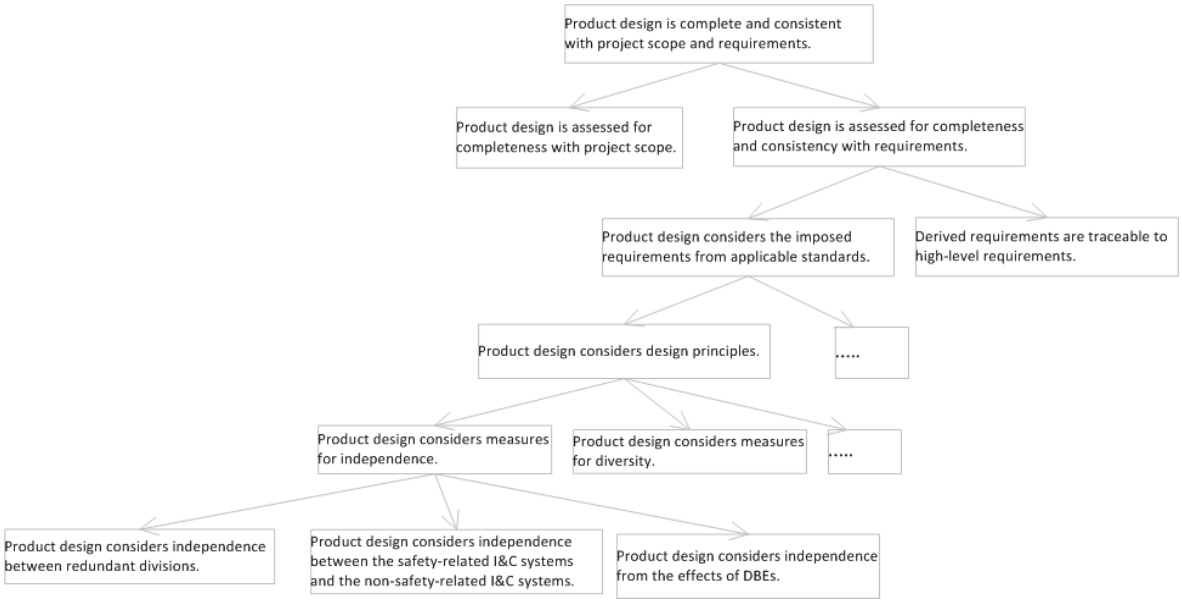


Figure 4. Claim decomposition

Depending upon the detail of the safety demonstration needed in a project, some of the above claims could be decomposed into sub-claims. Figure 4 shows a tree structure[1] depicting a strategy of decomposing the *Product Design SSA* claim on *Product design is complete and consistent with project scope and requirements*. The figure show how the high-level claim on completeness and consistency of product design is decomposed into sub-claims on, among others, product design considering independence measures. These sub-claims can be further decomposed; however, this is not within the scope of this report.

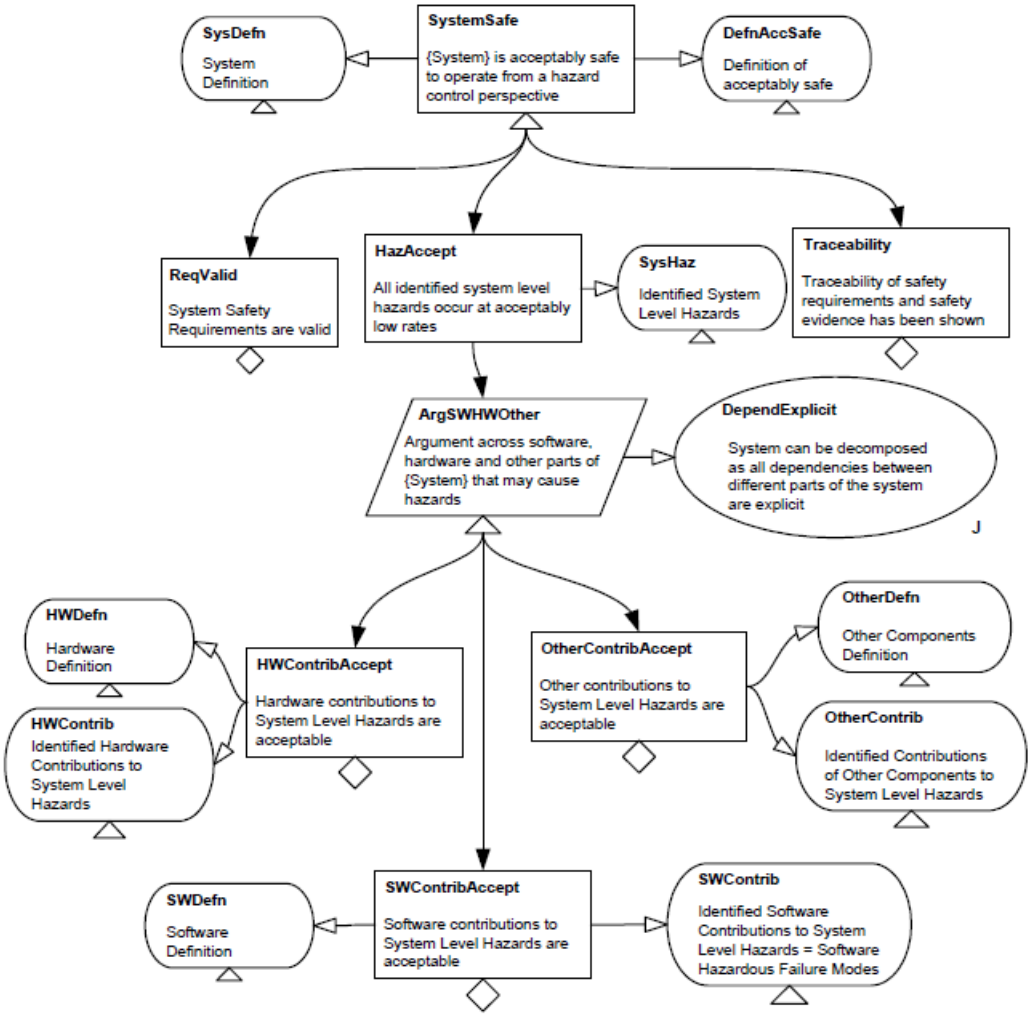


Figure 5. Safety case pattern structure on component contributions to system hazards (excerpt from (Weaver, 2003))

Available safety case patterns can also be used to elaborate some of the SSA claims. A safety case pattern is "a means of documenting and reusing successful safety argument structures" (Kelly, 1998). Safety case patterns are used to capture common approaches used to construct successful safety demonstration, and therefore reflect best practice. Figure 5 presents a safety case pattern structure taken from (Weaver, 2003) that presents an approach for arguing safety of a system. The argument focuses on identification of hazards and the assessment of the

[1] The tree in the figure does not present a safety case pattern. The decomposition is not complete, and relevant information such as evidence and context is not provided.

associated risks. This pattern could be used to construct the *Requirement* SSA claim on *All hazardous conditions are identified and are acceptable*.

7. Safety demonstration during systems engineering lifecycle

In PLANS workshops, it was 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. This topic will be investigated in more detail in PLANS during 2016. However, this Section provides an overview on the topic as a starting point for future work.

The International Council on Systems Engineering (INCOSE, http://www.incose.org) characterizes Systems Engineering is 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…) 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, covering 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 organizational processes.

So, 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. 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. 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. Thus, in PLANS project, it can be asked what is the role of safety demonstration and qualification in the overall systems engineering process and which processes specified in IEC 15288 have elements that can be understood to be part of or providing support to qualification process and safety demonstration documentation.

IEC 15288 defines four process groups: Agreement processes, Organizational Project-Enabling Processes, Technical Management Processes and Technical Processes.

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 IEC 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 project.

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) concerns about managing and controlling system elements and configurations over the life cycle of a system.

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 safety demonstration.

When talking about System Life Cycle Processes and safety demonstration in the context of PLANS, some questions arise:

- Are the Verification, Validation and Configuration Management Processes really processes or rather process views? These should be made more explicit.
- How much overlap there is between the Quality Assurance, System Analysis, and Verification Processes? Their relations should be clarified and made more explicit.
- Is there a need for a Qualification Process or a Licensing Process to extend the applicability of the standard IEC15288 to safety critical areas? Should there be a tailored nuclear-specific version or application guideline of IEC15288?

Two appendices describing how SDPG relates to IEC 15288 standard (IEC, 2015) on systems and software engineering are currently being developed. These appendices will be incorporated into the next version of the SDPG. The appendices will document how SDPG's safety demonstration phases and SSAs correspond to some of the processes and activities defined in IEC 15288. This work will clarify how planning safety demonstration and performing qualification and licensing (as per the guidance provided by the SDPG) relates with the existing systems engineering processes (as defined in IEC 15288), and show how safety demonstration case can be built by utilising the information (in particular evidence) produced while applying systems engineering processes.

8. NordicNSEC

PLANS has established a Nordic network of competence on nuclear digital I&C safety demonstration (NordicNSEC), which is a forum for knowledge exchange among experts from multidiscipline. NordicNSEC is at its early stages and is being extended by inviting more Nordic NPP experts from several disciplines, including at management level. PLANS sees this network as a medium to: increase awareness on safety demonstration; discuss experiences

in safety demonstration; communicate relevant work being performed by the Nordic and international NPP community, including results from PLANS.

9. Conclusions and future work

The NKS-R PLANS project was initiated in 2015 with the aim of providing detailed guidance on selected topics of safety demonstration planning for Digital Instrumentation and Control (DI&C) systems in Nuclear Power Plants (NPP). In 2015, by organising an industry expert workshop, PLANS elicited experiences and challenges on safety demonstration from 20 NPP industry experts, in particular experts from the Nordic NPP end user organisations. PLANS also elicited safety demonstration needs of the experts and their recommendations on how these can be solved by future activities of PLANS. PLANS is addressing these challenges by further developing a guide for planning safety demonstration, called Safety Demonstration Plan Guide (SDPG). Ongoing work on SDPG involves detailing an approach for safety demonstration planning covering the entire development lifecycle and identifying development artefacts that could be used as evidence to justify the claims on safety of the system. Moreover, the concepts of safety demonstration and how safety demonstration relates to systems engineering process are being clarified. Up-to-date results of PLANS have been presented at a joint workshop co-organised by PLANS and NKS-R MODIG (Modelling Of DIGital I&C) projects.

PLANS, in 2015, has established Nordic Nuclear Safety Experts Consortium on safety demonstration of DI&C systems (NordicNSEC), which is a forum for knowledge exchange among experts from multiple disciplines. This network is being extended by inviting experts from several end user organisations. PLANS sees this network as a medium to: increase awareness on safety demonstration; discuss experiences in safety demonstration; communicate relevant work being performed by the Nordic and international NPP community, including results from PLANS.

As a possible future work, PLANS could continue to address the needs of the end user organisations on safety demonstration by improving guidance and awareness on safety demonstration planning. This will be achieved by, among others, refining SDPG, actively maintaining NordicNSEC network, and progressively seeking feedback from industry. The extensions to SDPG will reflect the following desired future directions/activities proposed by the participants of the PLANS workshops. In this way, PLANS ensures that the results of the project are applicable to the participants, who are representatives of end user organisations.

10. References

Axenborg, M. L & Ryd, P. 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 Systems. Elforsk rapport 13:86. Elforsk.

Bel V, BfS, CNSC, CSN, ISTec, ONR, SSM, STUK. 2014. Licensing of safety critical software for nuclear reactors: Common position of international nuclear regulators and authorised technical support organisations.

Energiforsk - Swedish energy research centre. 2015. http://www.energiforsk.se/. Accessed on 09 December 2015.

ELFORSK – Shared financing for joint R&D. 2015. http://www.elforsk.se/. Accessed on 09 December 2015.

ENSRIC - Elforsk nuclear safety related I&C program. 2015. http://www.elforsk.se/Programomraden/Karnkraft/ENSRIC---IC/. Accessed on 09 December 2015.

Hauge, A. 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. Report HWR-1113. OECD Halden Reactor Project, Norway.

IEC. 2015. IEC 15288 Systems and software engineering — System life cycle processes, First edition, 2015-05-15.

Karpati, P, Hauge, A. A, Katta, V & Raspotnig, C. 2014. Safety Demonstration and Justification of DI&C Systems in Nuclear Power Plants – Elicitation with Regulators. Report HWR-1112. OECD Halden Reactor Project, Norway.

Karpati, P. To be published. Extracting the assurance argument from an interim safety demonstration – A case study from the nuclear field (Part 1: Argument comprehension). Report HWR-1149 (draft ver). OECD Halden Reactor Project, Norway.

Katta, V, Valkonen, J & Ryd, P. 2015. Workshop summary report – NKS-R PLANS Industrial expert workshop on safety demonstration and planning in Nordic NPP digital I&C projects. Available on request.

Kelly, T.P. 1998. Arguing Safety - A Systematic Approach to Managing Safety Cases. Doctor of Philosophy Thesis. University of York.

Merriam-Webster. 2016. “Argument” available at http://www.merriam-webster.com/dictionary/. http://www.merriam-webster.com/dictionary/argument. Accessed on 26 January 2016.

NordicNSEC - Nordic Nuclear Safety Experts Consortium on safety demonstration of DI&C systems. 2015. http://nordicnsec.ife.no/. Accessed on 09 December 2015.

SAFIR2018 - The Finnish research programme on nuclear power plant safety 2015 – 2018. 2015. http://safir2018.vtt.fi/. Accessed on 09 December 2015.

SSM. 2010. SSMFS 2008:1 The Swedish Radiation Safety Authority’s Regulations concerning Safety in Nuclear Facilities and general advice on the application of the regulations.

The Halden Reactor Project. 2015. http://www.ife.no/en/ife/halden/hrp/the-halden-reactor-project. Accessed on 09 December 2015.

U.S. Nuclear Regulatory Commission. 2015. Research Information Letter 1101: Technical Basis to Review Hazard Analysis of Digital Safety Systems.

Weaver, R. A. 2003. The Safety of Software – Constructing and Assuring Arguments. Doctor of Philosophy thesis, University of York.

Bibliographic Data Sheet **NKS-357**

Title	Safety Demonstration Planning for Digital I&C Projects – Challenges, Future Directions and Improving Guidance
Author(s)	Vikash Katta[1] Pontus Ryd[2] Janne Valkonen[3]
Affiliation(s)	[1]Institute for Energy Technology, Norway [2]Solvina AB, Sweden [3]VTT Technical Research Centre of Finland Ltd, Finland
ISBN	987-87-7893-441-3
Date	February 2016
Project	NKS-R / PLANS
No. of pages	22
No. of tables	0
No. of illustrations	5
No. of references	18

Abstract

max. 2000 characters

Licensee should submit a safety demonstration case and supporting documentation to the regulator describing how safety has been achieved. However, more often, submittals to regulators consist of vast amount of documentation without providing any explicit argumentation on how this documentation supports safety demonstration. There are large differences in current practice in different countries for safety demonstration, as well as some common challenges. The project aims to address some of these challenges by providing detailed guidance on how to plan and perform safety demonstration for Digital Instrumentation and Control (DI&C) systems in Nuclear Power Plants (NPP).

The project elicited the experiences and challenges related to safety demonstration of DI&C facing the NPP industry by organizing industry expert workshops. The experts who participated in the workshop recommended future activities for the project. These future activities reflect the needs of the industry in order to address some of the challenges related to safety demonstration. One need of the industry is the clarification of how to perform safety demonstration and how safety demonstration is related to the existing system engineering process. Another need is a multidisciplinary approach for safety demonstration that should involve personnel from different disciplines (e.g. I&C, safety, management, process) across organisation at the early stages of the project and plan for how to achieve and demonstrate safety.

The project has refined a guide for planning safety demonstration, called Safety Demonstration Plan Guide (SDPG) to address some of the challenges and needs of the industry. As per SDPG, the contents of the safety demonstration can be organised effectively using a set of Safety Subject Areas (SSA). SSA is an aspect of safety and the complete set of SSAs constitute the safety demonstration case. SDPG's refinement involved detailing on some of the SSAs. As a starting point for future work, the project has provided an overview on the topic of system engineering and the role of safety demonstration in the overall systems engineering process.

Key words

Safety demonstration, safety demonstration planning, safety case

SAFETY DEMONSTRATION PLANNING FOR DIGITAL I&C PROJECTS

When safety related instrumentation and control systems in a nuclear power plant are renewed, the licensee has to submit a safety demonstration to document that the change does not affect the safety of the plant in any way. This often results in vast amounts of documentation. There are large differences in current practice in different countries for safety demonstration, as well as some common challenges.

This project has addressed some of these challenges by providing detailed guidance on how to plan and perform safety demonstration for digital instrumentation and control systems in nuclear power plants. A hands on safety demonstration plan guide was developed in a previous project, and this guide has been further refined in this project.

Another step forward in Swedish energy research

Energiforsk – Swedish Energy Research Centre is a research and knowledge based organization that brings together large parts of Swedish research and development on energy. The goal is to increase the efficiency and implementation of scientific results to meet future challenges in the energy sector. We work in a number of research areas such as hydropower, energy gases and liquid automotive fuels, fuel based combined heat and power generation, and energy management in the forest industry. Our mission also includes the generation of knowledge about resource-efficient sourcing of energy in an overall perspective, via its transformation and transmission to its end-use. Read more: www.energiforsk.se

Energiforsk