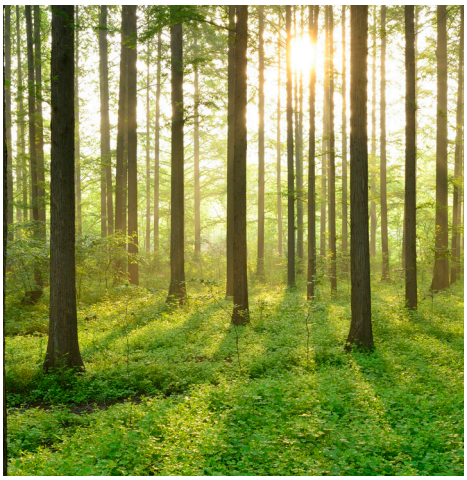
SAFETY DEMONSTRATION PLAN GUIDE

REPORT 2018:512



NUCLEAR

ENERGIFORSK NUCLEAR SAFETY RELATED I&C – ENSRIC

Energiforsk

Safety Demonstration Plan Guide

MARIE-LOUISE AXENBORG & PONTUS RYD

ISBN 978-91-7673-512-1 | © ENERGIFORSK July 2018 | Photo: TVO

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

Foreword

Safety demonstration/licensing of nuclear instrumentation and control systems is time consuming and costly. Efforts could be saved both for nuclear power plants and regulators if a common methodology could be used for planning and execution of safety demonstration.

This report suggests a structured approach to carry out planning and execution of safety demonstration/licensing. It is an updated version of the previously published Elforsk report 13:86 with the same name. Authors are Pontus Ryd and Marie-Louise Axenborg, consultants at Solvina AB.

The safety demonstration plan guide was developed within Energiforsk's ENSRIC - Energiforsk Nuclear Safety related I&C research program. The ENSRIC program is financed by Fortum, Karlstads Energi, Skellefteå Kraft, Teollisuuden Voima, Uniper, Vattenfall and the Swedish Radiation Authority.

Sammanfattning

Denna rapport är en Guide för hur man inom kärnkraftsindustrin planerar och utför demonstration av säkerhet (s.k. Säkerhetsdemonstration) i moderniserings- och nybyggnadsprojekt som innehåller digitala styr- och säkerhetssystem. Guiden har utvecklats i nära samarbete med en expertgrupp med stor gemensam erfarenhet och expertis inom området Säkerhetsdemonstration i flera relevanta projekt, Detta är en uppdaterad version av Guiden med hänsyn tagen till nya erfarenheter och referenser inom Säkerhetsdemonstration. Den speglar även den nya trenden mot att minimera omfattningen i ändringsprojekt vid uppdateringar av kärnkraftverkens styr- och kontrollutrustning.

Guiden etablerar tre viktiga syften med att göra Säkerhetsdemonstration. Det första syftet är att övertyga sig själv i projektet och som tillståndshavare att anläggningen är säker under och efter implementeringen av projektet och att dokumentera underlaget för denna slutsats. Det andra syftet är att demonstrera säkerhet, med tillhörande argumentation och bevis för granskare och ansvarig myndighet. Det sista men absolut inte minsta syftet är att minimera licensierings- och ekonomiska risker kopplade till projektet och den övergripande investeringen.

Licensierings- och andra övergripande projektrisker bedöms kunna minskas radikalt genom att tillämpa den här Guidens metodik för säkerhetsdemonstration. Metodikens hörnpelare är stegvis kommunikation med successiv acceptans och godkännande av resultat enligt överenskomna acceptanskriterier mellan projektets intressenter (leverantörer, projektet, granskare, tillståndshavare och myndighet) samt att detta påbörjas tidigt i projektet. För tillståndshavaren och investeraren betyder detta, utöver säkerställd och demonstrerad säkerhet med ökat förtroende från myndighet och allmänhet, även minskade risker för misslyckade investeringar genom mer förutsägbart projektgenomförande både med avseende på kvalitet, tid och pengar.

Guiden föreslår en struktur för hur Säkerhetsdemonstration planeras samt en livscykelmodell med faser och rapporteringssteg som relaterar till ett normalt utvecklingsprojekts faser. Planeringsfasen för en Säkerhetsdemonstration har avgörande betydelse. Genom att genomföra den fasen noggrant och i god tid kan projektets intressenter i förväg komma överens om hur, när och baserat på vad som acceptans och tillstånd uppnås. Erfarenheter från flera moderniserings- och nybyggnadsprojekt, men även från mindre komplexa projekt som innefattar digitala styr- och säkerhetssystem och smarta enheter, har visat att brist på tidig kommunikation och överenskommelser är en av de största anledningarna till oväntade tids- och kostnadsökningar.

Strukturen som presenteras i Guiden syftar till att vara användbar för projekt av olika storlek och omfattning genom att anpassas till det specifika projektets

omfattning. Guiden innehåller ett exempel på ett översiktsdiagram för Säkerhetsdemonstrationens livscykel samt malldokument för vad som ska ingå i en Säkerhetsdemonstrationsplan respektive -rapport. Guiden ger en generell modell för Säkerhetsdemonstration och den tillhandahåller användbara detaljer och referenser för specifika problemställningar inom området digitala styr- och säkerhetssystem.

Guiden har tagits fram på initiativ av Elforsk (som år 2015 blev en del av Energiforsk) och projektets styrgrupp som bestod av experter representerande Vattenfall, Fortum, Forsmarks Kraftgrupp (FKA), Oskarshamnsverkets Kraftgrupp (OKG), den svenska strålsäkerhetsmyndigheten (SSM), den svenska branschorganisationen Svensk Energi och en representant från Elforsk. Detta är en uppdaterad version av Guiden som utvecklats i samarbete med Energiforsk som en del av ENSRIC-programmet under 2018.

Summary

This document 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. The document has been developed in close collaboration with an expert group having comprehensive experience from digital I&C implementation and Safety Demonstration in relevant projects. This version of the Guide has been updated based on recent experiences and new references in the area of Safety Demonstration. It also reflects the trend towards more limited scope modification projects rather than large system exchanges when performing life time extension in NPP I&C.

The Guide establishes three important purposes with Safety Demonstration. The first purpose is to convince oneself (in the project and as Licensee) that the plant is safe during and after the project implementation and document the basis for that conclusion. The second purpose is to demonstrate the safety, with argumentation and evidence, to reviewers and the regulating authority. The last and not least of the three, is to minimize both licensing and commercial risks linked to the project and the overall investment.

Licensing and other overall project risks are deemed to decrease radically by applying this Guide's methodology for Safety Demonstration. The cornerstones of the methodology are sequential communication and gradual acceptance and approval of results according to agreed acceptance criteria between the stakeholders (suppliers, NPP project, reviewers, Licensee and the regulator), and all this to be started early in the project. For the Licensee or investor this means, in addition to the assured and demonstrated safety with increased confidence from the regulator and the public, also significantly reduced risk for failed investments thanks to more predictable project performance with regards to both quality of results, time and money.

The Guide suggests a structure for how to plan a Safety Demonstration and a life cycle model with phases or reporting steps related to normal project development phases. It is important to keep in mind that the planning phase of Safety Demonstration is most important. By performing this phase early and carefully, the stakeholders can agree and commit up front to how, when and based on what, acceptance will be achieved and agreed. Experience from several NPP modernization and new build projects, but also smaller less complex projects involving digital I&C and Smart Devices, have shown that lack of such agreements is one of the largest causes of delays and unexpected cost increase.

The structure presented in the Guide aims at being useful for all sizes of projects by adapting the scope and level of detail depending on the specific project scope. The Guide contains a typical example of a Safety Demonstration life cycle overview

diagram and template documents for what to include in a Safety Demonstration Plan and in Safety Demonstration Reports. The focus of the Guide is to give a general model for Safety Demonstration and it also provides useful detail references for specific problem areas when it comes to digital I&C systems in safety critical applications.

The development of the Guide was initiated by Elforsk, (which in 2015 became part of Energiforsk) and the project steering and expert group constituted by representatives from Vattenfall, Fortum, Forsmarks Kraftgrupp (FKA), Oskarshamnsverkets Kraftgrupp (OKG), the Swedish radiation safety authority (SSM), one Swedish trade organization (Energiföretagen Sverige) and one representative from Elforsk. This updated version has been developed for Energiforsk as part of the ENSRIC program in 2018.

List of content

Terms and abbreviations **11**

1 Introduction **15**

1.1 Background and basic idea of Safety Demonstration 15

1.2 Purpose of Safety Demonstration 16

1.3 Scope of Safety Demonstration 17

1.4 Purpose and scope of this Guide 17

1.5 Target group and reading instructions 18

1.6 Application of the guide in different scenarios 18

2 Life cycle and contents of Safety Demonstration **20**

2.1 The Safety Demonstration life cycle 20

2.2 Contents of Safety Demonstration 22

2.2.1 Safety Demonstration Case 23

2.2.2 Safety Subject Areas 24

3 Safety Demonstration Planning phase **27**

3.1 Objectives 27

3.2 Scope 28

3.3 Requirements 28

3.4 Safety Demonstration Case definition 28

3.4.1 Safety Subject Areas definition 28

3.4.2 Safety Demonstration strategies development 29

3.5 Relation to formal Safety Report and Safety Review 29

3.6 Safety Demonstration life cycle overview diagram 29

3.7 Phase results and stakeholder agreements 30

4 Safety Demonstration Qualification phases **32**

4.1 Qualification of the Overall Project and Product Conceptual Design 32

4.1.1 Scope 32

4.1.2 Requirements 34

4.1.3 Phase results and stakeholder agreements 34

4.2 Qualification of the Product Basic Design 35

4.2.1 Scope 35

4.2.2 Requirements 36

4.2.3 Phase results and stakeholder agreements 36

4.3 Qualification of the Product Detailed Design including FAT 38

4.3.1 Scope 38

4.3.2 Requirements 40

4.3.3 Phase results and stakeholder agreements 40

4.4 Qualification of Product as Installed and Commissioned including SAT 41

4.4.1 Scope 41

4.4.2 Requirements 43

4.4.3 Phase results and stakeholder agreements 43
4.5 Qualification of Product at One Year of Operation including Outage 45
4.5.1 Scope 45
4.5.2 Requirements 46
4.5.3 Phase results and stakeholder agreements 47
5 Safety Subject Areas – Contents of Safety Demonstration 48
5.1 SSA 1 - Project Scope 48
5.1.1 Purpose and scope 48
5.1.2 Strategy 49
5.2 SSA 2 - Safety Classification and Categorization 49
5.2.1 Purpose and scope 49
5.2.2 Strategy 49
5.3 SSA 3 - Requirements 50
5.3.1 Purpose and Scope 50
5.3.2 Strategy 50
5.4 SSA 4 - Product Design 51
5.4.1 Purpose and scope 51
5.4.2 Strategy 51
5.4.3 Separate handling of the I&C Architecture 52
5.5 SSA 5 - Product Design Qualification Status 53
5.5.1 Purpose and scope 53
5.5.2 Strategy 53
5.6 SSA 6 - Plant Documentation 54
5.6.1 Purpose and scope 54
5.6.2 Strategy 54
5.7 SSA 7 - QA and Plans including Organization and Competence Assurance 54
5.7.1 Purpose and scope 54
5.7.2 Strategy 55
5.8 SSA 8 - QA and Plans Compliance including Organization and Competence Assessment 56
5.8.1 Purpose and scope 56
5.8.2 Strategy 56
5.9 SSA 9 - NPP Operation, Maintenance and Modification 57
5.9.1 Purpose and scope 57
5.9.2 Strategy 57
5.10 Optional Areas 58
5.10.1 Base Product qualification 58
5.10.2 Integration in plant 58
5.10.3 Human Factor Engineering (HFE) and Human System Interface (HSI) 58
5.10.4 Regulations, codes, guidelines and standards 59

6	**Specific challenge areas for digital I&C**		**60**
	6.1	Defense-in-depth, diversity and common cause failure	60
	6.2	Deterministic behavior	61
	6.3	Independence – functional and physical separation	61
	6.4	Performance – timing and accuracy	61
	6.5	Failure tolerance and functional reliability	62
	6.6	Failure detection by self-diagnostic functions and periodic tests	62
	6.7	Fail-safe design, handling of new failure modes and initialization	62
	6.8	IT security	63
	6.9	Verification & Validation strategy for Programmable Electronics Systems	64
	6.10	Suitability and qualification of platform and equipment	64
	6.11	Formal methods of software development	64
	6.12	System classes, function categories and graded requirements for software	64
	6.13	Human factors engineering (HFE) and Human System Interface (his)	65
	6.14	Smart Devices and programmable Electronics	65
	6.15	Prioritization	66
	6.16	Digital Communications	66
	6.17	Use of wireless technology	66
	6.18	Management of the functional requirements specification	66
	6.19	Development of and adherence to configuration management	67
	6.20	Environmental qualification of safety system platforms	67
	6.21	Reliability (taking credit for digital systems in probabilistic risk assessment)	67
7	**References**		**68**
Appendix A:	**Safety Demonstration PLAN Template**		**70**
Appendix B:	**Safety demonstration REPORT Template**		**72**
Appendix C:	**Guiding questions for Safety Demonstration in respective Safety Subject Areas**		**73**
Appendix D:	**Figure 2.1 Full Page Format**		**82**
Appendix E:	**Figure 3.2 Full Page Format**		**83**

Terms and abbreviations

Terms

Argument	A logical sequence or series of statements from a premise to a conclusion.
Assumption	A premise that is taken for granted, i.e. not validated. Often, it is taken for granted implicitly. (From US Nuclear Regulatory Commission, 2015)
Base Product	In this Guide used to cover I&C platforms (including firmware, operating system, additional options in SW etc.) and I&C equipment as provided from the supplier before the adaptation to the NPP specific application.
Claim	A true-false statement about the value of a defined property of a system. (From US Nuclear Regulatory Commission, 2015)
Classification and Categorization (Safety-)	Safety Classification is a general requirement of e.g. IAEA Safety Fundamentals, and the principles for this are applied differently in different NPPs. With regards to I&C the IEC 61226 [12] talks of Safety Categorization of functions with corresponding classification of associated structures, systems and components. There are also comparable US standards applicable (even though the ANSI 51.1 and 52.1 points to IEC standards), e.g. IEEE-279, -308 and -603 [17]. The resulting classification then determines relevant design criteria and provides basis for graded approach on detail of QA and documentation etc. The latter is applied also in the Safety Demonstration.
Complete, Correct and Consistent ("3C")	In this guide "3C" is a central concept. The completeness aspect requires the end product to be completely defined and the definition to be validated against higher-level definition or governing documents before performing release and review of the product. The review evaluates both the completeness, correctness and consistency of what is written and designed. "3C" is a general work process with two steps: 1. Define the reference of "complete" including boundaries, evaluate the definition and validate.

	2. Design and evaluate for completeness against the definition and evaluate, validate and verify correctness and consistency. Finally reconfirm the completeness definition from 1. Example: Top level reference of complete defined as the valid Safety Analysis Report (SAR) and the Plant as operated (as defined in the TWICE project)
Evidence	Data supporting the existence of truth of something. (From US Nuclear Regulatory Commission, 2015)
Instructing Documentation	Those documents in the Plant Documentation (see below) that describe or govern operation and maintenance of the plant but also Management and QA documents.
Licensee	The owner of the Nuclear Power Plant (NPP) is also the owner and responsible for the license for nuclear operation of the plant. From a NPP project perspective the project sponsor is usually the licensee.
Plant Documentation	All technical documentation describing the plant (including SAR) and all instructing documentation describing operation and maintenance of the plant. It is the documentation that the Safety Demonstration shall ensure to be complete and correct when the project is finalized. Generally, Plant Documentation are all "living documents" which are to be updated continuously during the Safety Demonstration.
Product	In this guide the term is used to denote the complete digital I&C system, Smart Device or component as integrated in the NPP, i.e. the system/components including the specific NPP application configuration. Base Product is used to denote the digital I&C system, Smart Device or component as it is "available on the market" as a platform or general component.
Qualification	The work to formally demonstrate safe, complete, correct and consistent plant function by demonstrating that for the defined project scope (itself concluded "3C"): a) The requirements have been "3C" defined for the intended scope and use; they have been traceably decomposed and addressed to functions, and that the functions, as designed and traceably implemented in identified systems and equipment, "3C" meet these requirements. All shall be supported by traceable

	design process integrated Verification and Validation (V&V) activities; b) The design and implementation have been performed under sufficient configuration management, according to identified processes with their integrated V&V activities, by persons with relevant competence.
Regulator	The regulatory body and/or authorized technical support organization acting on behalf of its authority. (From Del V et al., 2014)
Safety Demonstration	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 [2].
Safety Demonstration Plan	A plan identifying how the safety demonstration will be achieved by identifying the types of evidence that will be used, and how and when this evidence shall be produced [2].
Safety Report	In this Guide used to correspond to Safety Analysis Report (Säkerhetsredovisning) as defined in SSMFS 2008:1 [3].
Safety Subject Area (SSA)	Aspect of safety, as defined in the project. The complete set of SSA constitute the Safety Demonstration Case. See further description in section 2.2 and section 5 of this Guide.
Smart Device	(Smart sensors or actuators) intelligent measuring, communication and actuation devices employing programmed electronic components to enhance the performance provided in comparison to conventional devices [2].

Abbreviations

3C	Complete, Correct and Consistent, see Terms above
CM	Configuration Management
CCF	Common Cause Failure
COT	Commercial off the shelf software
FAT	Factory Acceptance Test
HFE	Human Factors Engineering
HSI	Human System Interface

HVAC	Heating, Ventilation, and Air Conditioning
I&C	Instrumentation and Control
KSAR	Completed SAR after commissioning
MCR	Main Control Room
NPP	Nuclear Power Plant
PES	Programmable Electronics System
PSA	Probabilistic Safety Analysis
PSAR	Preliminary Safety Analysis Report
QA	Quality assurance
SAR	Safety Analysis Report (when nothing else is noted; as presently valid for the NPP)
SAT	Site Acceptance Test
SDC	Safety Demonstration Case
SDP	Safety Demonstration Plan
SDR	Safety Demonstration Report
SSA	Safety Subject Area, see Terms above
SSC	Structures, Systems and Components
SSM	Swedish Radiation Safety Authority
STUK	Finnish Radiation and Nuclear Safety Authority
TS	Technical Specifications (STF)
TWICE	Ringhals TWo Instrumentation and Control Exchange project
UPSAR	Updated Preliminary Safety Analysis Report (or SAR as planned for commissioning and operation after installation. KSAR replaces as SAR with possible findings and updates after commissioning)
V&V	Verification and Validation

1 Introduction

1.1 BACKGROUND AND BASIC IDEA OF SAFETY DEMONSTRATION

The need for Safety Demonstration has evolved with the need for modernizations of old Nuclear Power Plants (NPP) and the parallell introduction of digital technology (programmable electronics systems (PES) or computer based systems), but has also shown to be essential for new build and any other complex projects. The increasing integration of programmable electronics into conventional equipment furthermore leads to a need to also evaluate safety verification and demonstration need for "simple" process equipment (see section 6.14). In SSM 2016:25 [2] the regulators of six European countries have summarized the current practices, common positions and recommendations for successful licensing of modernizations including software-based systems. The reporting of safety as prescribed in SSMFS 2008:1 [3] needs complementing information and step-vice approval to be successful. Figure 1-1 illustrates how Safety Demonstration as recommended in common positions in SSM 2016:25 [2] and in this Guide provide the coordination and communication of information along the project life cycle. Safety Demonstration provides summarized project information with explaining motivations in support of safety and milestone all through the project life cycle. Safety Demonstration also supports the project process with overall structure and coordination of information and thereby reduces licensing risk as well as other risks.

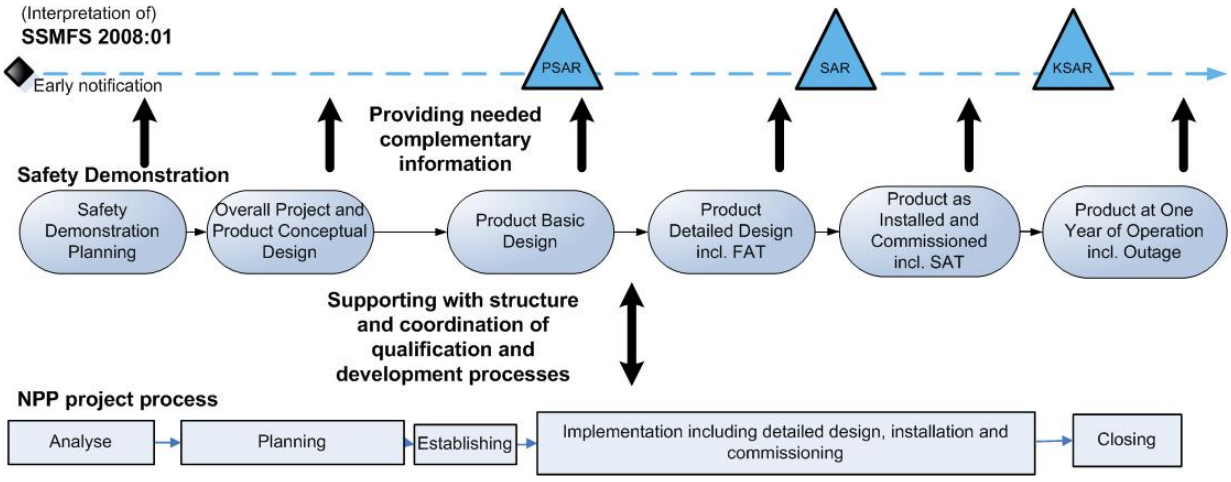


Figure 1-1 ***Safety Demonstration: communication of information throughout the life cycle.***
Safety Demonstration supports the development of safety analysis reports (SAR) and the licensing process between the Licensee and the regulator. The reporting of safety as illustrated in the top of the figure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

A common wish for cooperation and coordination regarding the format and contents of Safety Demonstration for I&C modernization projects as expressed between the regulator and the utilities e.g. in [4] as well as between Swedish utilities e.g. in [5] was the starting point for developing this Guide

The development of this Guide was initiated by Elforsk (a swedish research organisation owned by Svensk Energi and Svenska Kraftnät, which in 2015 became part of Energiforsk). The Guide suggests a simple procedure for how to develop the plan for the Safety Demonstration of a project including digital and programmable control systems performing a safety function. It is agreed upon by expert representatives from Vattenfall, Fortum, Forsmarks Kraftgrupp (FKA), Oskarshamns Kraftgrupp (OKG), the Swedish radiation safety authority (SSM), one Swedish trade organization (Energiföretagen Sverige) and one representative from Elforsk. In the development of the Guide international recommendations and experiences have been a central component. The Guide was updated in 2018 to reflect the recent development in the area of NPP I&C modernizations and in the performance of Safety Demonstration. Recent research performed by ENSRIC, and internationally is concluded in two statements relevant for this Guide:

1. New focus for Nordic as well as international NPPs is on *maintaining* nuclear power through lifetime extensions of existing units and that maintaining systems is really a credible alternative to redesign and upgrade projects [26].
2. Early planning, information and demonstration complementing SAR and TS (i.e Safety Demonstration) and coordinated early communication with authority are needed for successful modification projects, relevant for large as well as for smaller project.

1.2 PURPOSE OF SAFETY DEMONSTRATION

Safety Demonstration, as described in this Guide, has three major purposes:

1. To convince "oneself", i.e. the NPP project and Licensee, that and on what basis the NPP will be safe during and after project implementation.

Specifically for products involving digital and programmable technology which is difficult or impossible to verify and validate completely by test it is utterly important to control and demonstrate not only the product adequacy but also the processes and competences involved during the development. There are also complex interrelations to the overall plant design and safety analyses that puts great challenges to e.g. configuration management and traceability. To systematically and sequentially document how and based on what arguments and evidences the project and Licensee convince "oneself" on the plant safety, i.e. fulfillment of the safety objectives, along the project life cycle, then becomes an important "key to success" factor. It then also facilitates the stepwise safety review and regulator approvals that from experience are concluded essential for success.

2. Demonstrate safety and adequate quality to safety reviewers and regulator, communicating early and all through the project life cycle

Complementing the formal Safety Analysis Report (SAR) with Safety Demonstration, allows additional detail and to document and discuss further the arguments and evidences used to convince the licensee and the project themselves. It also allows addressing a "whole issue" in one place, not forced by a formal SAR structure to write little pieces of the puzzle in different places. This allows for a much-improved review (to confirm or challenge the conclusions on fulfillment of

the safety objectives) as well as sequential agreements or approvals. The latter can start very early with agreements on prerequisites like scope definitions and requirements, evolving through the project life cycle to ultimate complete conclusion on overall NPP safety. Requirements of performing Safety Demonstration is also part of the seven European nuclear regulators common position [2].

3. Minimizing project- and NPP licensing risks

Sequential communication and mutual acceptance agreements starting early between the licensee and the regulator about the scope, requirements and conceptual design minimize licensing risks, which from experience is seen as one of the most significant risks in nuclear modernization and new build projects [1][10]. The number of late changes and delays are reduced by formally communicating the important challenges and issues for resolution acceptance early. For the Licensee this reduces the risk of failed investments in time and money that later has to be reworked or discarded. Another advantage is that early communication between the regulator and the Licensee increases the Licensee's chances to comply with new regulations on time which in turn would strengthen the public confidence for the power plant owner as well as for the regulator.

1.3 SCOPE OF SAFETY DEMONSTRATION

Safety Demonstration is a method to assure and demonstrate safety in a well-structured format along the whole life cycle of a project. It includes the reporting of all activities and all information of relevance to support the claim that the plant is safe during and after a change or new build. *It does not in any way replace or supersede the formal PSAR/SAR and TS, but where the SAR and TS describes the resulting NPP and its Qualification as safe, the Safety Demonstration opens for complementing demonstration throughout the complete design life cycle. It allows further explaining motivations in support of safety and milestone reviews compared to what would be written in the SAR. See further section 3.5 on the relation to the formal SAR.*

The Safety Demonstration is, if applied from beginning, not supposed to introduce much additional work but rather to use, structure and assess the documentation that is in most cases already produced in the project processes.

1.4 PURPOSE AND SCOPE OF THIS GUIDE

The purpose of this Guide is to present a common framework for how to plan and perform a Safety Demonstration that efficiently interfaces the work processes at the NPP and at the same time fulfills the needs to support a successful licensing. Adopted by all Swedish utilities it will facilitate the regulators work and be a basis for efficient exchange of experiences between projects, utilities and regulator. Furthermore, the guide aims at being well harmonized with European recommendations.

The Guide describes an approach for developing the safety plan corresponding to the definition from SSM 2016:25 [2] saying that:

> *"A safety plan[1] shall be agreed upon at the beginning of the project between the licensor and the licensee. This plan shall identify how the safety demonstration will be achieved. More precisely, the plan shall identify the types of evidence that will be used, and how and when this evidence shall be produced".*

The Guide provides references to a standardized project process life cycles to visualize the relation between the Safety demonstration and the normal processes at the NPP. Additionally, it points to standards and guidelines providing input to the requirements on all phases of Safety Demonstration.

1.5 TARGET GROUP AND READING INSTRUCTIONS

This Guide is intended to be used by all persons involved in safety management for the NPP, specifically by persons involved in projects where Safety Demonstration should be performed. This can be persons assigned to coordinate the Safety Demonstration or anyone working with Quality assurance, Safety Review and Safety Reporting. The Guide provides an overview of the elementary parts of Safety Demonstration and is therefore a source of information to be used by project managers. It may also be referred to by the regulator.

In Section 2 of this Guide reporting phases of Safety Demonstration are derived based on different design life cycles. Important parts of a Safety Demonstration Plan (including a Safety Demonstration Case definition with its Safety Subject Areas) are described briefly in the same section, with contents further detailed in section 5.

Sections 3 and 4 of the Guide contain a step-by-step instruction for how to plan, perform and document a Safety Demonstration. Section 4 specifies the scope and requirements of each reporting phase and it specifies the outputs and stakeholder agreements expected for each phase.

Section 6 summarizes, with relevant references, specific safety critical challenge areas identified for digital or software based I&C systems.

Template drafts of a Safety Demonstration PLAN and REPORT are suggested in Appendix A and B respectively and a "quick guide" with guiding questions for respective Safety Subject Area are provided in Appendix C.

1.6 APPLICATION OF THE GUIDE IN DIFFERENT SCENARIOS

The method presented in this Guide was developed in dealing with large and complex projects but has shown generally applicable to any project involving more than a few persons, and when information is to be exchanged between several stakeholders during the project life cycle. The Safety Demonstration can and has to be customized for each new project, but it should be based on a common structure.

The elements of the guide can be used either in full or in selected parts, e.g. for introduction and application of Smart Devices and also in very limited

[1] A safety plan is not necessarily a specific document

modification projects performing component exchanges applying e.g. re- or reverse engineering) [ref. "life time extension]. Agreement on how and to what extent the Guide's advice is best applied is always part of the planning phase. Both the safety demonstration life cycle and the choice of included SSAs should be adapted in a less complex project.

Application of the Guide on a more limited scope, could for example focus on demonstrating the qualification (or suitability) of the Smart Device or component *for the intended use in a first stage* and the qualification *as integrated in the NPP parts in the second*. A Safety Demonstration lifecycle for such an application could consist of a planning phase, defining the limited Safety Demonstration Case and the plan, with two or three reporting stages – one arguing the suitability of the Smart Device or component itself (combining section 0 and 4.3) and one (or two) arguing the suitability as integrated in the actual plant (i.e. section 4.4). If two qualification reporting stages are used, one just before installation and one after.

Figure 1-2 Simplified Safety Demonstration life cycle. The complete Safety Demonstration life cycle is presented including its relation to other relevant design life cycles and references in section 2.1 and Figure 2-1.

The definition of the Safety Demonstration Case (section 2.2) can be done very simple. One general recommendation is to make sure to include aspects (possibly as SSAs) covering the product, process and documentation scope as illustrated in the two parallel balance models in section 2.2, Figure 2-4.

2 Life cycle and contents of Safety Demonstration

2.1 THE SAFETY DEMONSTRATION LIFE CYCLE

In this guide the life cycle sequence of phases indicated as marked by the frame in Figure 2-1 is used. It was derived in relation to a number of life cycles for product design as presented in selected standards and guidelines:

- "SSM 2016:25 Licensing of safety critical software for nuclear reactors. Common position of seven European nuclear regulators and authorized technical support organizations" [2].
- "IEC 61513 NPPs – Instrumentation and control important to safety – General requirements for systems"[8].
- "SSM 2006:27 Safety justification of software systems" [6].
- "IEC 15288 Systems and software engineering — System life cycle processes" [9].

Furthermore, it has taken into account the required formal reporting to the Swedish regulator (SSM) and for reference also the structure for formal reporting as required by Finnish radiation and nuclear safety authority (STUK).

In Figure 2-1 the life cycles of selected relevant references are presented side by side with the Safety Demonstration plan life cycle. The illustration shows the relation between phases as interpreted when writing this guide and defining the phases of Safety Demonstration. The yellow framed section identifies the phases of Safety Demonstration used in this Guide, the phases are derived from the life cycle of a general design process. The figure also indicates relation to corresponding phases of general design life cycles suggested in relevant standards and guides and can provide further guidance on references in the demonstration in each phase. The time lines at the top shows the required reporting according to SSM and STUK respectively.

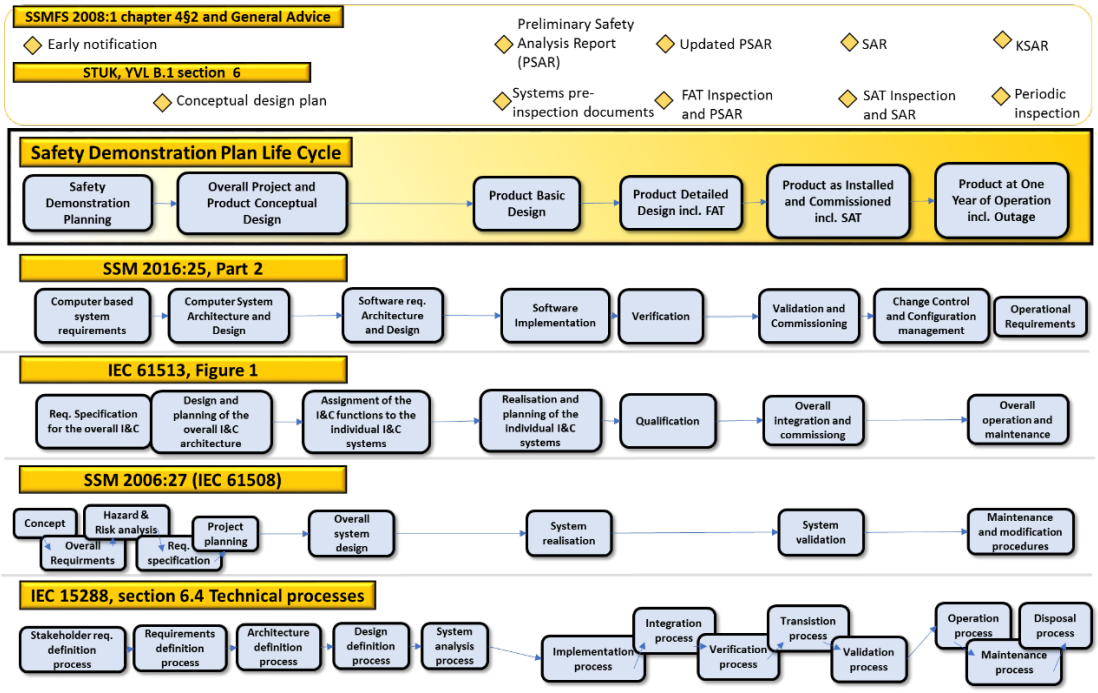


Figure 2-1 ***Safety Demonstration Life Cycle*** **(available also in Appendix D: full page format).**

The life cycle used in this Guide is divided in six phases. The phases are presented below and further described in section 3 (planning) and 4 (the following qualification phases).

- 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

Figure 2-2 illustrates the planning phase and the subsequent qualification phases of Safety Demonstration in the context of the V-model describing how the plant is changed from version "1.0" to "2.0".

The V-model represents a typical technical design development process together with the phase outputs of the Safety Demonstration life cycle defined in this guide. The callouts indicate another example of design process phases, where e.g. Functional and System Design corresponds to Basic Design. Compare with Figure 2-1, which indicates different design process phases nomenclature. Further discussions on phases and V&V strategies are found later in the guide, e.g. section 5.7 and 6.9.

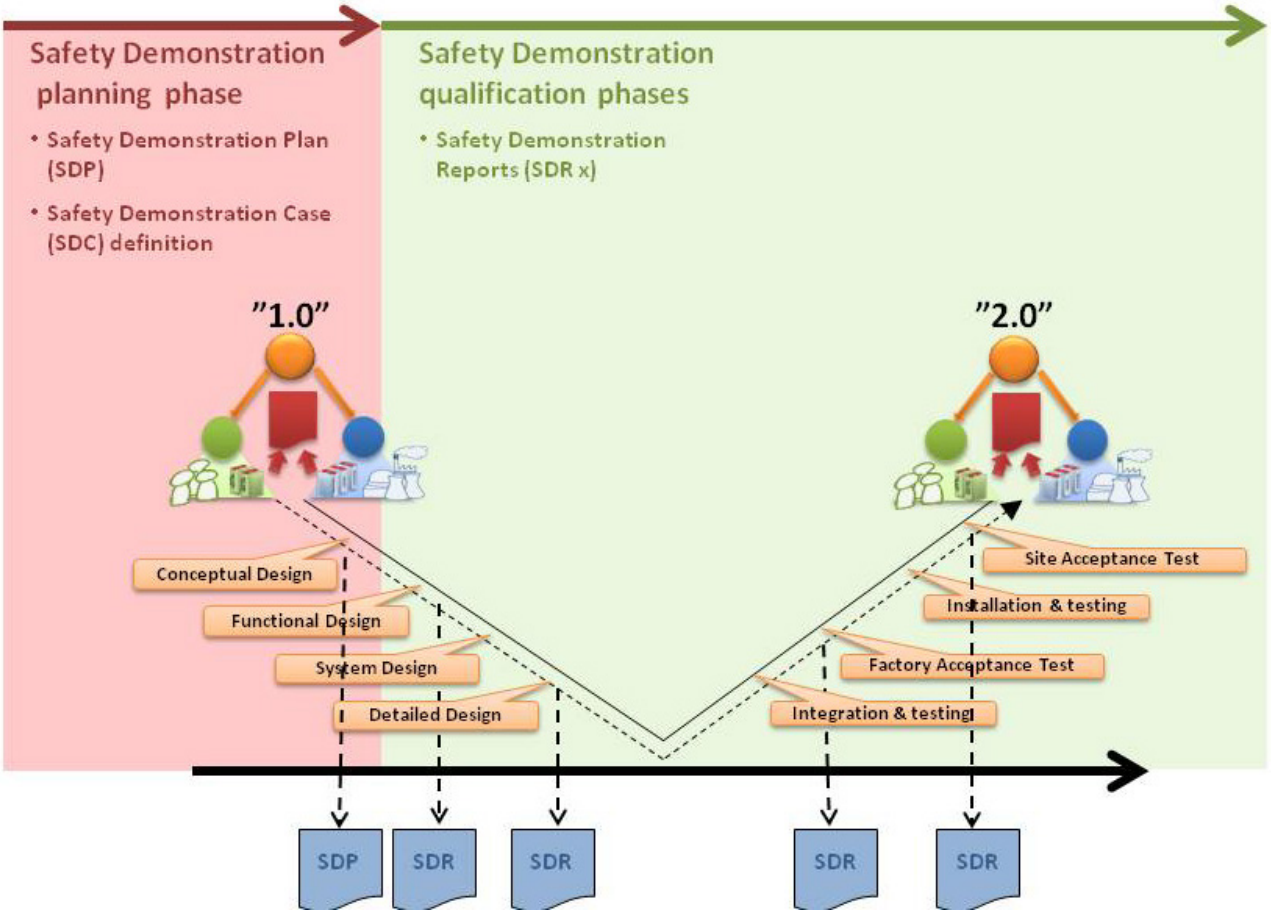


Figure 2-2 ***Safety Demonstration in the V-model.***

2.2 CONTENTS OF SAFETY DEMONSTRATION

Important principles of Safety Demonstration are in addition to the central concept of "3C" (see Terms and Abbreviations)

- Not "3C" until demonstrated "3C" - i.e. focus on positive assurance and demonstration.
- Graded approach – demonstrate safety with level of detail commensurate to its importance to safety
- Qualify not only adequate product but also work processes and competence of people involved

The last bullet is in correspondence with what is stated in SSM 2016:25 [2] with regards to what need to be demonstrated:

> *"evidence related to the quality of the development process, evidence related to the adequacy of the product and evidence of the competence and qualifications of the staff involved in all of the system life cycle phases"*

A Safety Demonstration is preferably based on a Safety Demonstration Case which serves to show that the NPP is safe after the implementation of a modernization or new build project. The Safety Demonstration Case definition contains a set of Safety Subject Areas (aspects of relevance to safety), with scope, purpose and

demonstration strategy outlined, assumed necessary to assess and demonstrate in support of a conclusion on plant safety. A sometimes attractive method to define the scope of the different areas is to formulate claims or claims hierarchies using a safety case methodology, see e.g. [2] and [10]. Each area's demonstration purpose, once defined, is fulfilled during the reporting phases by identification of suitable evidence together with argumentation. Figure 2-3 illustrates a typical model for how a Safety Demonstration Case can be defined with Safety Subject Areas (SSA) and then demonstrated fulfilled by reporting completeness, correctness and consistency with arguments and evidences. The reporting is successively accumulating along the life cycle, until a certain objective of an area is demonstrated as fulfilled. If this happens while phases still remain, the conclusion is revisited for confirmation in later stages.

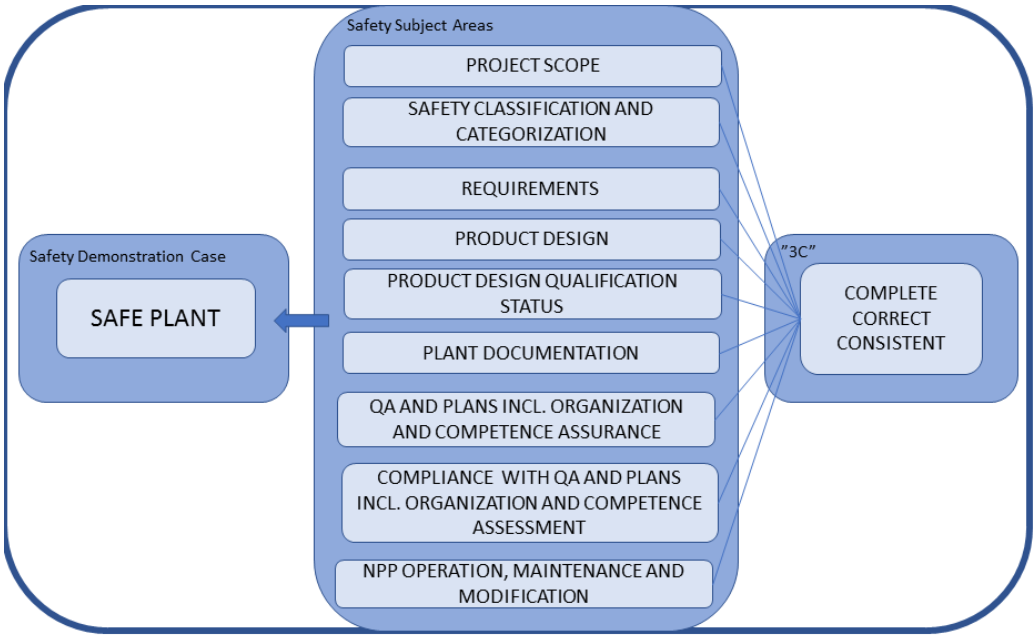


Figure 2-3 Illustration of a model for how to build the Safety Demonstration case. This model is used throughout this Guide.

2.2.1 Safety Demonstration Case

The Safety Demonstration Case is defined early in the project, in the planning phase of the Safety Demonstration life cycle. Here all scopes and purposes are formulated and the demonstration strategy to be used, including type of evidence (typically V&V-activities such as reviews, inspections, audits, analysis and tests) is indicated for each area.

The process to define the Safety Demonstration Case is a unique process for every new project. It is a central part of the Safety Demonstration and has to be performed with focus and assignment of the suitable resources in terms of time as well as staff with the relevant experience and competence.

To capture the complete scope of the Safety Demonstration it is important to include all aspects of safety at the operating NPP. In Figure 2-4 the total Safety Demonstration scope is described in a "balance model" resting on two legs; the

product or actual NPP with its design requirements and configuration information, and the process or organization with its instructing documentation including management and QA systems. It may be relevant to separate the green triangle in two, one representing the project (temporary) organization and one representing the operating organization (Licensee). The most safety important part of the complete configuration information is reported in the SAR.

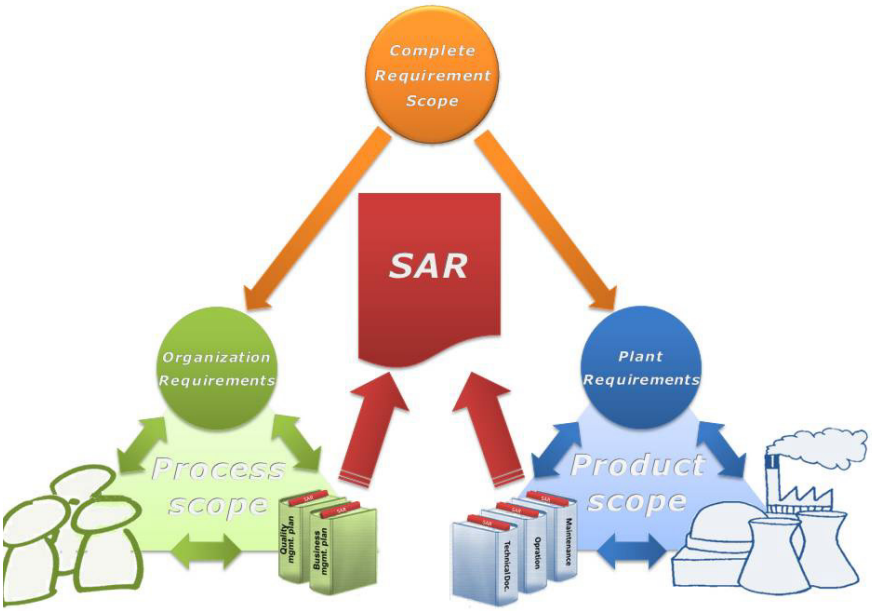


Figure 2-4 The figure illustrates the total scope of a Safety Demonstration Case by including not only the product scope, but also the process scope (i.e. the organization, processes and staff involved) as well as the required documentation for both. The figure is based on two parallel "balance models" (Process scope in green and Product scope in blue) illustrating the necessary balance of "what is required", "what is there" and "what we say is there". Keeping track of these three components and their interrelation for the process and for the product continuously throughout the project is essential for a complete and successful Safety Demonstration and licensing.

During the Safety Demonstration life cycle the areas in the Safety Demonstration Case are assessed and reported on with arguments and evidence as they develop in support of fulfillment. In each reporting phase of the Safety Demonstration life cycle the Safety Demonstration Case is evaluated based on the planned or presented evidence or confirmed based on earlier conclusions drawn.

> *"A safety case is not closed before the actual behavior of the system in real conditions of operations has been found acceptable." 2016:25 [2]*

2.2.2 Safety Subject Areas

In this Guide it is recommended to organize the Safety Demonstration Case into a number of Safety Subject Area (SSA). A SSA is defined to highlight a specific part or aspect of a Safety Demonstration.

This Guide identifies a set of recommended standard areas which are presented below and in more detail in section 5. The set of areas needs to be developed with

the specific project in focus to capture the issues and areas that are most important. At the end of section 5 several additional areas are suggested.

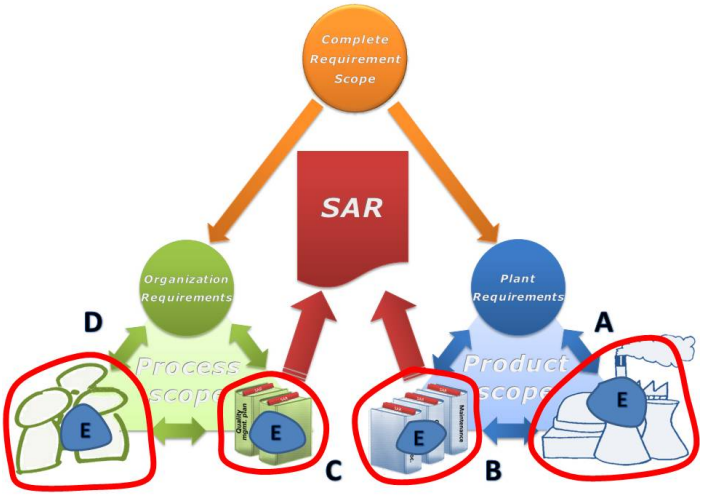
The following are the standard Safety Subject Areas:

1. Project Scope
2. Safety Classification and Categorization
3. Requirements
4. Product Design
5. Product Design Qualification Status
6. Plant Documentation
7. Quality assurance (QA) and Plans including Organization and Competence Assurance
8. QA and Plans Compliance including Organization and Competence Assessment
9. Nuclear Power Plant (NPP) Operation, Maintenance and Modification

The activity to define SSAs is the first step in the development of the project Safety Demonstration Case. Even though each SSA is discrete and needs to be defined precisely and with an open mind, the areas are also chosen to contain information that will support other areas.

The first three areas, *Project Scope*, *Safety Classification and Categorization* and *Requirements* are used throughout the rest of the areas to assess completeness, to support a graded approach and to assess correctness respectively. Figure 2-5 illustrates the interrelation of these three areas, and how they in turn are intended to relate to other areas. The requirements for the project are assessed for completeness vs the project scope, and the detail of presentation and assessment of the requirements is in proportion to safety importance in the Requirements area. A complete and correct definition of the safety classification and categorization principles is important by itself but also to support a graded approach, where the depth and detail of demonstration should be governed by the relevance for safety. The product design is then addressed in relation to scope, grading and requirements in the *Product Design* and *Product Design Qualification Status* areas. The corresponding process scope is addressed in the *QA and Plans including Organization and Competences* and the *NPP Operation, Maintenance and Modification* areas.

Many of the issues expected to be encountered originate from interface problems and from unknown or undocumented entities. Therefore, the selection of what is considered *safety scope* out of the *complete scope* is important. Figure 2-5 illustrates the safety scope as one of five subareas of the SSA 1 - *Project Scope*.



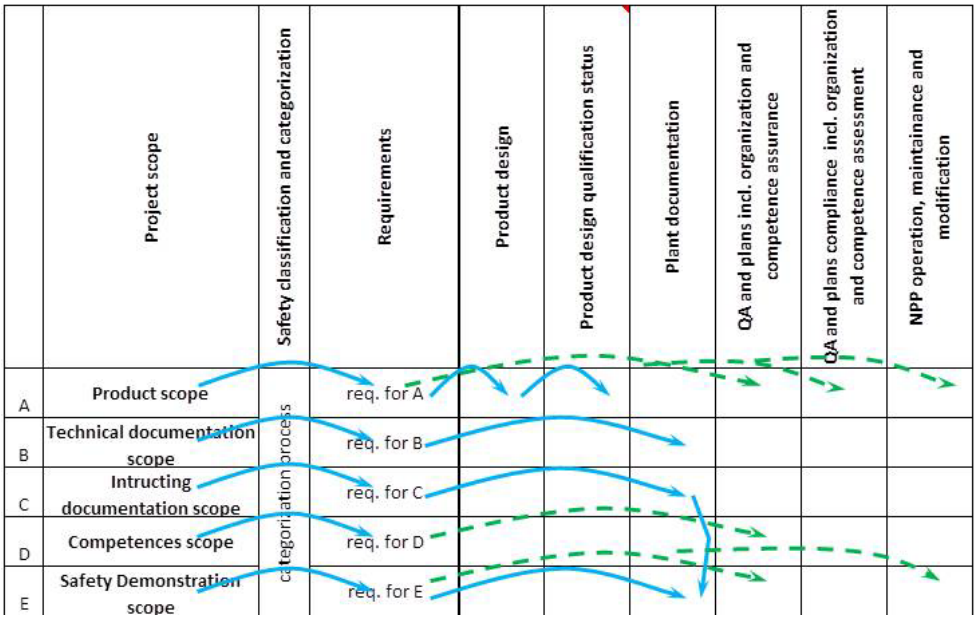


Figure 2-5 In the figure the project scope definition is divided into five subareas (A-E). Arrows describe how certain SSAs support or feed other SSAs. Blue solid arrows represent the Product related issues while green dashed arrows represent quality system, organization and competence related issues. The *complete* project scope (A-D) needs to be defined in order to assess the definition of the Safety Demonstration scope (E) out of that.

3 Safety Demonstration Planning phase

In this section the *Safety Demonstration Planning* phase is described. This phase contains the important activities of defining the Safety Demonstration Case with suitable Safety Demonstration Areas providing the basis for the demonstration of safety for the project throughout the project life cycle. In the *Safety Demonstration Planning* phase, the life cycle of the Safety Demonstration is developed in relation to the project life cycle and with appropriate safety reporting to the regulator and stakeholder. The Safety Demonstration life cycle as defined in this Guide is illustrated in Figure 3-1, highlighting the *Safety Demonstration Planning* phase with the output of this phase, the Safety Demonstration Plan (SDP).

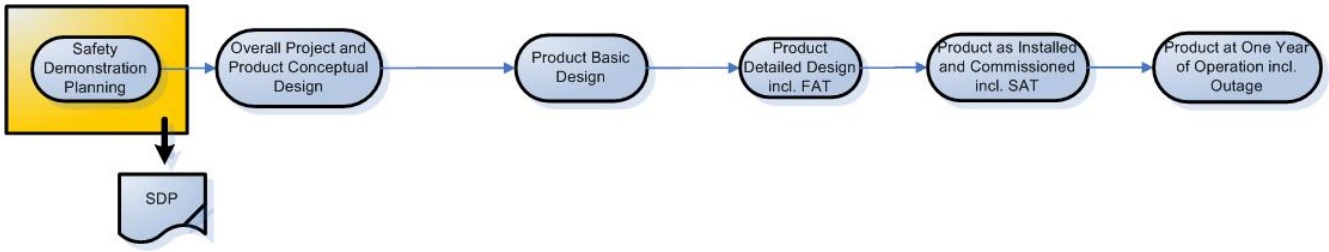


Figure 3-1 The *Safety Demonstration Planning* phase prepares the Safety Demonstration Plan (SDP) and plans for the formal safety review and Safety Report.

3.1 OBJECTIVES

The objectives of a *Safety Demonstration Planning* phase are:

- To identify how (what – by whom – when – how) the NPP project will assure and demonstrate Plant Safety, both during and after the modernization or new build.
- To identify what will be presented to the regulator and when, both for information, review and for requesting formal permits respectively.
- To define the Safety Demonstration Case and contents grouped into SSAs with accompanying strategies to demonstrate compliance.
- To elaborate on the approach for Safety Demonstration, and the strategy for implementation to a level of detail that makes the licensing process practical, comprehensible and straight-forward enough to the parties involved.
- To allow for smooth transformation of relevant parts of the qualification into the formal safety report, e.g. Preliminary Safety Analysis Report (PSAR), Safety Analysis Report (SAR), Technical Specifications (TS) and to support safety reviews, which all together will be used in the request for operating permit after the plant modernization or new build.
- To document the philosophy, outline and plans for the Safety Demonstration Reports.

3.2 SCOPE

The scope of the *Safety Demonstration Planning* phase is to develop and agree on a Safety Demonstration Plan including the scope of the Safety Demonstration, the processes involved, the schedule and the required organization, see Table 3-1.

3.3 REQUIREMENTS

The requirement on the *Safety Demonstration Planning* phase is to produce a plan including a Safety Demonstration Case definition agreed upon and committed to by all stakeholders involved.

3.4 SAFETY DEMONSTRATION CASE DEFINITION

The Safety Demonstration Case definition is a central activity for a successful Safety Demonstration and therefore needs to be prioritized and assigned with sufficient resources in terms of time and competences. For more details see "Safety Demonstration Case" under section 2.2.

3.4.1 Safety Subject Areas definition

A relevant and sufficient set of SSAs with underlying scope and strategies are to be defined. These areas shall together be able to demonstrate that the plant is safe during and after the implementation of the project.

Table 3-1 Showing the scope of the *Safety Demonstration Planning* phase (column marked yellow) and all subsequent qualification phases. In the *Safety Demonstration Planning* phase all SSAs are specified. The areas given in this table are suggested standard areas.
s (specify); The area is specified during the phase.
F (focus); There is important information expected to these areas during the phase.
i (identify); Information might be available and in that case the area needs focus.
c (confirm); The information in this area is already qualified in a previous phase, but the status should be confirmed.

	Planning Phase	**Qualification phases**				
SSA	Safety Demonstration Planning	Overall Project and Product Conceptual Design	Product Basic Design	Product Detailed Design including FAT	Product as Installed and Commissioned incl. SAT	Product at One Year of Operation incl. Outage *
1 - Project Scope	s	F	c	c	c	-
2 - Safety Classification and Categorization	s	F	c	c	c	c
3 - Requirements	s	F	c	c	c	c
4 - Product Design	s	i	F	F	c	c
5 - Product Design Qualification Status	s	-	F	F	F	c
6 - Plant Documentation	s	-	i	F	F	c

	Planning Phase	Qualification phases				
7 - QA and Plans incl. Organization and Competence Assurance	s	F	c	c	c	c
QA and Plans Compliance incl. Organization and Competence assessment	s	i	F	F	F	i
Operation, Maintenance and Modification	s	-	-	i	F	F

* the actual project might be ended before "one year of operation including outage" and therefore the last phase of the Safety Demonstration may have to be planned and governed by the Licensee, independent of the project.

3.4.2 Safety Demonstration strategies development

For each SSA a strategy about how to demonstrate safety is developed. The strategy contains description of what type of evidence that will be used and arguments for safety.

3.5 RELATION TO FORMAL SAFETY REPORT AND SAFETY REVIEW

Safety Demonstration is an integrated part of the Project Safety Review and should support the formal Safety Report i.e. SAR and TS to the regulating authority. Processes and strategies for Safety Review should be specified during the *Safety Demonstration Planning* phase and include the NPP standard routines for how to perform Safety review as well as the role of the Safety Demonstration in those processes. The role of the Safety Demonstration Plan (SDP) and Reports (SDRs) in relation to other Plant Documents (including SAR, PSAR, TS, PSA etc.) should be specified.

The Safety Demonstration Reports can allow and provide complementing and more explicit and detailed references and argumentation in relevant subjects for the specific project, that the overall balance of detail in the SAR isn't suitable for. Safety Demonstration can also provide the gathered description and assessment discussion of a certain issue, where the corresponding information in the SAR may be scattered in several bits and pieces, due to format constraints.

3.6 SAFETY DEMONSTRATION LIFE CYCLE OVERVIEW DIAGRAM

The Safety Demonstration Plan should have an overview diagram showing the time wise correlation between the activities of the Safety Demonstration stakeholder (including regulator, Licensee, the NPP project and possible suppliers,) and the outputs of the Safety Demonstration. A general example of a Safety Demonstration overview diagram can be found in Figure 3-2

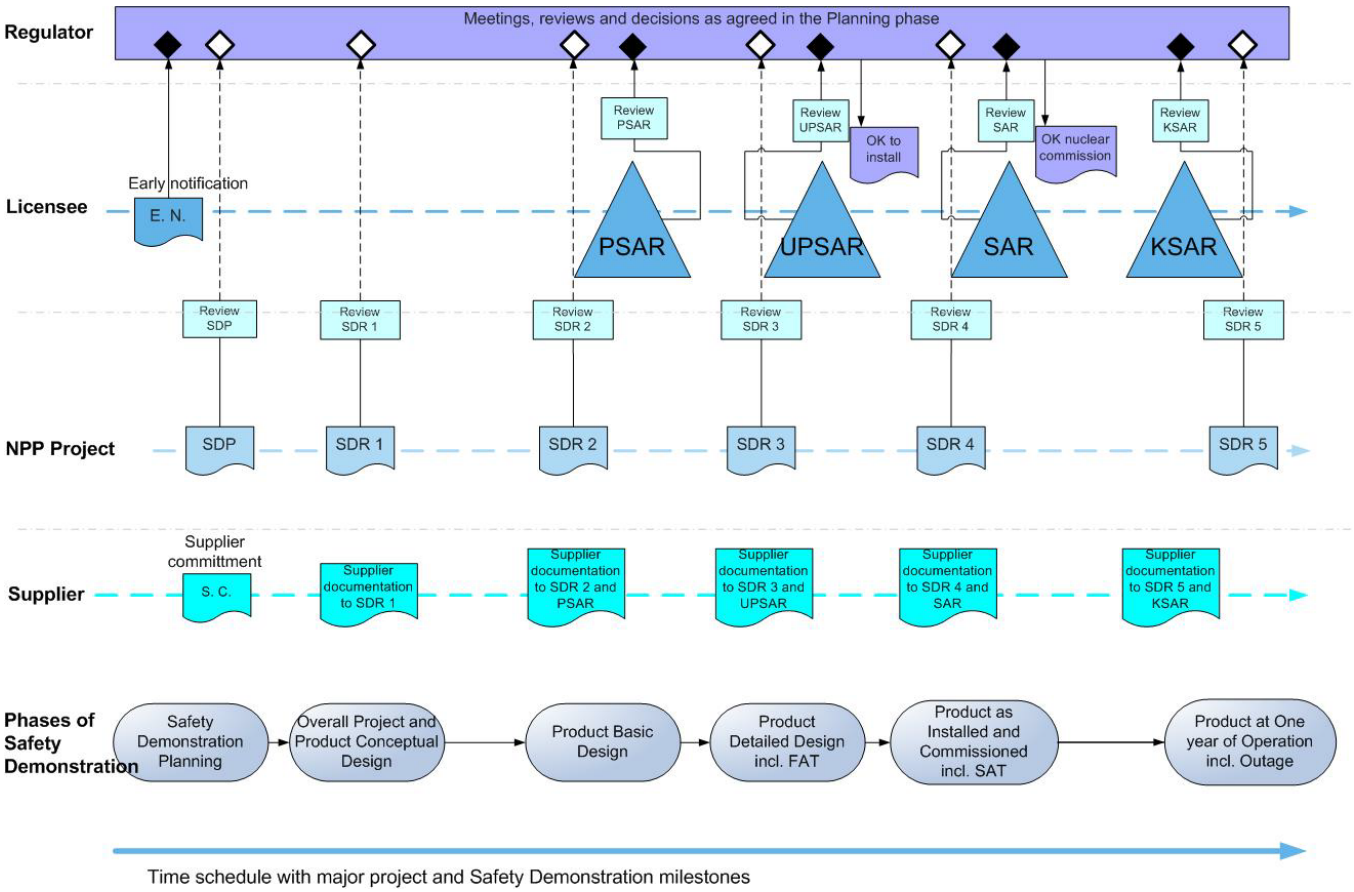


Figure 3-2 Illustration of a typical life cycle overview diagram in a Safety Demonstration Plan. Important activities and output documents during the Safety Demonstration life cycle are introduced for the main project stakeholders; Supplier, NPP Project, Licensee and Regulator. The figure is available also in Appendix E: in full page format

3.7 PHASE RESULTS AND STAKEHOLDER AGREEMENTS

Phase outputs:

- Safety Demonstration Plan (SDP) including the Safety Demonstration Case.

Stakeholder activities:

- The activities of stakeholders during the *Safety Demonstration Planning* phase is given in Table 3-2.

Table 3-2 Presents the typical activities related to Safety Demonstration expected to take place in the Safety Demonstration Planning phase. The stakeholders given in the table might be represented by "sub-stakeholders" and additional stakeholders might be suitable to appoint in a specific project.

	Safety Demonstration Planning
Supplier	- Provide input to SDP - Accept plan and commitments according to plan
NPP project	- Produce SDP including Safety Demonstration Case (SDC) definition - Ensure that the SDP and SDC are reviewed and approved

	Safety Demonstration Planning
Licensee	- Review and approve SDP with commitments - Communicate SDP with regulator
Regulator	- Agree to SDP and accept regulator actions

Phase result agreements:

- All the defined stakeholders are to accept the contents of the SDP, i.e. the definitions of what, when, by whom and high-level how to do to complete the Safety Demonstration.

4 Safety Demonstration Qualification phases

In this section five Qualification phases of Safety Demonstration are described with scope and requirements. The outputs and agreements needed for the phase to be qualified are specified in the last section of each phase. The Safety Demonstration Report for each phase is based on an update and confirmation of the Safety Demonstration Case defined in the *Safety Demonstration Planning* phase as discussed in Section 3. The contents in SSAs and Safety Demonstration as a whole, are further addressed in Section 5.

4.1 QUALIFICATION OF THE OVERALL PROJECT AND PRODUCT CONCEPTUAL DESIGN

The first qualification phase in a Safety Demonstration, illustrated in Figure 4-1, puts focus on the qualification of the project establishment, with scope and high-level requirements and on the Product Conceptual Design. The objective with the phase is to prepare the first Safety Demonstration report (SDR 1).

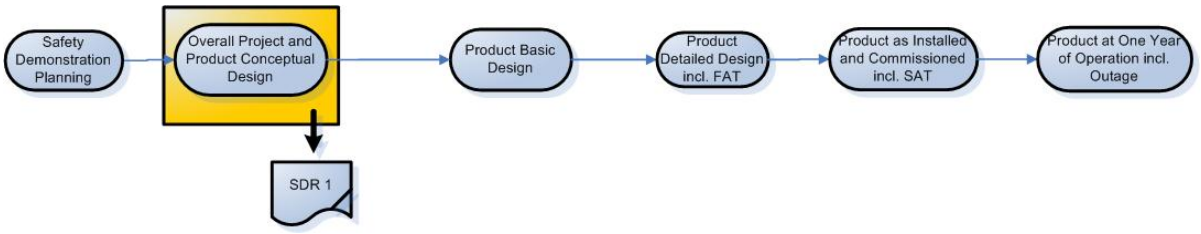


Figure 4-1 The first qualification phase in the Safety Demonstration life cycle prepares the first Safety Demonstration Report (SDR 1) and information for the early notification report to the regulator.

4.1.1 Scope

The scope of the *Overall Project and Product Conceptual Design* qualification phase (see Table 4-1) is to identify and assess:

- Project Scope
- Principles for Safety Classification and Categorization
- Overall Requirements
- Project Quality Processes, Management System and Plans
- Organization and Competences
- Possibly also Conceptual or Architectural Design including I&C system platform.

Table 4-1 Presenting the focus for the Safety Demonstration in the *Overall Project and Product Conceptual Design* qualification phase.
F (focus): There is important information expected to this area during the phase.
i (identify): Information might be available and in that case the area needs focus.

SSA	Overall Project and Product Conceptual Design	Scope	Requirements
1 – Project Scope	F	Project scope definition (including Product, technical documentation, instructing documentation, competences)	Project scope definition "3C" and agreed by all stakeholders.
2 - Safety Classification and Categorization	F	Overall principles for safety classification and categorization	Safety classification and categorization principles "3C" as defined
3 - Requirements	F	Overall high-level requirements specification	High-level requirements "3C", e.g. that I&C requirements originate with traceability from the Plant design basis (may require significant iteration) and that relevant portions of chapter 6 challenge areas are properly reflected.
4 - Product Design	i	Product Architectural Design (or Conceptual Design)	The design version identified and assessed for "3C". *
5 - Product Design Qualification Status	-	Not in scope this phase unless chosen to add	If applicable, any V&V records identified support product design qualification at present status
6 - Plant Documentation	-	Not in scope this phase unless chosen to add	If applicable, any identification of impact to documentation in scope (new, to be revised or deleted)
7 - QA and Plans incl. Organization and Competence Assurance	F	Quality Management system, organization and plans. Specifically, CM, V&V, Competence and staffing management for the whole project life cycle	QA and plans defined "3C". CM in place and sufficient coverage of V&V as planned. Safety Culture in clear organization with competence and staffing management in place.
8 - QA and Plans Compliance incl. Organization and Competence Assessment	i	Compliance to QA and plans as defined above for present phase. Handle the area as "F" when applicable.	Qualified QA Compliance as defined for the phase. Any deviations motivated and accepted.
9 - NPP Operation, Maintenance and Modification	-	Not in scope for this phase.	-

*The Product is identified and assessed for completeness in the *Product Design* area and qualified with V&V records in the *Product Design Qualification Status* area. The processes for product design are assessed for "3C" in the QA and Plans incl. Organization and Competence Assurance area.

4.1.2 Requirements

The requirements on the *Overall Project and Product Conceptual Design* phase are to demonstrate a defined scope of the phase and to assess the scope for "3C", according to Table 4-1.

4.1.3 Phase results and stakeholder agreements

Phase output:

- First Safety Demonstration Report (SDR 1) version issued, including a confirmed or updated Safety Demonstration Case.

Stakeholder activities:

- The stakeholder activities during the *Overall Project and Product Conceptual Design* phase is given in Table 4-2.

Table 4-2 Presents the typical activities related to Safety Demonstration expected to take place in the Overall Project and Product Conceptual Design phase. The stakeholders listed in the table might be represented by "sub-stakeholders" and additional stakeholders might be suitable to appoint in a specific project.

	Qualification of the Overall Project and Product Conceptual Design
Supplier	- Provide supplier scope SDR input to NPP project
NPP project	- Produce SDR - Ensure that the SDR is reviewed and approved
Licensee	- Review and approve SDR - Communicate SDR with regulator
Regulator	- Accept defined scope, high-level requirements and possible conceptual or architectural design as well as QA and plans

Phase result acceptance:

- All stakeholders are to accept the contents of SDR 1 i.e. the project scope, safety classification and categorization principles, the high-level requirements, the project governance and quality assurance, plans and organization.
- The conceptual or architectural design, if applicable.

4.2 QUALIFICATION OF THE PRODUCT BASIC DESIGN

The second qualification phase in a Safety Demonstration, illustrated in Figure 4-2, puts focus on the *Product Basic Design*, its preliminary Qualification and when applicable also a preliminary Safety Report. If needed this qualification phase can be performed in more than one step for example Functional Design and System Design. The preferred steps should be defined in the SDP as described in section 3. The objective of the phase is to prepare the second Safety Demonstration report (SDR 2) and to provide information for the Preliminary Safety Analysis Report (PSAR).

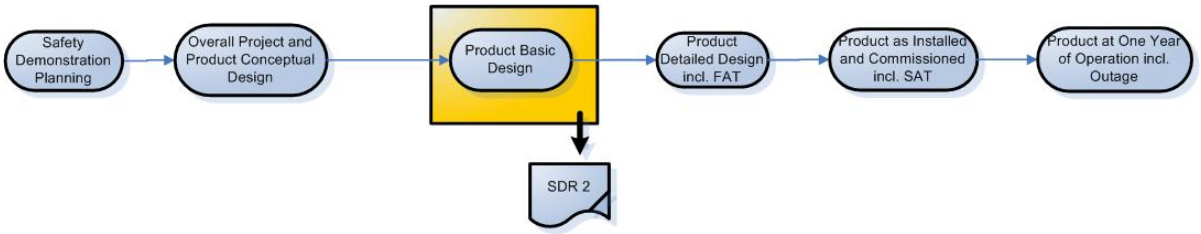


Figure 4-2 The second qualification phase in the Safety Demonstration life cycle prepares the second Safety Demonstration Report (SDR 2) and provides information for the preliminary Safety Analysis Report (PSAR).

4.2.1 Scope

The scope of the *Product Basic Design* phase (see Table 4-3) is to identify and assess the:

- Product design version with implemented design requirements
- Product design qualification relevant to the design version
- QA and plans compliance as applicable in this phase
- Preliminary Safety Analysis Report (PSAR), when applicable

During this phase the impact of the project on the present Plant Documentation can be identified. Additional to the focus areas all SSAs that have been reported on are confirmed unchanged or revised in the phase report.

Table 4-3 Presenting the focus for the Safety Demonstration in the *Product Basic Design* qualification phase.
F (focus): There is important information expected to this areas during the phase.
i (identify): Information might be available and in that case the area needs focus.
c (confirm): The information in this area is already qualified in a previous phase, but the status should be confirmed.

SSA	Product Basic Design	Scope	Requirements
1 - Project Scope	**c**	Project scope definition	Confirmed "3C" as assessed before, including possible changes
2 - Safety Classification and Categorization	**c**	Overall principles for safety classification and categorization	Confirmed "3C" as assessed before, including possible further specification and/or changes
3 - Requirements	**c**	High-level requirements and traceability to derived requirements (e.g. typically Functional-, System- and Interface, HSI, HW and SW requirements)	High-level requirements confirmed "3C" as assessed before (or as changed) and derived requirements traceable and "3C"
4 - Product Design	**F**	Product basic design	The design version identified and assessed for "3C". *
5 - Product Design Qualification Status	**F**	Product basic design qualification with reference to V&V records	Qualification of product basic design "3C".
6 - Plant Documentation	**i**	Plant Documentation	The project impact on Plant Documentation "3C" defined. A PSAR or equivalent is presented and agreed when applicable.
7 - QA and Plans incl. Organization and Competence Assurance	**c**	Same as earlier phase	Confirmed "3C" as assessed before, including possible changes.
8 - QA and Plans Compliance incl. Organization and Competence Assessment	**F**	Compliance to QA and plans as defined above for present phase.	Qualified QA Compliance as defined for the phase. Any deviations motivated and accepted.
9 - NPP Operation, Maintenance and Modification	**c**	Any identified impact on normal NPP organization operation, maintenance and change handling	Sufficient plans for the identified impact, if applicable.

*The Product is identified and assessed for completeness in the *Product Design* area and qualified with V&V records in the *Product Design Qualification Status* area. The processes for product design are assessed for "3C" in the QA and Plans incl. Organization and Competence Assurance area.

4.2.2 Requirements

The requirements on the *Product Basic Design* phase are to demonstrate a defined scope of the phase and to assess the scope for "3C" according to Table 4-3.

4.2.3 Phase results and stakeholder agreements

Phase output:

- Second Safety Demonstration Report (SDR 2) version issued including a confirmed or updated Safety Demonstration Case definition.

- Preliminary Safety Analysis Report (PSAR), if applicable.

Stakeholder activities:

- The activities of each stakeholder during the *Qualification of the Product Basic Design* phase is given in Table 4-4.

Table 4-4 Presents the typical activities related to Safety Demonstration and expected to take place in the Product Basic Design phase. The stakeholders given in the table might be represented by "sub-stakeholders" and additional stakeholders might be suitable to appoint in a specific project.

	Qualification of Product Basic Design
Supplier	- Provide supplier scope SDR input to NPP project
NPP project	- Produce SDR - Ensure that the SDR is reviewed and approved
Licensee	- Review and approve SDR - Communicate SDR with regulator
Regulator	- Accept basic design status

Phase result acceptance:

- All stakeholders are to accept the contents of the SDR 2, i.e. the Basic Design and its Qualification, compliance to QA and Plans and any updates to earlier reporting and the Safety Demonstration Case definition.
- Preliminary Safety Report (PSAR), if applicable.

4.3 QUALIFICATION OF THE PRODUCT DETAILED DESIGN INCLUDING FAT

The third qualification phase in a Safety Demonstration, illustrated in Figure 4-3, puts focus on the manufactured and integrated product ready for shipping to site or for installation and correspond to Factory Acceptance Test (FAT). The objective with the phase is to prepare the third Safety Demonstration report (SDR 3) and to provide information for the Updated Preliminary Safety Analysis Report (UPSAR).

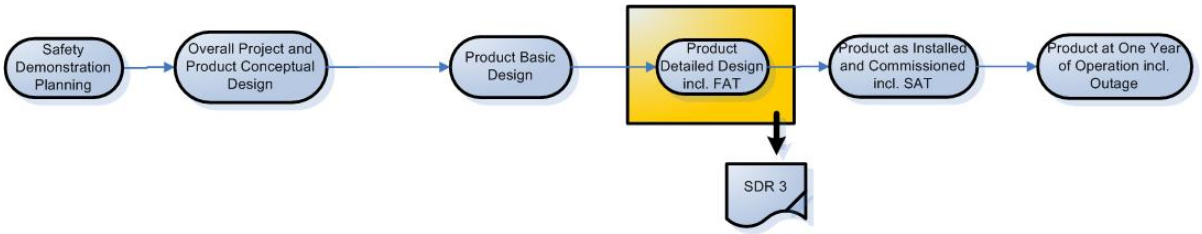


Figure 4-3 The third qualification phase in the Safety Demonstration life cycle prepares the third Safety Demonstration Report (SDR 3) and provides information for the Updated Preliminary Safety Analysis Report (UPSAR to decide on installation start on and/or SAR to start commissioning on as applicable).

4.3.1 Scope

The scope of the *Product Detailed Design including FAT* (see also Table 4-5) phase is to assess the

- Product detailed design version
- Product design qualification of the detailed design
- QA and plans compliance as applicable in this phase
- Project impact on the plant documentation as it develops in this phase
- Updated Preliminary Safety Analysis Report (UPSAR)

Within the scope of this phase is also to start identifying the organization and processes needed for normal operation, maintenance and modification. Additional to the focus areas *all* SSAs that have been reported on earlier are either to be confirmed unchanged or revised in this phase report.

Table 4-5 Presenting the focus for the Safety Demonstration in the Product Detailed Design incl. FAT qualification phase.
F (focus): There is important information expected to these areas during the phase.
i (identify): Information might be available and in that case the area needs focus.
c (confirm): The information in this area is already qualified in a previous phase, but the status should be confirmed.

SSA	Product Detailed Design including FAT	Scope	Requirements
1 - Project Scope	c	Project scope definition	Confirmed "3C" as assessed before, including possible changes
2 - Safety Classification and Categorization	c	Overall principles for safety classification and categorization	Confirmed "3C" as assessed before, including possible further specification and/or changes
3 - Requirements	c	Defined high-level requirements and traceability to derived requirements	High-level requirements confirmed "3C" as assessed before (or as changed) and derived requirements traceable and "3C"
4 - Product Design	F	Product detailed design at FAT	The design version identified and assessed for "3C". *
5 - Product Design Qualification Status	F	Design qualification at FAT	Qualification of Product detailed design and FAT "3C". When applicable, accepted to ship to site for installation.
6 - Plant Documentation	F	Plant Documentation that should be in place during the detailed design phase according to plans.	The required and agreed Plant Documentation for the present phase is "3C". Also, an Updated PSAR and TS when applicable.
7 - QA and Plans incl. Organization and Competence Assurance	c	Same as in earlier phase.	Confirmed "3C" as assessed before, including possible changes.
8 - QA and Plans Compliance incl. Organization and Competence Assessment	F	Compliance to QA and plans as defined above for present phase.	Qualified QA Compliance as defined for the phase. Any deviations motivated and accepted.
9 - NPP Operation, Maintenance and Modification	i	Any identified impact to normal NPP operation, maintenance and change handling (governance and organization)	Sufficient plans for timely handling of the identified impact, if applicable.

*The Product is identified and assessed for completeness in the *Product Design* area and qualified with V&V records in the *Product Design Qualification Status* area. The processes for product design are assessed for "3C" in the QA and Plans incl. Organization and Competence Assurance area.

4.3.2 Requirements

The requirements on the *Product Detailed Design incl. FAT* phase are to demonstrate the defined scope of the phase and to assess the scope for "3C", according to Table 4-5.

4.3.3 Phase results and stakeholder agreements

Phase output:

- Third Safety Demonstration Report (SDR 3) including a confirmed or updated Safety Demonstration Case definition.
- Updated Preliminary Safety Report when applicable.

Stakeholder activities:

- The activities of each stakeholder during the *Qualification of the Product Detailed Design including FAT* phase is given in Table 4-6.

Table 4-6 Presents the typical activities related to Safety Demonstration and expected to take place the *Product Detailed Design including FAT* phase. The stakeholders given in the table might be represented by "sub-stakeholders" and additional stakeholders might be suitable to appoint in a specific project.

	Qualification of Product Detailed Design including FAT
Supplier	- Provide supplier scope SDR input to NPP project
NPP project	- Produce SDR - Ensure that the SDR is reviewed and approved
Licensee	- Review and approve SDR - Communicate SDR with regulator and request permission to start installation - Decision on installation
Regulator	- Accept Design at FAT status - Permission to start of installation, if applicable

Phase result acceptance:

- All stakeholders to accept the contents of the SDR 3 i.e. the detailed design and its Qualification. Also, compliance to QA and plans, readiness for installation and updates to earlier reporting and possible updates on the Safety Demonstration case definition.
- Decision to start installation according to NPP procedures, based on SDR 3 acceptance above.
- Regulator permission to start installation, if applicable.
- Updated Preliminary Safety Analysis Report (UPSAR), if applicable.

4.4 QUALIFICATION OF PRODUCT AS INSTALLED AND COMMISSIONED INCLUDING SAT

The fourth qualification phase in a Safety Demonstration, illustrated in Figure 4-4, puts focus on the installed and commissioned product corresponding to Site Acceptance Test (SAT). The objective with the phase is to assess that the product has been implemented completely and correctly in the plant for safe turnover to operation and to prepare the fourth Safety Demonstration report (SDR 4) and updated material for the SAR, if applicable.

The phase may need staged reporting, one in support on decision to start nuclear operation for testing (SAT 2) and one in support on decision for turnover to normal operation and maintenance after successful SAT 2 and complete V&V. This may, due to the short time from test completion to necessary decision, call for SDR 4 to be issued in advance, clearly defining what is required to demonstrate additionally from SAT 1 in support of decision to start nuclear testing or SAT 2 and from SAT 2 in support of decision to turnover to normal operation and maintenance respectively. The additional reporting can then be performed efficiently with SDR 4 SAT 1 and SDR 4 SAT 2 supplements complementing the SDR 4 issued in advance.

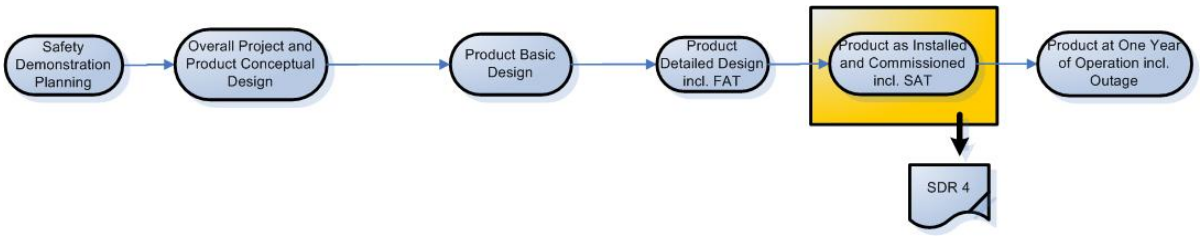


Figure 4-4 The fourth qualification phase in the Safety Demonstration life cycle prepares the fourth Safety Demonstration Report (SDR 4) with possible supplements supporting the decisions to start nuclear testing and to start normal operation. If applicable it also provides information for revision of the Safety Analysis Report (SAR).

4.4.1 Scope

The scope of the *Product as Installed and Commissioned including SAT* phase (see Table 4-7) is to assess and verify the

- Product design qualification of the installed and commissioned design
- QA compliance as applicable in this phase
- Plant documentation needed for commissioning and operation

Within the scope of this phase is also to identify and assess the organization and processes needed for normal operation, maintenance and modification. Additional to the focus areas *all* SSAs that have been reported on earlier are either to be confirmed unchanged or revised in the phase report.

Table 4-7 Presenting the focus for the Safety Demonstration in the *Product as Installed and Commissioned including SAT* qualification phase.
F (focus): There is important information expected to these areas during the phase.
i (identify): Information might be available and in that case the area needs focus.
c (confirm): The information in this area is already qualified in a previous phase, but the status should be confirmed.

SSA	Product as Installed and Commissioned including SAT	Scope	Requirements
1 - Project Scope	c	Project scope definition	Confirmed "3C" as assessed before, including possible changes
2 - Safety Classification and Categorization	c	Qualified safety classification and categorization	Confirmed "3C" as assessed before, including further specification and/or possible changes
3 - Requirements	c	Defined high-level requirements and traceability to derived requirements	High-level requirements confirmed "3C" as assessed before or as changed and derived requirements traceable and "3C"
4 - Product Design	c	Design as installed and commissioned incl SAT	The design version confirmed "3C" as assessed before or as changed with same requirements as in earlier phase
5 - Product Design Qualification status	F	Design qualification at SAT, functional V&V	Qualification of installed product design "3C". No unacceptable assumptions remaining to confirm by V&V.
6 - Plant Documentation	F	Plant Documentation that should be in place for nuclear commissioning tests and operation	The required and agreed Plant Documentation for the present phase is "3C". Also a valid SAR and TS for operation.
7 - QA and Plans incl. Organization and Competence Assurance	c	Same as in earlier phase	Confirmed "3C" as assessed before, including possible changes.
8 - QA and Plans Compliance incl. Organization and Competence Assessment	F	Compliance to QA and plans as defined above for present phase.	Qualified QA compliance as defined for the phase. Any deviations motivated and accepted.
9 - NPP Operation, Maintenance and Modification	F	Normal NPP operation, maintenance and change handling (governance, documentation, tools and organization)	Organization sufficient and prepared to safely operate, maintain and modify NPP as qualified and handed over.

SSA	Product as Installed and Commissioned including SAT	Scope	Requirements
*The Product is identified and assessed for completeness in the *Product Design* area and qualified with V&V records in the *Product Design Qualification Status* area. The processes for product design are assessed for "3C" in the QA and Plans incl. Organization and Competence Assurance area.			

4.4.2 Requirements

The requirements on the *Product as Installed and Commissioned including SAT* phase are to demonstrate a defined scope of the phase and to assess the scope for "3C" (according to Table 4-7).

4.4.3 Phase results and stakeholder agreements

Phase output:

- Fourth Safety Demonstration Report (SDR 4) including confirmed or updated Safety Demonstration Case definition. Possibly also supplemental SAT 1 report in support of decision to start nuclear SAT 2 and SAT 2 report in support of decisions to start normal operation after SAT 2.
- Safety Analysis Report (SAR), if applicable.

Stakeholder activities:

- The activities of each stakeholder during the *Product as Installed and Commissioned including SAT Qualification* phase is given in Table 4-8.

Table 4-8 Presents the typical activities related to Safety Demonstration and expected to take place the Product as Installed and Commissioned incl. SAT phase. The stakeholders given in the table might be represented by "sub-stakeholders" and additional stakeholders might be suitable to appoint in a specific project.

	Qualification of Product as Installed and Commissioned including SAT
Supplier	- Provide supplier scope SDR input to NPP project
NPP project	- Produce SDR, possibly with separate SAT 1 and SAT 2 reports respectively - Ensure that the SDR and its supplements are reviewed and approved
Licensee	- Review and approve SDR, and possible supplements - Communicate SDR with regulator and request permission to start nuclear SAT 2 and operation - Decision on start nuclear SAT 2 - Decision on turnover to operation and maintenance after SAT 2 complete
Regulator	- Accept Design at SAT 1 and SAT 2 status respectively - Permission to start nuclear SAT 2 and/or turn over to operation as applicable

Phase result acceptance:

- All stakeholders to accept the contents of the SDR 4 possibly supplemented with SAT 1 and SAT 2 reports as described in the introduction to section 4.4. This means acceptance of the product as installed, commissioned and validated in the NPP together with the conclusion on appropriate organizational preparedness, and Plant Documentation for safe operation, maintenance and changes assured.
- Staged decisions to start nuclear SAT 2 and to turn over to operations and maintenance after SAT 2 respectively, based on the acceptance of SDR 4 and all according to the NPP procedures.
- Regulator permission to start nuclear SAT 2 and turnover to operation after SAT 2, where applicable.

4.5 QUALIFICATION OF PRODUCT AT ONE YEAR OF OPERATION INCLUDING OUTAGE

The fifth qualification phase of a Safety Demonstration puts focus on the safe operation and maintenance of the plant with the new Product installed. The phase is entered after the commissioning or after SAT and covers the first period of operation including the following refueling outage. The objective is to assess that the plant can be operated safely and satisfyingly for final acceptance, to prepare the fifth and final Safety Demonstration Report (SDR 5) and complementing material to the SAR (KSAR). Normally the project ends during this phase and the reporting focuses on the plant as operated by the normal NPP organization.

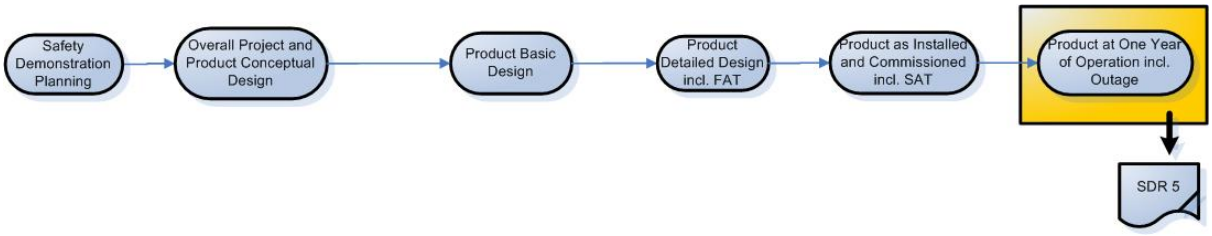


Figure 4-5 The fifth qualification phase in the Safety Demonstration life cycle prepares the fifth Safety Demonstration Report (SDR 5) and eventual complementing information to the SAR (KSAR).

4.5.1 Scope

The scope of the *Product at One Year of Operation including Outage* phase (see Table 4-9) is to assess and verify

- That the product design as operated does not unacceptably challenge the design as it was Qualified in earlier phases.
- Processes and documentation in place, functional and applied, in the NPP organization for safe and correct operation, maintenance and handling of changes in the plant.
- QA Compliance as applicable for the Project in this phase, to the degree the project is still active.

Table 4-9 Presenting the focus for the Safety Demonstration in the Product at One Year of Operation incl. Outage qualification phase.
F (focus): There is important information expected to these areas during the phase.
i (identify): Information might be available and in that case the area needs focus.
c (confirm): The information in this area is already qualified in a previous phase, but the status should be confirmed.

SSA	Product at One Year of Operation including Outage	Scope	Requirements
1 - Project Scope	-	As earlier phases when applicable; project may be finished	-
2 - Safety Classification and Categorization	c	Qualified safety classification and categorization	Confirmed "3C" as assessed before, including possible changes

SSA	Product at One Year of Operation including Outage	Scope	Requirements
3 - Requirements	c	Defined high-level requirements and traceability to derived requirements	High-level requirements confirmed "3C" as assessed before or as changed and derived requirements traceable and "3C"
4 - Product Design	c	Design as operated.	The design version confirmed "3C" as assessed before, or as changed with same requirements as in earlier phase.
5 - Product Design Qualification Status	c	Design Qualification as operated	No unacceptable findings with regards to the product qualification during operation and outage
6 - Plant Documentation	c	Plant Documentation that should be in place for NPP operation	Confirm "3C" as taken into operation or as after change or revision.
7 - QA and Plans incl. Organization and Competence Assurance	(c)	As earlier phases when applicable; project may be finished - if so assess operating organization in SSA 9 - *NPP Operation, Maintenance and Modification*	-
8 - QA and Plans Compliance incl. Organization and Competence Assessment	i	As earlier phases when applicable; project may be finished.	-
9 - NPP Operation, Maintenance and Modification	F	Normal NPP operation, maintenance and change handling (governance, documentation, tools and organization)	Demonstrated Safe and correct operation, maintenance and modification (both that the proper governance and a sufficient organization with tools and documentation is in place and that the governance has been properly applied and complied to)

*The Product is identified and assessed for completeness in the *Product Design* area and qualified with V&V records in the *Product Design Qualification Status* area. The processes for product design are assessed for "3C" in the QA and Plans incl. Organization and Competence Assurance area.

4.5.2 Requirements

The requirements on the *Product at One Year of Operation including Outage* phase are to demonstrate a defined scope of the phase and to assess the scope for "3C" according to Table 4-9.

4.5.3 Phase results and stakeholder agreements

Phase output:

- Fifth Safety Demonstration Report (SDR 5) including a confirmed and updated Safety Demonstration Case definition. The SDR 5 may be a simplified version, confirming the SDR 4 with supplements and complements reporting on the actual NPP operation and outage.
- Complements to Safety Analysis Report (KSAR), when applicable

Stakeholder activities:

- The activities of each stakeholder during the *Product at One Year of Operation including Outage* phase is given in Table 4-10.

Table 4-10 Presents the typical activities related to Safety Demonstration and expected to take place in the Product at One Year of Operation incl. Outage phase. The stakeholders given in the table might be represented by "sub-stakeholders" and additional stakeholders might be suitable to appoint in a specific project.

	Qualification of Product at One year of Operation including Outage
Supplier*	- Provide supplier scope SDR input to NPP project
NPP project*	- Produce final SDR - Ensure that the SDR is reviewed and approved
Licensee	- Follow-up and report on first period of operation and outage - Communicate with regulator and request permission to end project "test period"
Regulator	- Permit ending of project "test period"

* It need to be noted that at One Year of Operation the NPP project might be finished and not present anymore as a stakeholder. Similarly, the Supplier might not be a disposable stakeholder as the project contract might have been terminated.

Phase result acceptance:

- All stakeholders to accept the contents of the SDR 5, i.e. confirmed design Qualification as operated in plant and processes, tools and documentation in place, satisfyingly, functional and applied in the NPP organization for safe and correct operation, maintenance and modernizations in the plant.
- Acceptable to end Supplier and NPP Projects.
- Complement to SAR (KSAR) is valid.
- Regulator can end project test phase inspection period and close the "act".

5 Safety Subject Areas – Contents of Safety Demonstration

This section addresses the contents of Safety Demonstration, by addressing the proposed standard SSAs one by one. Each area is defined by purpose and scope. Advice on a strategy for how to perform the demonstration is discussed with examples and possible reference to relevant standards or guidelines that can provide further guidance. In section 5.10 a number of optional areas are discussed. In Appendix C *Guiding questions for Safety Demonstration in respective Safety Subject Areas* are provided.

The set of SSAs to select for a specific Safety Demonstration must always be decided case by case, depending on the scope and challenges faced in each individual project. The set of SSAs are first defined assessed for 3C and agreed in the *Safety Demonstration Planning* phase and documented in the Safety Demonstration Plan. Along the Safety Demonstration life cycle the 3C is reassessed and the set of SSA and their scope, purpose and demonstration strategies may very well be adjusted to remain judged as 3C. The assessment of the Safety Demonstration Case as 3C and suitable to demonstrate fulfilment of the safety objectives is an important part of the Safety Demonstration – the argument for conclusions on safety is the combination of that the safety demonstration case is 3C fulfilled and that the safety demonstration case definition itself is 3C.

5.1 SSA 1 - PROJECT SCOPE

5.1.1 Purpose and scope

The purpose of the *Project Scope* SSA is to assure that the total scope of the project has been defined with boundaries, including the impact of the project on the existing NPP. The area assures that definitions are captured completely and correctly and implemented in valid project documents. The purpose with identifying and assessing the project scope in this area is also that it will be used as reference for completeness evaluation in the other areas. It also gives basis for assessment of completeness of the "safety scope" out of the total project scope.

The scope of the *Project Scope* SSA is to identify and assess the scope including:

- Product scope (functional, physical and geographical)
- Technical documentation scope (Technical Specifications, maintenance, operation)
- Instructing documentation scope (instructions, quality system, management system)
- Competence scope
- Safety Demonstration Scope (optional)

The Safety Demonstration Scope can be added when an explicit possibility to confirm or challenge the selection of Safety Demonstration scope from the whole scope is wanted.

5.1.2 Strategy

Identify the defined scope of functional, physical and geographical plant changes (this is the "product scope"), the scope of technical Plant Documentation, the scope of instructing Plant Documentation including possible management system documentation and the scope of competence including deliverables and training. Include any other scope that the project has to deliver. Include clear demarcations of what is not within the scope. Assess the identified scopes for "3C".

Example:

The project scope definitions should be possible to identify within the project documentation (e.g. Project plan) and assessments are performed by reviews.

Further guidance can be found in e.g.:

- IEC 81346 [11], gives advice on how to address functional, physical and geographical views.

5.2 SSA 2 - SAFETY CLASSIFICATION AND CATEGORIZATION

5.2.1 Purpose and scope

The purpose of the *Safety Classification and Categorization* SSA is to describe and assess the principles for and application of Safety Classification in the project. The principles defined in this area are, in addition to being important themselves, applied on the *Project Scope* as defined in section 5.1 to govern the detail and amount of explicit Safety Demonstration to be proportional to the importance to safety (graded approach) as described further in Figure 2-5.

The scope of the *Safety Classification and Categorization* SSA is to identify and assess the principles and application of:

- Functional safety categorization with corresponding structures, systems and components (SSC) classification for the product.
- Safety classification for graded approach applied to technical documentation.
- Safety classification for graded approach applied to instructing documentation.
- Safety classification for graded approach applied to project and NPP organization and competence assurance.

5.2.2 Strategy

Identify the safety classification and categorization principles that will be used in the project and assess for "3C" referring to the *Project Scope* and evaluate the feasibility to use the identified principles as a basis for a "graded approach" (adapting the detail of demonstration to be proportional to the safety importance) in the safety demonstration.

Example:

For the product design the safety categorization principles defined for functions with classification of associated systems and equipment. For instructing or process

documentation the safety classification principles often aren't that clear, but one example is the principles for when to safety review operations and maintenance instructions, that can be used in support of the purpose of this area.

Further guidance can be found in e.g.:

- IEC 61226 [12] international standard defining safety categorization, presenting category A, B and C and advice on assignment of technical requirements to categories for I&C functions in NPP.
- SSM 2016:25 [2] give detailed advice for system classes, function categories and graded requirements for software
- IEC 62138 [13] international standard describing grading principles and requirements for software of I&C systems performing category B and C functions
- IAEA SSG-39 [14] guidelines for safety classification of systems
- There are also comparable US standards applicable, e.g. IEEE-279, -308 and -603 [17].

5.3 SSA 3 - REQUIREMENTS

For modernization projects one important prerequisite for the *Requirements* SSA is that a plant safety analysis is in place and can be used as a basis for building the project concept and to formulate I&C requirements in relation to [2].

5.3.1 Purpose and Scope

The purpose of the *Requirements* SSA is to identify and assess the actually identified requirements that the project scope needs to be built upon. Requirement management and other processes or methodology aspects are assessed in the QA and Plans including Organization and Competence SSA. Additionally, the area should identify all associated assumptions, pre-conditions and design basis. Requirements defined should cover the complete *Project Scope* as identified above. Several other areas will demonstrate to what degree the requirements specified here have been implemented completely and correctly in each Safety Demonstration phase.

The scope of the *Requirements* SSA is to identify and assess all high-level requirements, assumptions and preconditions relevant for the project scope. That includes not only product design requirements, but also requirements on design- and work processes (QA) and requirements on staffing and competence. To assess the traceability from high-level requirements to derived detailed requirements as the design process progresses along the life cycle, is also within the scope of this area. One can however decide and agree during the *Safety Demonstration Planning* phase when defining the Safety Demonstration Case, to handle the requirement breakdown and its traceability in the *Product Design* SSA

5.3.2 Strategy

Identify and assess the requirements for "3C". In the early concept stage it is the high-level requirements and for I&C systems their traceability to the plant level

requirements that are expected. In later design phases the traceable requirements break-down (from high-level to functional and system design and further to detailed design, if not decided to be handled in the *Product Design* SSA). Typical activities to refer to in the assessment are reviews performed.

Example:

Typical requirements are technical design requirements, e.g. the I&C system requirements; functional-, system- and software requirements. For more specifics on typical important areas for digital I&C system requirements, see section 6. Assumptions made and prerequisites or design basis for a requirement should be tied to the requirement – this provides traceability to the plant safety analyses and design basis. There are numerous regulations and standards that formulate requirements for digital I&C systems, and some will be identified in section 6, further guidance can be found in e.g.:

- IEEE 603 [17] with supplement IEEE 7-4.3.2 [18], standard stating minimum functional and design criteria for the power, and I&C portions of nuclear power generating station safety systems.
- IAEA Specific Safety Requirements, SSR-2/1 [21] establishes requirements applicable to the design of NPP and elaborates on the safety objective and concepts that provide the basis for deriving the safety requirements.

5.4 SSA 4 - PRODUCT DESIGN

5.4.1 Purpose and scope

The purpose of the *Product Design* SSA is to identify the present product design version and assess its completeness to a level of detail relevant for each phase of the Safety Demonstration.

The scope of the *Product Design* SSA is to identify a relevant product design and to assess the design for completeness against the project scope and design requirements. It also belongs to the scope to identify possible limitations in whether the total set of high-level requirements have been implemented yet or not.

5.4.2 Strategy

Identify the design version that is the specification of the product design relevant for the present phase in the Safety Demonstration and assess for "3C". Assessment for completeness is performed by comparing to the *Project Scope* and to the implementation of *Requirements* specified and imposed. Performed design reviews support this assessment.

Further assessment of the correctness of the product design with reference to V&V records is handled in the *Product Design Qualification Status* SSA as further described in section 5.5 below.

Example

An example of a "deviation" can be in a project with both safety improvements and a power uprate, where at a certain phase the present design identified to cover only the safety enhancement requirements and not the power uprate requirements. By clearly stating this here, it is possible to avoid looking for V&V records and discussing obvious non-compliance in the *Product Design Qualification Status* area for the not yet implemented requirements.

Further guidance can be found in e.g.:

- 2016:25 part 2 [2] give detailed advice on computer system architecture and design and on software requirements, architecture and design through the life cycle phases.
- IEC 81346 [11], gives advice on how to address functional, physical and geographical views, which can support clear description of the product.
- IAEA Specific Safety Requirements, SSR-2/1 [21] establishes requirements applicable to the design of NPP and elaborates on the safety objective and concepts that provide the basis for deriving the safety requirements.

5.4.3 Separate handling of the I&C Architecture

Definitions of I&C Architecture
IAEA SSG-39 Design of Instrumentation and Control Systems for NPP [14] "Organizational structure of the instrumentation and control systems of the plant that are important to safety".

EPRI Technical Report Principles and Approaches for Developing Overall Instrumentation and Control Architectures that Support Acceptance in Multiple International Regulatory Environments [25]: "The organizational structure of the I&C systems, including the main functions performed by the I&C systems, the classification and boundaries of each system, the interconnection and independence between systems, the priority and voting between concurrently acting signals and the human-system interface (HSI) (Adapted from IEC 61513)."

To define and handle the overall I&C architecture as a separate area in the safety demonstration is advantageous. This can be done as part of SSA 4 and 5 or by defining separate SSAs. The I&C Architecture including the identification of all applicable criteria and requirements can be defined and assessed early in the Basic Design phase or already in the Conceptual Design phase. The Architecture definition can also be verified early through engineering analysis, long before finalizing the I&C Systems design. The overall Architecture perspective should be kept all the way through the project and the final validation tests are performed on the I&C Architecture level providing the last evidence to the Product Qualification and suitability demonstration in SSA 5. In smaller modification projects the identification of the projects possible impact to Plant Design Basis and the I&C Architecture is also advantageous to minimize risks to discover unexpected requirements, new failure modes or risks for CCF late in the design process and to facilitate early verification of the planned design solution.

The I&C Architecture design might be impacted by requirements and guidelines in several categories including Defense in Depth, simplicity, functional architecture, classification, single failure and redundancy, independence, data communication, diversity and common cause failure, HFE, shared systems between reactor units, overall I&C design, operating and maintenance aspects, testing and calibration aspects, reliability and IT security. It is also impacted by constraints from other design and planning activities in the project e.g. safety analysis, PRA/PSA, process design, long term operation aspects, economic analysis etc. [25]. I&C Architecture is on Plant design level which means that it needs to be performed together with Plant design i.e. often quite long before I&C systems design.

5.5 SSA 5 - PRODUCT DESIGN QUALIFICATION STATUS

5.5.1 Purpose and scope

The purpose of the *Product Design Qualification Status* SSA is to demonstrate that the product design can be qualified to fulfill the requirements completely and correctly. The area focuses on qualifying the product with reference to V&V records such as reviews, inspections, analyses and tests. The qualification can concern the integrated system in plant as well as the separate product "platform". In many cases it is relevant to assign a specific area for "Base Product Qualification", e.g. the general I&C platform, Commercial Off-The-Shelf (COTS) products and such. The Qualification of the "platforms" is a prerequisite for Qualification of the Plant specific integrated system design.

The scope of the *Product Design Qualification Status* SSA is to conclude and assess the design qualification with supporting V&V records.

5.5.2 Strategy

Conclude and argue the assessment of *Product Design Qualification* status, i.e. conclude on the status of how well the present product design as identified in the *Product Design* SSA has been "3C" designed by imposing a "3C" set of requirements (identified in the *Requirements* SSA) into a "3C" design process manned by resources with suitable competence (both identified in the *QA and Plans including Organization and Competence Assurance* SSA). Furthermore, conclude and argue compliance to the requirements with reference to V&V records. The level of detail in arguing the conclusion should be proportional to the safety importance.

Example:

Useful verifications for this area are relevant V&V records, e.g.: requirement specification review records, installation inspection records, analysis reports, e.g. single failure analysis like response time analysis with complementing tests etc.

Further guidance can be found in e.g.:

- IEC 60880 [15] standard giving advice on software verification and software aspects on system validation.

- IEC 61513 [8] standard giving advice and specifying requirements for system validation and system qualification for I&C systems important to safety
- SSM 2016:25, part 2 [2] giving detailed advice on verification and validation through the life cycle phases

5.6 SSA 6 - PLANT DOCUMENTATION

5.6.1 Purpose and scope

The purpose of the *Plant Documentation* SSAs is to assess that the Plant Documentation produced by the project is complete, correct and consistent.

The scope of the *Plant Documentation* SSA is to assess that new documentation is available where needed, that it correctly represents the present design version and that old documentation is up to date or removed in the resulting Plant Documentation.

5.6.2 Strategy

In early phases identify how the project impact on present Plant Documentation including technical and instructing documentation. Define what will remain unchanged, what is new and what needs to be revised or deleted. Along the life cycle of the Safety Demonstration the documentation develops to correctly represent the present design version and qualification status "3C". *Completeness* is assessed with reference to the *Project Scope* SSA and to the existing Plant Documentation. *Correctness* and *consistency* is assessed with reference to design and documentation reviews (assessed in the *Product Design* SSA) that confirm proper requirement fulfillment and consistency of documentation with regard to the actual design. The level of detail should be proportional to the safety importance.

Example

Examples of documents included in Plant Documentations are PSAR/SAR, Technical Specifications and their review records. Other examples are system descriptions, design descriptions and specifications, drawings, V&V records, QA records etc. Lists of Plant Documentation with their corresponding status and review records are one way this area could be demonstrated.

Further guidance can be found in e.g.:

- SSMFS 2008:1 [3] specifying the regulations for how to perform safety reporting and what to include in the reports to the regulator.

5.7 SSA 7 - QA AND PLANS INCLUDING ORGANIZATION AND COMPETENCE ASSURANCE

5.7.1 Purpose and scope

The purpose of the *QA and Plans including Organization and Competence Assurance* SSAs is to demonstrate that the quality assurance program provides the framework

and guidance as needed for implementing and executing the project with its defined scope and life cycle and that necessary traceability to records will be provided. The purpose is also to identify and assess that the plant- and possible supplier organization with necessary competence management are assured for the project. This area focuses on demonstrating that the necessary processes are available in the project while the *QA and Plans Compliance including Organization and Competence Assessment* SSA deals separately with the demonstration of the actual *compliance* to the defined processes and the status of the actual organization. Furthermore, this area handles processes for competence and organization during the project while section 5.9 handles competences and organization for operation and maintenance *after* the project.

The scope of the *QA and Plans including Organization and Competence Assurance* SSA is to identify and assess the quality assurance program including Requirements Management (RM) with Configuration Management (CM) and Verification & Validation (V&V) strategies and plans. The scope is also to assess the organization governance focusing on safety culture assurance, the organization with clear delineation of responsibilities as well as competence and staffing assurance methods to apply in the project.

5.7.2 Strategy

Identify the QA system including design control processes as well as project plans and assess for completeness referring to the *Project Scope* and to full life cycle of the project. Assess with detail proportional to safety importance, the Design control processes and their fulfillment of safety requirements and ability to govern the design, changes and V&V to produce traceability from high-level requirements to implemented product with relevant V&V records, all under proper configuration management. This includes assessment of V&V coverage in V&V plans. In case needs and requirements are not met by the existing QA processes, assess the consequences and the strategy for how the required levels will be reached. Furthermore, evaluate the Safety culture, the organization as well as achieved competence and staffing.

Further guidance can be found in e.g.:

- IEC 60880 [15] standard giving advice on software design- and verification and validation process.
- IAEA General Safety Requirements, GSR Part 2 [19] presents requirements on a management system.
- IAEA General Safety Guide, GS-G-3.1 [23] gives guidance for how to implement management system and processes.
- IAEA Specific Safety Requirements, SSR-2/2 [22] establishes requirements for the safe commissioning and operation of NPP.
- IEC 61508 [16] standard stating general requirements for management of functional safety and the overall safety life cycle for programmable electronic systems (PES).
- IEC 61513 [8] applies IEC 61508 to nuclear power and gives advice for design process and system validation and system qualification for I&C systems important to safety

- IEEE 7-4.3.2 [18] standard criteria for I&C of nuclear power generating station safety systems.
- SSM 2016:25 [2] part 1 giving e.g. organizational requirements and part 2 giving detailed advice on change control and configuration management.
- The CEMSIS project [7] with its subtasks provides further guidance addressing requirements specification and -management.

5.8 SSA 8 - QA AND PLANS COMPLIANCE INCLUDING ORGANIZATION AND COMPETENCE ASSESSMENT

5.8.1 Purpose and scope

The purpose of the *QA and Plans Compliance including Organization and Competence Assessment* SSA is to demonstrate compliance to the quality assurance program and associated processes and plans as well as to conclude sufficient safety culture, clear organization with sufficient competence and staffing in place. This area focuses on the demonstration of the actual compliance to the defined processes and the status of the actual organization, while the *QA and Plans including Organization and Competence Assurance* area described in section 5.7 serves to demonstrate that the necessary processes are available in the project. Compliance to processes for competence assurance and organization in the operating and maintaining organization *after* the project is handled separately in section 5.9.

The scope of the *QA and Plans Compliance including Organization and Competence Assessment* SSA is to assess that QA processes have been properly followed along the life cycle of the project. within the scope is also to identify deviations and to provide justifications for these deviations. The level of detail should be in proportion to the safety importance, i.e. most detail in descriptions and assessments of QA and Design control processes for the system's important safety. Furthermore, the safety culture and clear responsibilities of the actual organization as well as the competence and staffing should be assessed. Strategy

5.8.2 Strategy

Assess compliance to the QA System and plans identified in the *QA and Plans including Organization and Competence Assurance* SSA in section 5.7, down to the present stage of the Project. Typically, internal and external audits or self-assessments support this assessment for overall QA. In proportion to safety importance also perform follow-up to check that the design control processes and plans are followed to produce the relevant documents down to the present phase, e.g. that the planned V&V activities really were performed and documented. Any deviations should be assessed for consequences.

Example:

Examples of verifications in this area are summary of audits performed and possible corrective actions status. Another example is ticking off that planned V&V actions of the phase have been performed as planned.

Further guidance can be found in e.g.:

- No further references given. This area is follow-up on compliance to what is assessed in the *QA and Plans including Organization and Competence Assurance* area, so any references there giving advice on how to audit and perform follow-up are relevant.

5.9 SSA 9 - NPP OPERATION, MAINTENANCE AND MODIFICATION

5.9.1 Purpose and scope

The purpose of the *NPP Operation, Maintenance and Modification* SSA is to demonstrate that the receiving (operating) organization, including the Management/QA system, is in place, is capable and have the proper documentation, support and tools to safely operate, maintain and make changes to the NPP with the safety and quality required. This area focuses on the demonstration of the sufficient competences and organization for operating and maintaining the NPP after the project while the competences and organization required *during* the project is handled in section 5.7 and assessed in section 5.8.

The scope of the area is to assess that plant documentation, training and tools provided to support the plant operation, maintenance and modification organization and processes. Furthermore, the organization should be assessed with regards to safety culture, organization and delineation of responsibilities, competence and staffing.

5.9.2 Strategy

Assess to what degree the organization with required competence, processes, and tools to safely operate, maintain and modify the plant are completely and correctly in place. Assess this by addressing the organizations future tasks of operation, maintenance and modification with regards to:

- Organization (safety culture, roles and responsibilities, competence and staffing)
- Working processes and instructions (Instructing Documentation)
- Plant technical documentation
- Necessary tools

Example:

Examples of verifications for the organization are e.g. organizational assessments with regards to safety culture, requirements on competence and matching assessments, manning analyses etc. With regards to processes and instructions, typically review records are in support of sufficiency. That the Plant Documentation is in place and sufficient can be concluded with reference to the Plant Documentation area demonstration. That tools necessary are in place is a mere assessment.

Further guidance can be found in e.g.:

- SSM 2016:25 [2] part 1 giving e.g. organizational requirements.

- IAEA Specific Safety Requirements, SSR-2/2 [22] establishes requirements for the safe commissioning and operation of NPP.

5.10 OPTIONAL AREAS

This section contains a collection of areas that have been identified as important in different contexts. They are presented here as suggestions worth considering for any Safety Demonstration Case, but only if there is a specific need. There may also be additional areas that could defined and applied, depending on the specific scope of a project.

These areas might be integrated parts of the standard SSA or they may be defined as a separate SSA depending on the priority assumed for the specific area in the specific Safety Demonstration Case.

5.10.1 Base Product qualification

If a digital I&C system is being introduced it can be valuable to make a separate area to handle the qualification of the digital I&C system platform (including firmware, operating system, additional options in SW etc) and I&C equipment (compare to COTS, commercial off the shelf software). Reasons to separate can be to more easily delineate responsibilities for Base Product and application qualification respectively (the latter requires that the Base Product is qualified as a prerequisite).

5.10.2 Integration in plant

If a project spans over several years so that other changes may be performed in parallel with the present project, it may be relevant to put special focus on the actual integration, by defining it as a separate area. If this area is selected, procedures for operability verification ("DKV") can be included here, otherwise they belong to the *Plant Documentation* area (Instructing Documents) and to *NPP Operation, Maintenance and Modification*s area for ultimate conclusion.

5.10.3 Human Factor Engineering (HFE) and Human System Interface (HSI)

HFE should be viewed as an integrated aspect of the design, but it can in some cases be relevant to have a separate area to address the HFE aspects, with special emphasis and using the terminology often used in that area.

If main control room changes, or emergency or remote-control rooms and equivalent, are included and the *Project Scope* contains introduction of significant technology changes, it could also be relevant to address Human System Interface (HSI) and the control room design qualification specifically in this area.

Sometimes having a specific area, or at least separate handling with separate plans, is requested by the regulator. It shall not however be acceptable to handle these issues completely separate, since it is an essential integrated part of the complete system qualification. Further to this topic see also specific challenge area discussion in section 6.

5.10.4 Regulations, codes, guidelines and standards

To have a separate area for this sub part of the total set of requirements, could be considered e.g. in organizations or projects where there is a specific focus on the handling of the requirements that originate from regulations, codes, standards and guidelines. Otherwise this is not a recommended area as all requirements of a project should rather be integrated in the same *Requirements* area. Relating to the regulations, codes, standards and guidelines as a mean to argue the requirements completeness and correctness is one important aspect but only one of many.

6 Specific challenge areas for digital I&C

This section aims to identify and briefly discuss aspects of digital or computer based I&C that experience has shown carry specific challenges. The aspects can be used when defining the Safety Subject Areas, their purpose, scope and formulating strategies as discussed in section 5, to assist in defining a good coverage and level of detail in the safety demonstration. They should of course also be considered when high-level requirements are specified based on the plant design basis and safety analysis.

A key to success for any I&C containing NPP project is thus to address these challenge areas already in the Planning and Conceptual Design phases, to minimize risks for significant re-design efforts in later phases with great cost and time impact. They also must engage and get commitment from the whole project and may not be left the sole responsibility of the ones responsible for the Safety Demonstration reports.

Since many of the challenges are interrelated, the subsections in this section may very well overlap somewhat, since the objective of the section is to serve as a check list or guideline in support of completeness of coverage.

General good advice and further references are found in SSM 2016:25 [2]. The list in this chapter has been compared and updated with input from IAEA NP-T-1.13 [20].

6.1 DEFENSE-IN-DEPTH, DIVERSITY AND COMMON CAUSE FAILURE

IAEA NP-T-1.13 [20] refers defense-in-depth to a structure consisting of levels, where should one level fail the subsequent level enters. Digital I&C interacts with every system in a NPP, and may have devices with multiple functions. A failure in I&C or device can affect several functions and also several levels of defense-in-depth. There may be significant interrelation or dependencies between the overall NPP- and the I&C diversity and defense-in-depth, which must be carefully considered as early as possible. It is necessary to determine how the concepts of diversity, redundancy, physical separation and functional independence have to be applied to achieve the necessary safety and reliability.

Decisions taken as to the devices used at the plant level (e.g. sensors and actuators) will also require careful consideration since modern instrumentation is increasingly utilizing software components which is also discussed in section 6.14 handling Smart Devices.

NRC Regulatory Guide 1.152 [24] says: “The design techniques of functional diversity, design diversity, diversity in operation, and diversity within the four echelons of defense in depth (provided by the reactor protection, engineered safety features actuation, control, and monitoring instrumentation and control systems) can be applied as defense against common-cause failures.”

Software common cause failure (CCF) and software design diversity are handled in SSM 2016:25 [2] which also discusses further references. It is reasonably so that

regardless of efforts to avoid the possibility for or unacceptable consequences of software or computer CCF, diversification will most probably be required.

6.2 DETERMINISTIC BEHAVIOR

Cyclic and deterministic behavior is part of the Base Product qualification to be demonstrated. The Base Product qualification may very well put restrictions on the application to remain valid (e.g. limits on allowable processor load). Furthermore, absolute deterministic behavior can turn out difficult to prove, making e.g. time response tests still necessary to confirm proper response.

6.3 INDEPENDENCE – FUNCTIONAL AND PHYSICAL SEPARATION

Assuring required independence within a digital I&C system application in a NPP requires assuring e.g.:

- Independence between divisions of the I&C system.
- Independence between power trains ("subs") as well as HVAC and similar support systems to the I&C System, to the extent possible.
- Physical separation within a division between lower and higher safety classes and categories.
- Functional separation meaning that no unacceptable normal control and safety functional interaction exists

Communication separation is also important to include in the above items.

SSM 2016:25 [2] discuss independence as an entity of the computer system architecture defined as:

> *"The hardware components (processors, memories, I/O devices) of the computer based system, their interconnections, physical separation and electrical isolation, the communication systems, and the mapping of the software functions on these components."*

It also says that:

> *"Total independence seldom exists; it is therefore extremely hard (usually impossible) to demonstrate, and so should not be required."*

Dependability is another common term used when discussing these issues, e.g. in several IEC standards.

6.4 PERFORMANCE – TIMING AND ACCURACY

Requirements on time response can be a challenge for computer-based systems. Where the old analog systems often were fast, the cycle times in computer-based systems can give quite slow results in comparison, certainly if the system architecture is unfortunate with regards to having to "stack" several cycle times after each other. The latter can be the situation, e.g. with sampling I/O and the function divided in parts to several processors in series. Changed timing can also

impact sequencing. These aspects are important to take into account early in the design cycle. See also section 6.2 discussing deterministic behavior.

Depending on measurement range and the bit resolution available, accuracy can also become a challenge. The "set point study" may thus very well be another thing to address and update early, to avoid later shortcomings and challenges hard to resolve. The accuracy may also challenge maintenance procedures (e.g. calibration checks and adjustments) as well as methods and requirements on tools.

6.5 FAILURE TOLERANCE AND FUNCTIONAL RELIABILITY

Requirements within this aspect influence the level of redundancy specified for certain systems and can influence the technology selected for I&C systems. This involves e.g. to handle:

- N+2 criteria i.e. a safety function to be able to carry out their functions even though an individual component in any system would fail to operate and, additionally, any component affecting the safety function would be out of operation simultaneously due to repairs or maintenance.
- N+1 criteria i.e. a safety function to remain operable even in the case of a single failure.

6.6 FAILURE DETECTION BY SELF-DIAGNOSTIC FUNCTIONS AND PERIODIC TESTS

One of the advantages with modern computer based I&C systems is the self-supervision and diagnostics available. The extent to use this and how to be able to credit in e.g. single failure analysis for failure detectability needs to be carefully considered. Also, the relation to periodic testing scope and intervals comes to mind here. Finding the correct mix of self-supervision and periodic tests is the key, and significant reductions in periodic testing can be one tempting incentive for I&C modernization.

Another challenge that needs to be considered is that online troubleshooting may require connecting tools, which are normally not allowed to have connected to e.g. safety systems during operation, restricting the amount of troubleshooting being possible during operation of the NPP.

6.7 FAIL-SAFE DESIGN, HANDLING OF NEW FAILURE MODES AND INITIALIZATION

To maintain a fail-safe design when applying computer-based systems, requires the whole chain of possible states within the software and hardware to be correctly specified and implemented. New failure modes and dependencies may also appear in the logics when introducing digital I&C, which must be taken into account. Fail-safe design of computer-based systems important to safety will inevitably use on-board self-diagnostics to ensure that failures are detected, and as a result, will use appropriate default states attained in the system. Also, for initialization, where initial values may have to be defined not only for the outputs, but also "inside" the

function to maintain correct functionality at start-up and for the first number of computing cycles, needs to be considered.

6.8 IT SECURITY

As nuclear facilities modernize digital I&C systems, the vulnerability of computer systems comes to light. Attention to computer security has intensified and regulators have issued new regulations which e.g. cover computers used in safety and safety related systems, which should be protected from possible cyber-attacks, and also computers used to control and monitor the plant.

The IT security challenge needs to involve assurance of:

- Only authorized users can access assigned functions by means of user accounts, password management and administrative functions.
- Intrusion attempts and unauthorized or unintentional change of information on both development and target systems are detected and prevented.
- Only intended and sanctioned software changes are installed on the target system.
- Prevent malicious software (i.e. virus) from being transferred to the I&C system and its tools.
- Backup procedures available to be able to restore system or part of system to a specific configuration.

IT security is the more technical aspect of the wider challenge of information security.

SSM 2016:25 [2] says: "The objective of information and system security is to guarantee and preserve the dependability safety of computer-based systems by preventing security incidents or by minimizing their impacts. In this context, security seeks to prevent unauthorized accesses to information, software and data in order to ensure that three attributes are met, namely:

- The prevention of disclosures that could be used to perform mischievous, malicious or misguided acts which could lead to an accident or an unsafe situation (confidentiality),
- The prevention of unauthorized modifications (integrity),
- The prevention of unauthorized withholding of information, data or resources that could compromise the delivery of the required safety function at the time when it is needed (availability)."

The same reference also provides regulators common positions that can be a good starting point for what is required to handle, in complement or with other words to what is written above.

Discussion on these important matters is done also in several other references, e.g. NRC Regulatory Guide 1.152 [24]. See also platform and equipment suitability and qualification in section 6.10.

6.9 VERIFICATION & VALIDATION STRATEGY FOR PROGRAMMABLE ELECTRONICS SYSTEMS

One of the consequences of computer or software-based systems are that they are practically "never 100% testable". This fact puts requirements to the whole design and V&V process, beginning already in the early definitions phases. To minimize risks related to software CCF or latent failures etc., the V&V strategy must include the early specifications phases and the traceability to NPP design basis. Not only *correctness* of the specified but also *completeness* and *consistency* must be evaluated and concluded in each design phase.

A valuable or necessary approach is to develop a strategy for complete coverage of V&V on I&C systems and I&C architecture as well as on plant level. The strategy should strive to perform as complete qualification as possible already in the design phase, and to be followed up and validated by complete coverage of tests in the validation qualification phases.

Planning and performing the actual tests are of course important to have full coverage of the functions specified, but to test under all possible combinations of inputs and states is not possible. Therefore, the coverage of testing of parts and integrated systems in test bays, full factory test runs (FAT) and the installation and commissioning testing (SAT) is important to plan and assess early. As part of software development an important element of V&V is independent review, especially for use in safety systems or platforms.

6.10 SUITABILITY AND QUALIFICATION OF PLATFORM AND EQUIPMENT

Modern updates of standards like IEEE 7-4.3.2 [18], Regulatory Guide 1.152 [24], IEC 60880 [15] etc. identify the requirements and challenges of applying computer-based systems in safety important functions and systems.

The suitability demonstration and qualification must not only address the digital I&C system itself but also include tools and methods. When considering so called Smart Devices they must also be shown suitable and qualified for the application considered.

6.11 FORMAL METHODS OF SOFTWARE DEVELOPMENT

Formal methods of software development, that is methods that use mathematics and logics for defining, specifying and verifying systems, provide precise definitions of requirements as well as increasing safety for critical systems. The mathematical nature of the formal methods may be hard to grasp and should therefore be chosen wisely so that it is understandable by entire technical staff, see IAEA NP-T-1.13 [20].

6.12 SYSTEM CLASSES, FUNCTION CATEGORIES AND GRADED REQUIREMENTS FOR SOFTWARE

To ensure that proper attention is paid to the design, assessment, operation and maintenance of the systems important to safety, all systems, components and

software at a nuclear facility should be assigned to different safety classes. The safety classification approaches used in nuclear power plants are based on the safety philosophy and the plant design basis. All structures, systems and components (SSCs), including software for digital I&C systems, are classified based on their function and significance with regards to safety. Graded requirements may be advantageously used in order to balance the software, as well as the whole I&C qualification effort. For further discussion and advice, see SSM 2016:25 [2]

6.13 HUMAN FACTORS ENGINEERING (HFE) AND HUMAN SYSTEM INTERFACE (HIS)

Usually the HFE/HSI efforts focus on operations and the main control room, but also emergency control rooms and other maneuver locations as well as maintenance aspects in e.g. relay rooms are important. There are also important HFE/HSI aspects with regards to installation, dismantling, software loading etc.

Addressing HFE/HSI aspects in early stages gives possibilities to make design decisions significantly reducing later problems e.g. by deciding to maintain panels "as is" instead of introducing screen based controls.

6.14 SMART DEVICES AND PROGRAMMABLE ELECTRONICS

According to IAEA NP-T-1.13 [20], Smart Devices are devices such as sensors and valve actuators that contain computer-based technologies and are configurable to make them suitable for a variety of applications. Smart Devices are displacing traditional analogue sensors and actuators in many industrial applications as they can offer a significant number of benefits such as improved stability, self-diagnostics and additional features. This displacement is likely to result in some traditional analogue devices becoming obsolete, and not being available for use in the nuclear industry. Smart Devices have been considered difficult to qualify in the nuclear industry owing to detailed design information not being readily available as a result of proprietary considerations around the embedded functions.

The decision to apply such devices in safety important applications, must be preceded by both suitability evaluation of the device itself (compare with section 6.10 about platform qualification) and the possible impact from its integration in the NPP application. The latter may challenge defense-in-depth, diversity and vulnerability to common cause or common mode failures of the NPP and must thus be carefully analyzed.

The increasing integration of programmable electronics into conventional equipment (e.g. FPGA, HDL, Smart devices etc) leads to a need to also evaluate safety verification and demonstration needs for "simple" process equipment (e.g. pumps, lifting devices, valves).

SSM 2016:25 [2], further discusses the application of so called Smart Devices .

6.15 PRIORITIZATION

The basic principles of priority between different I&C functions which control the same process system actuator, are important to assure being adequately defined and implemented. For functions and actuators necessary to support the plant safety analyses, process and safety engineering define the required priority in the I&C functional requirements. For functions/actuators where priority is not defined in the I&C functional requirements, the requirements are defined within architecture design. This challenge area can also be important to coordinate with other, in particular "Fail-safe design, handling of possible new failure modes and initialization" in section 6.7 and "Independence – functional and physical separation" in section 6.3.

6.16 DIGITAL COMMUNICATIONS

The use of computers enables the possibility to transfer large amount of digital information, the transfer can occur between safety related systems and non-safety systems or between different safety classes (for safety systems and classes etc. see section 6.12). The use of digital communication raises awareness to issues such as independence for inter-channel communication, contamination of higher safety classes by lower safety classes systems and loss of separation between safety and non-safety systems. The interconnecting structure in a computer based system, i.e. a communication network rather than a point to point connection, enables new ways for failures to propagate in the system. To avoid these issues, it is essential to separate systems, additional guidance can be found in IAEA NP-T-1.13 [20].

6.17 USE OF WIRELESS TECHNOLOGY

The use of Ethernet in NPP has led to usage of wireless technology connected with Wi-Fi, which enables both enhanced communication due to availability of data and also reduced cost due to avoidance of costly industrial wiring. However, the use of wireless technology arises additional challenges in security. Electromagnetic interference (EMI) from equipment in the plant can cause interferences with wireless signals, and the devices themselves are also potential sources of EMI.

6.18 MANAGEMENT OF THE FUNCTIONAL REQUIREMENTS SPECIFICATION

The purpose of requirement management is to establish a common understanding between the customers and vendors, which should be the basis for planning and managing the project. Ambiguous requirements or changes in the middle of a development cycle can invalidate the design and result in expensive rework, incorrect documentation etc. Vague requirement management may allow faster decisions and more flexibility but can lead to negative consequences. A too formal requirement management can lead to bottlenecks and seem to burdensome. The requirement management formalism should be determined to ensure success in the project. Good system requirements are; attainable; testable; verifiable; traceable.

6.19 DEVELOPMENT OF AND ADHERENCE TO CONFIGURATION MANAGEMENT

Configuration management provides means to control the design, test and installation status of a Product. Configuration management should be applied to all levels in the project, from the system architecture level to software/hardware configuration level. In addition to this, also address tools and other support software. System specifications and requirements should be covered by the configuration management. A well-defined system configuration ensures *consistency* and traceability throughout the development process and during the complete life cycle of the Plant.

6.20 ENVIRONMENTAL QUALIFICATION OF SAFETY SYSTEM PLATFORMS

Environmental, seismic and electromagnetic interference/radiofrequency compatibility (EMI/RFI) are addressed as stressors for safety systems. Digital equipment is becoming more introduced into NPPs, making the plant more vulnerable for EMI/RFI effects. Therefore, attention to electromagnetic compatibility is a must and should be considered as a part of the design and qualification of I&C equipment.

Environmental and seismic qualification testing is costly, and the market for nuclear qualified equipment is small. Consequently, environmentally qualified equipment is expensive, and many I&C vendors consider the market too small to warrant the investment that maintaining a nuclear qualified product line requires. This needs to be taken into account and possible workarounds to be found to assure supply of spare parts during the life cycle of the Plant.

6.21 RELIABILITY (TAKING CREDIT FOR DIGITAL SYSTEMS IN PROBABILISTIC RISK ASSESSMENT)

There lies a challenge in providing clear guidance on how digital I&C systems can be included in probabilistic risk assessment (PRA). PRA normally models random failure modes, but since digital I&C use software, systematic failure modes are dominating. A deterministic approach, see section 6.2 about deterministic behaviour, is recommended by most international standards, see e.g. IAEA NP-T-1.13 [20], for the safety demonstration of systems.

7 References

4. Edvinsson, H.; Ryd, P., (2011), Modernization of I&C in Ringhals Unit 2 – Licensing and Safety Demonstration Experience, NPE 2011, Milan.
5. SSM (2016) SSM 2016:25 Licensing of safety critical software for nuclear reactors. Common position of seven European nuclear regulators and authorised technical support organizations.
6. 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.
7. Borg, A. (2013), Strategier för kommunikation SSM-TH I de tidiga faserna i komplexa tillsynsärenden Digital I&C, SSM Forskningsuppdrag. Commercial-in-confidence – refer to SSM who financed the investigation
8. Guerra, S., Menon, C., (2013), I&C modifications and implementation: requirements, issues and approaches, Adelard. Commercial-in-confidence – refer to SSM who financed the investigation
9. SSM (2006) SSM 2006:27 Safety Justification of Software Systems – Software Based Safety Systems Regulatory Inspection Handbook
10. Pavey, D.J., CEMSIS Cost Effective Modernisation of Systems Important to Safety, Final Public Synthesis Report (2004), UK. http://www.cemsis.org
11. IEC (2011) IEC 61513 NPPs – Instrumentation and control important to safety – General requirements for systems, Edition 2.0.
12. IEC (2015) IEC 15288 Systems and software engineering — System life cycle processes
13. Ryd, P, (2010), Concluding on Plant Safety and Functional reliability based on Safety Case Assessment with Configuration Management and Requirements-Solution-Verification Evidence, NPE 2010, Amsterdam.
14. IEC (2009) IEC 81346 Industrial systems, installations and equipment and industrial products - Structuring principles and reference designations, Part 1: Basic rules, Edition 1.0
15. IEC (2009) IEC 61226 Nuclear power plants – Instrumentation and control important to safety –Classification of instrumentation and control functions, Edition 3.0
16. IEC (2004) IEC 62138 Nuclear power plants – Instrumentation and control important for safety –Software aspects for computer-based systems performing category B or C functions, Edition 1.0.
17. IAEA (2016) Specific Safety Guide SSG-39 Design of Instrumentation and Control Systems for Nuclear Power Plants.
18. IEC (2006) IEC 60880 Nuclear power plants – Instrumentation and control systems important to safety – Software aspects for computer-based systems performing category A functions, Edition 2.0
19. IEC (2010) IEC 61508 Functional safety of electrical/electronic/ programmable electronic safety-related systems –Part 1: General requirements, Edition 2.0
20. IEEE (2009) IEEE 603 2009 - Standard Criteria for Safety Systems for Nuclear Power Generating Stations.
21. IEEE (2016) IEEE 7-4.3.2-2016 Standard Criteria for Programmable Digital Devices in Safety Systems of Nuclear Power Generating Stations

22. IAEA (2016) General Safety Requirements GSR Part 2 Leadership and Management for Safety.
23. IAEA (2015) Nuclear Energy Series No. NP-T-1.13 Technical Challenges in the Application and Licensing of Digital Instrumentation and Control Systems in Nuclear Power Plants
24. IAEA (2012) Specific Safety Requirements SSR2/1, Safety of nuclear power plants: Design
25. IAEA (2016) Specific Safety Requirements SSR-2/2, Safety of Nuclear Power Plants: Commissioning and Operation
26. IAEA (2006) Safety Guide GS-G-3.1 Application of the management system for facilities and activities.
27. NRC (2011) Regulatory Guide 1.152, Criteria for use of computers in safety systems of nuclear power plants.
28. EPRI (2014) Technical Report Principles and Approaches for Developing Overall Instrumentation and Control Architectures that Support Acceptance in Multiple International Regulatory Environments
29. Energiforsk, ENSRIC, F. Bengtsson, Lifetime extension of nuclear instrumentation and control systems, 2016

Appendix A: Safety Demonstration PLAN Template

This template is general and might be adapted depending on the needs of the specific Safety Demonstration, though the five main headlines should always be included. For clarity the content of each headline is briefly described with grey text. Two separate appendixes are recommended to be included with the Plan, namely the Safety Demonstration Case definition (in a table format) and the Safety Demonstration Plan overview diagram.

1. INTRODUCTION

1.1 Background

Briefly summarizes the project for which the Safety Demonstration is to be performed.

1.2 Document overview and reading instructions

Gives overview and instructions for how to read the present plan.

1.3 Purpose

Specifies the main purpose with performing the safety demonstration for the specific project.

1.4 Scope

Specifies what is included and all limitations and interfaces.

1.5 Roles and responsibilities

Specifies all stakeholders in the project and their respective roles and responsibilities in the Safety Demonstration.

1.6 Strategies and relation to other documentation

Includes at least two parts, namely; 1. Strategy for how the Safety Demonstration Case (SDC) is defined and 2. Strategy for reports and review including the relation between Safety Demonstration Reports and other Plant Documentation (SAR etc).

2. SAFETY DEMONSTRATION CASE DEFINITION

Defines the Safety Subject Areas with their scope and the strategy for demonstration and assessment including arguments and expected evidence. Appendix: Safety Demonstration Case definition.

3. ASSESSMENT OF SAFETY DEMONSTRATION CASE DEFINITION

Discussion and assessment of how well the SDC defined is deemed sufficient to demonstrate the project results, the NPP as safe when finalized.

4. SAFETY DEMONSTRATION PLAN

This section should describe the time schedule of the Safety Demonstration, specifying the reporting and review strategy. Appendix: Safety Demonstration Plan overview diagram.

Appendixes:

Safety Demonstration Case: Definition

Safety Demonstration Plan: Overview Diagram

Appendix B: Safety demonstration REPORT Template

This template is general and might be adapted depending on the needs of the specific Safety Demonstration, though the five main headlines should always be included. For clarity the content of each headline is briefly described with grey text.

1. INTRODUCTION

1.1 Background

Briefly repeats the summary of the project for which the Safety Demonstration is to be performed.

1.2 Document overview and reading instructions

Gives overview and instructions for how to read the present plan.

1.3 Focus and baseline of the present report

Describes the Safety Subject Areas in focus for the present report and the baseline that is assessed in the report.

1.4 Strategy for reporting

Describes how the report evolves and relates to earlier and coming version.

2. ASSESSMENT OF THE SAFETY DEMONSTRATION CASE DEFINITION

Discussion and assessment of how well the SDC defined is deemed sufficient to demonstrate the project results, the NPP as safe when finalized. If needed a description of how and why the SDC has been updated to remain sufficient. (Revise and issue new version of SDP with its Appendix: Safety Demonstration Case definition only when significant change to the SDC definition).

3. EVALUATION OF THE SAFETY DEMONSTRATION CASE

Reports and assesses the status of each Safety Subject Area as defined and according to the relevant phase expectations. This section might be chosen to put in a separate appendix instead of a report section.

4. OPEN ITEMS SUMMARY TABLE

Summarizes all remaining open items originating from any Safety Subject Area, together with action, responsible party and time plan and criteria for when the open item need to be resolved. Also lists any open items closed since last report.

5. TOTAL ASSESSMENT

Overall qualification status assessment summary and conclusion on safety for the present phase.

Appendix C: Guiding questions for Safety Demonstration in respective Safety Subject Areas

This SSA check list contains several guiding questions which could be used for defining the Safety Demonstration Case and for demonstration safety in the different Safety Subject Areas. The attachment can be seen as the basis for a check list but should not be considered complete and must be adapted for each application.

SSA 1 – PROJECT SCOPE

The project scope includes the total scope of the project, which in addition to the technical scope also can refer to e.g. the documentation, competence and training scope.

Technical Scope – Generally

To identify how a change in an existing plant affects the plant it is important to know what the change is based on, i.e. how the plant looks and works before the change is made. When changes are made to a plant, the existing documentation is often used as a basis for describing the scope and requirements for the change.

- Is the documentation describing the existing plant identified, available, correct and sufficiently clear?

Technical Scope - Functionally

A prerequisite for evaluating requirement and solutions is that the functional scope is clearly defined. For example, to be able to evaluate whether a time response requirement is met, it must be known where the function begins and ends. There is a significant difference if the function refers to the entire chain from detecting a deviating state in the process until it is corrected or if the function relates only to the chain from a change in the input signal to the control signal in the automation system.

Below are a few guiding questions for the functional scope:

- What is included in the functional scope? Does the function cover the chain:
    - From detected change in the process state to changed process state?
    - From detected change in the process state to the control signal?
    - From input signal to control signal?
- What are the functional interfaces between any subprojects and subcontracts as well as adjoining projects and activities? Is responsibility for functional *completeness* included in cases where the I&C is only part of the function?

- Is documentation describing the existing facility identified, available, correct and sufficiently clear regarding the functional scope? For example, are there sufficiently clear process descriptions/function descriptions or overview diagrams describing the functional scope?

Technical Scope - Physically (interfaces)

The physical scope refers to the technical change and the technical equipment in the facility. Below are a few guiding questions for the physical scope:

- Is the physical scope:
    - From a sensor output or is the sensor included?
    - From a sensor output or from an input card connection?
    - To the physical switch/actuator or to the terminal block on set/actuator or to output card connection?
- Where are the physical interfaces between any subprojects, subcontracts or adjoin projects and activities?

Technical Scope - Geographically

The geographical scope provides prerequisites for the requirements regarding internal and external events, such as fire and earthquake, environmental qualification requirements etc. Below are a few guiding questions for the geographical scope:

- Is the physical boundary defined in areas where the equipment is exposed to special environments, for example explosion, radiation, temperature, humidity, dust etc?
- Outside? Indoor?
- Shared or separate fire compartments?
- Restrictions on existing buildings regarding e.g. cabling and switchgear?
- Where are the geographic/spatial interfaces between any subprojects, subcontracts or adjoining projects and activities?

Documentation Scope

This refers only to the *scope of* documentation that will be included, i.e. its contents will be discussed in further detail in SSA 6. Below are a few guiding questions for the scope of documentation:

- Is the technical documentation included and to what extent?
- Is the instructing or work process documentation included and to what extent?
- Is there a delivery interface towards existing documentation?
- Should the project provide documentation as basis for updating existing operating, maintenance, quality and workflow documentation or is it included in the scope to deliver new *complete* documents?
- Does it include integrating the documentation in the documentation system?
- Is it included in the scope to tell which of the existing document should be deleted, replaced or revised?
- Is there a need to define a Safety demonstration scope from the *complete* Project Scope?

Competence and Training Scope

This refers only to the extent of training and competence needed, this means that implementation is included in SSA 7, 8 and 9. Below are a number of guiding questions for the competence and training scope:

- Is training of staff included?
- Does training plans include initial basic training as well as regular competence development?
- Does it involve recruitment of staff, e.g. automation engineers and operating personnel?
- Does it involve development of service agreement and providing competence during and after the warranty period?

SSA 2 – SAFETY CLASSIFICATION AND CATEGORIZATION

The Safety Classification is an important basis for application of graded approach in Safety Demonstration e.g. for detail and accuracy in requirements definition, product description and qualification etc. General principles are handled in this SSA while the actual safety classification is described in SSA 4. Below are a few guiding questions for the Safety Classification scope:

- Are there principles for Safety Categorization/Classification of Functions? Are the principles clear and easy to apply?
- Are there principles for Safety Classification of Structures, Systems and Components (SSC)? Are the principles clear and easy to apply?
- Are there specific principles for Safety Classification of the I&C part of Structures, Systems and Components?
- How will Safety Classification and graded approach be applied to technical and instructing documentation?

SSA 3 – REQUIREMENTS

The purpose of this SSA is to identify high level requirements for the project scope, including requirements on product design, work processes, staffing and competence, safety etc. It is also valuable in this SSA to identify important conditions (e.g. design basis) for the project. Below are a few guiding questions for the requirements:

General

- What are the high-level requirements of the project and the product?
- Do requirements adequately relate to the valid Plant Design Basis?
- Are the requirements traceable from high level input requirements?
- Are there specific requirements on the Safety Demonstration in the Project?

Product requirement

- Are requirements on the functional scope *complete*, i.e. are there requirements on all parts of the functional scope?

  - Are all functions specified?
  - Are the safety classifications specified for the functions?
  - Are there performance requirements for the functions?
  - Under which failures and tests/maintenance during operation should the function still be in its performance?
  - Under which assumptions, e.g. ambient conditions and operating conditions, should the function be?
  - Are the requirements on interfaces between sub-deliveries defined?
  - Are the security requirements for IT and requirements for remote connection captured?
  - Is existing documentation describing the plants function defined, correct and sufficiently clear regarding functional requirements? For example, are there sufficiently clear process descriptions/ function descriptions or overview drawings describing functional requirements?
  - Are requirements on where equipment may be placed (e.g. requirements for physical protection and/or requirements for where servers may be placed for security purposes) taken into account?
  - Are internal standards for requirements on e.g. programming captured?
  - Have requirements to ensure future operations, maintenance and changes been identified?

- Is the physical scope of requirements *complete*?
  - Are all requirements, regulations and applicable standards to the type of equipment caught?
  - Are requirements on testability and ability for maintenance, e.g. accessibility, considered?

- Is the geographical scope of requirements *complete*?
  - Have all the design preconditions for the geographical scope been caught, e.g. explosion, radiation, humidity, dust, seismic (vibration), EMC, temperature, gas, chemistry, corrosivity etc?

- Are the functional, physical and geographical requirements *correct*?
  - Compared with requirements, regulations and applicable standards as well as with requirements from the plant and process design.
  - What should the function look like? What time response, accuracy and reliability requirements should apply?
  - Have aspects related to physical and geographical implementation been considered, e.g. separation requirements, ambient conditions ("shake and bake"), installation and maintenance aspects?

- Are the functional and physical requirements as well as the environmental conditions *consistent*?
    - Are the requirements unambiguous or contradictory, inconsistent in terminology or in relation to interface definitions?

Process requirements

- What are the requirements on working processes, e.g. design, QA, Qualification, requirements management processes?
- Are there any requirements on instructing documentation (procedures, instructions, checklists etc)?

Requirements on staffing and competence

- What are the requirements on competences and staffing (numbers) in the project organization?
- What are the requirements on competence and staffing in the line organization taking over at the project finalization?

SSA 4 – PRODUCT DESIGN

The purpose of SSA 4 is to identify the current Product Design version relevant to the project scope. The degree of detail of the descriptions and evaluations in SSA 4 should be prepared with a graded approach based on safety importance (Safety Classification). Below are a few guiding questions for the Product Design:

- Is the solution (architecture and systems) unambiguously defined in a version or configuration.?
- Is the solution *complete*, i.e. is the construction specified for the entire functional, physical and geographical scope or are there gaps?
- Additional *completeness* is valued in relation to the safety significance. Have all the requirements been implemented in the solution, or are there any that have not yet been implemented (intentionally or obviously missed) in the current version?
- Is the design description *consistent* regarding e.g. terminology and definitions in scope, interfaces and requirements?
- The *correctness* of the solution is handled under Product Design Qualification.

SSA 5 – PRODUCT DESIGN QUALIFICATION STATUS

The focus in SSA 5 is to evaluate V&V records, e.g. reviews, inspections, analyses and tests. Qualification might be performed and demonstrated for Architecture, Systems, Platforms as well as on Equipment level. Qualification of the design fulfils the requirements *completely*, i.e. a verified and validated solution. Below are a few guiding questions for the scope of SSA 5.

- Has the solution been shown to meet all requirements through V&V-activities such as audit, inspection, analysis and/or testing? How and with which references?

- Is there evidence for all requirements? For the whole physical scope? Is it sufficiently comprehensive when it comes to input and output intervals, failure modes and errors, ambient conditions, environment etc?

SSA 6 – DOCUMENTATION

The purpose in this SSA is to identify the impact of the Project and Plant documentation in relation to the scope identified in SSA 1. Below are a few guiding questions for the scope of Documentation.

- To the extent that is included in the scope, identify which documents to be deleted, added or revised.
- Define a plan when each document is expected to be in place or become expired.
- Follow up on the plan and on that the results are of sufficient quality and comply with format and content requirements.

SSA 7 – QA AND PLANS INCLUDING ORGANIZATION AND COMPETENCE ASSURANCE

The purpose in SSA 7 is to evaluate that there are sufficient work processes, project plans and project organization for management and control in the **project** phase (including internal and supplier). SSA 8 below is intended to be used for evaluation of the *actual compliance* to the processes and plans as well as the *realization* of a clear organization with sufficient competence and staffing in place. In SSA 9 the same scope is discussed for the line organization who will take over when the project is ended. Below are a few guiding questions as help in understanding the scope of SSA 7, divided into the two perspectives.

Management system

- Are the management and quality assurance systems sufficient for the project task?
    - Sufficient for guidance on how to deliver the full Project scope?
    - Sufficient for guidance on configuration control?
    - Sufficient for guidance on how the project is to be planned, organized, competence-assured and staffed?
    - Sufficient regarding compliance with the Work Environment Act and requirements for personal safety?
    - Sufficient regarding insight and surveillance of supplier processes and plans?
- Is there an effective risk management process which is considered sufficient?
- Does the project have plans that cover the full scope and life cycle? Are the plans of the I&C project coordinated with other disciplines (e.g. mechanical, electrical, construction etc.), subprojects and possible superior projects?
- Is the design and V&V planning and governance sufficient in relation to the priority rating (e.g. safety classification and availability)?

  - Does the design control provide sufficient traceability from requirements through Product Design to verification?
  - Does V&V and test plans have sufficient coverage regarding requirements, product scope and test cases?
  - Are there any plans for installation, commissioning and commissioning test that govern the work well enough and in the *correct* sequence? Are the plans clear regarding interfaces with production, e.g. when in sequence and time the plant should be in partial or full effect? Are the commissioning tests well-planned with respect to operating economics and effort to minimize start and stop considered?

- Are there adequate checklists for the areas where this is considered appropriate? Using checklist is good for reducing mistakes and ensuring that work steps etc, are not overlooked. Using checklists provides support in keeping track of several things in both normal and stressful situations. Checklists are also effective when similar work is to be performed repeated times. General checklists should always be used with awareness that there may be specific aspects for each case that may not be included in the checklist.

Organization and Competence Assurance

- Is the defined organization sufficient regarding competence and staffing?
  - Is delineation of responsibilities clear in the organization?
  - Are the needs for resources and competence in the I&C area specified?
  - Are the needs for resources and competence with sufficient knowledge of the current plant and process specified?
  - Is the need for involvement of operation and maintenance specified?
  - Are needs for resource and competence with experience of similar projects taken into account?
  - Is the governance and plan for how to monitor and control the supplier in place? Are there established competence requirements for the individuals who deliver for the supplier, e.g. requirements for certified programmers (requirements can be handled under SSA 3)?

SSA 8 – QA AND PLANS COMPLIANCE INCLUDING ORGANIZATION AND COMPETENCE ASSESSMENT

The purpose of SSA 8 is to demonstrate compliance to SSA 7, i.e. the actual **project** execution and compliance to the processes and plans. Below are a few guiding questions for SSA 8.

- Are responsibilities adequately taken through the organization?

- Are the processes and plans adequately applied?
    - Is the organisation sufficient regarding competence and staffing in practice?
    - Have the plans been followed?
    - Have all activities been carried out, and if not, are deviations handled in an acceptable way?
- Has sufficient V&V coverage been obtained?
- Have risks been handled adequately and on time?
- Has adequate Safety Culture been realized in the project?

SSA 9 – NPP OPERATION, MAINTENANCE AND MODIFICATION

A successful project need to assure the preparation of the operation, maintenance and modification of the plant after the project. Therefore, readiness preparations for the line organization should be part of the project scope of delivery. Below are a few guiding questions for SSA 9.

Evaluation of the receiving organization including management system.

- Do the personnel have clear responsibilities and clear tasks in the takeover process and in the final organization after project completion?
- Is Safety Culture, with respect to operation and maintenance, adequately governed in the receiving organization?
- Are there personnel with sufficient competence?
    - Is there a functioning support/service agreement for machine and software?
    - Is there a phone number to call for support/service?
- Are there instructions and guidelines for staff work?
    - Are there functioning processes for project experience feedback which enable that important experiences from the project are considered for future operations, maintenance and changes?
    - Are there sufficiently clear directions for how warranty work will be performed?
    - Are there sufficiently clear directions for how changes/maintenance/emergency work will be carried out during the warranty period? What does the buyer do and not during the warranty period and what does it mean for the operation?
    - Are there sufficiently clear directions for how support and service will work?
    - Is there information about the life cycle of the automation product, e.g. need for preventive maintenance? Are there any preventative maintenance plans (e.g. computer replacement) that are decided on a higher level in the organisation? Are there any strategies for

purchasing spare parts and are there important spare parts in storage?
    - Are there processes for the I&C engineers work, e.g. regarding the maintenance of systems? Are there any routines for working in the system (e.g. IT security)?
    - Is there a management plan for documentation?

- Do the personnel have sufficient tools?
    - Is there a functioning remote connection for support that fulfil the IT security requirements?
    - Are any other necessary tools in place?

- Are there licenses for computer programs and rights to use and change in application programs?
- Is the documentation supplied with the project sufficient for future operation, maintenance and changes?

Appendix D: Figure 2.1 Full Page Format

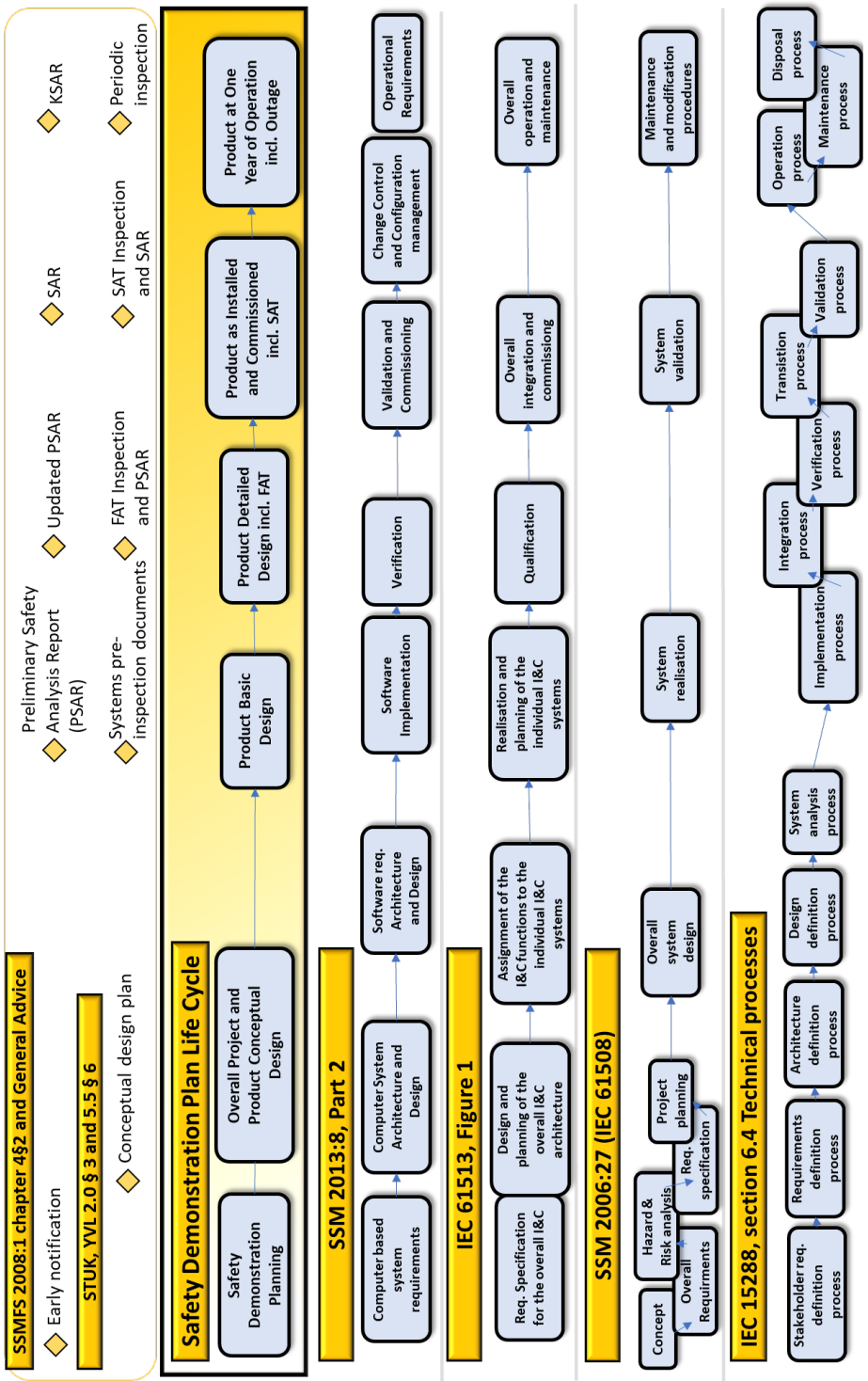


Figure 2.1 The figure shows how the Safety Demonstration life cycle relates to different (design) life cycles suggested in selected relevant standards and guidelines. The framed section identifies the phases of Safety Demonstration used in this Guide. These phases are derived from the life cycle of a general design process. The figure shows relation to corresponding phases of general design life cycles and can provide guidance on references to relate to in the demonstration in each phase. The time lines at the top shows the required reporting according to SSM and STUK respectively.

Appendix E: Figure 3.2 Full Page Format

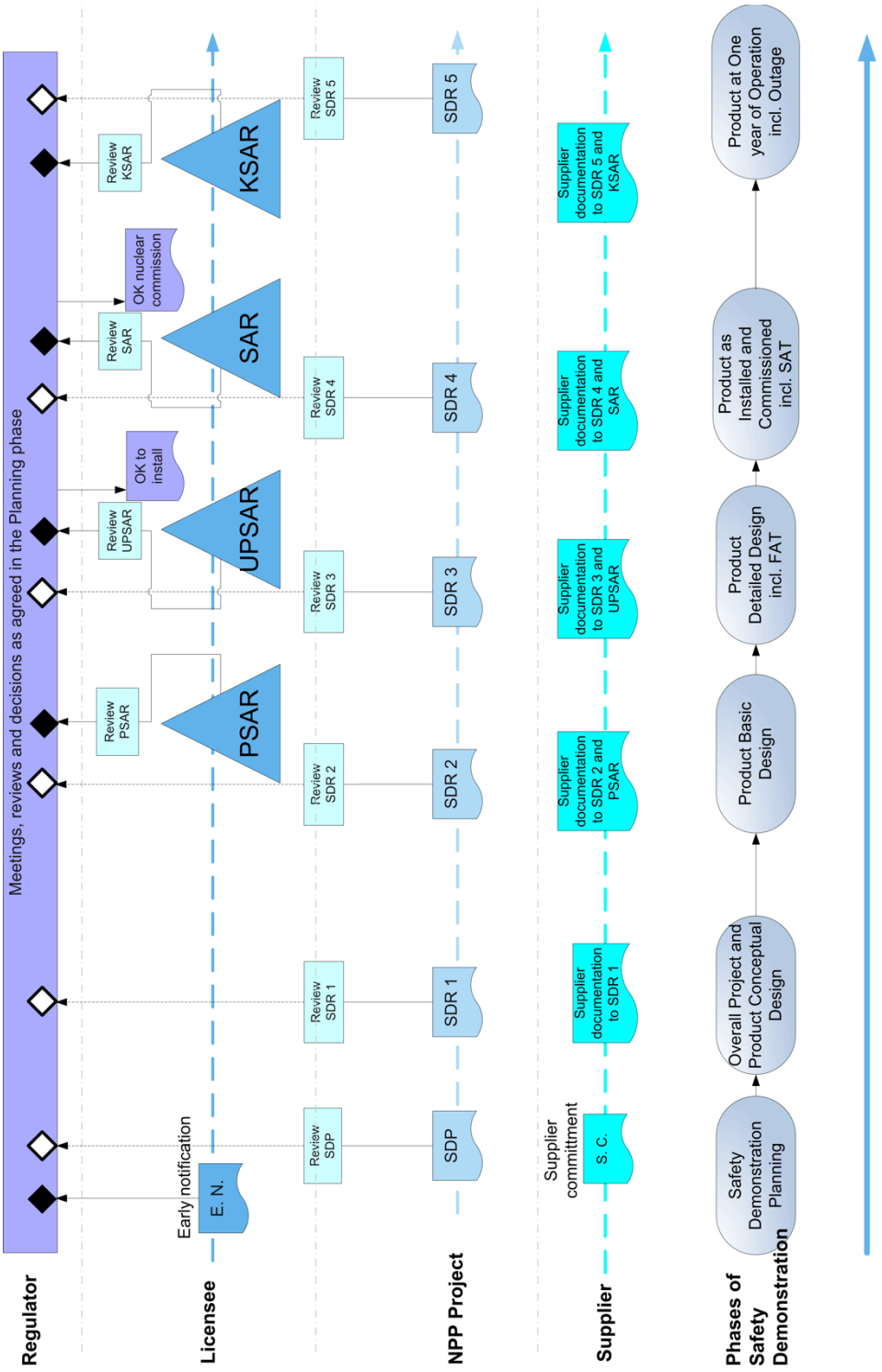


Figure 3.2 Illustration of a typical life cycle overview diagram in a Safety Demonstration Plan. Important activities and output documents during the Safety Demonstration life cycle are introduced for the main project stakeholders; Supplier, NPP Project, Licensee and Regulator.

SAFETY DEMONSTRATION PLAN GUIDE

In this guide a generalized method is presented for how to plan and perform safety demonstration for instrumentation and control systems in nuclear power plants. The method is developed to be applicable for large as well as small projects and for new build and modifications projects. The method is based on several different national and international experiences.

Three important purposes for performing Safety Demonstration are identified in this guide. The first is to convince oneself, in the project and as Licensee, that the plant is safe during and after the project implementation and document the basis for that conclusion. The second purpose is to demonstrate the safety, with argumentation and evidence, to reviewers and the regulating authority. The last and not least of the three, is to minimize both licensing and commercial risks linked to the project and the overall investment.

The guide suggests a structure for how to plan a Safety Demonstration and a life cycle model with phases related to normal project development phases. The most important phase of Safety Demonstration is the planning phase. The focus of the guide is to give a general model for Safety Demonstration and it also provides useful detailed references for specific problem areas when it comes to digital I&C systems in safety critical applications.

Using the method suggested in this guide should simplify the performance of Safety Demonstration and facilitate the possibility to exchange experiences between projects, between Swedish and Finnish sites as well as between authorities.

Energiforsk is the Swedish Energy Research Centre – an industrially owned body dedicated to meeting the common energy challenges faced by industries, authorities and society. Our vision is to be hub of Swedish energy research and our mission is to make the world of energy smarter!

Energiforsk