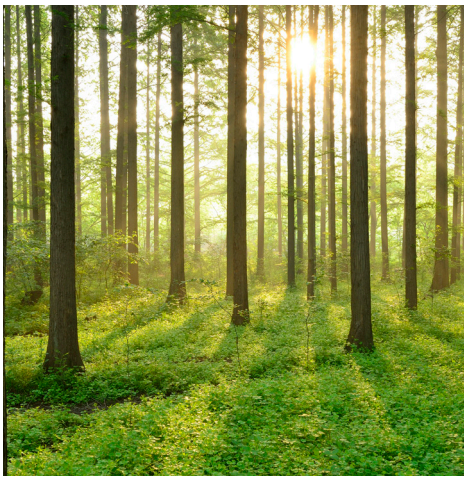
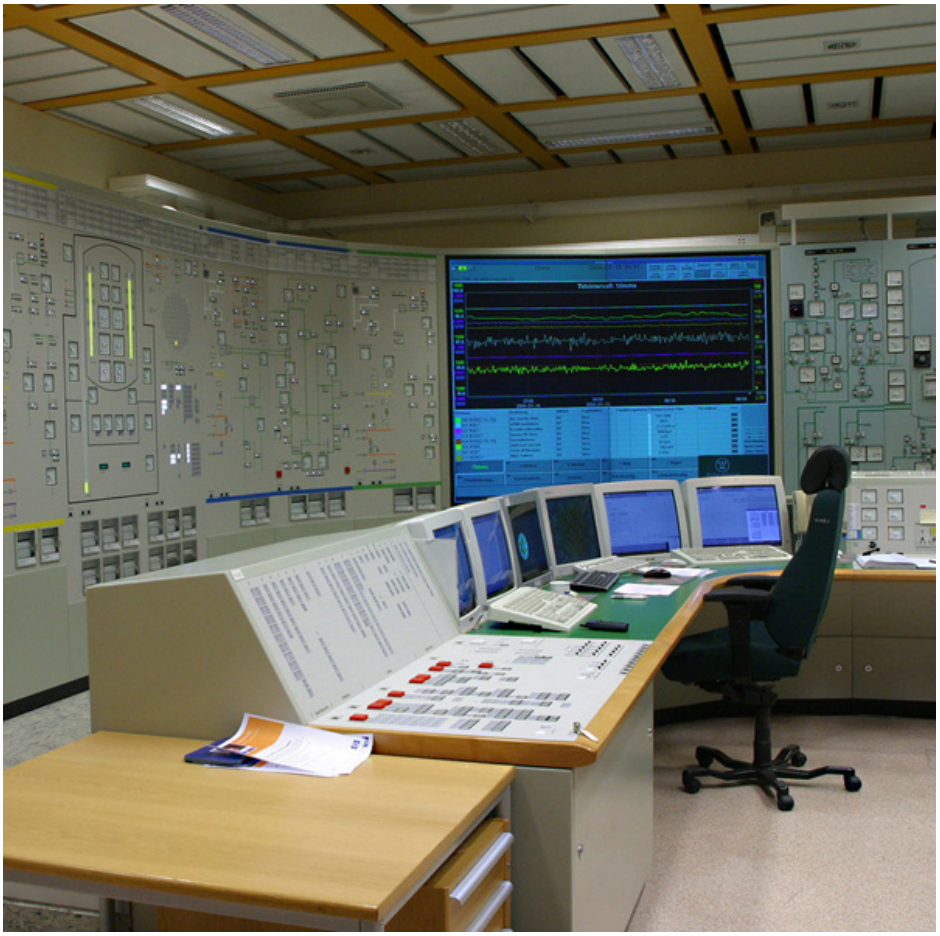
IMPLEMENTING COMPUTERIZED INSTRUMENTATION AND CONTROL SYSTEMS AT SWEDISH NUCLEAR POWER PLANTS

REPORT 2019:562



NUCLEAR

ENERGIFORSK NUCLEAR SAFETY RELATED I&C – ENSRIC



Energiforsk

Implementing Computerized Instrumentation and Control Systems at Swedish Nuclear Power Plants

Assessment of modernization projects

BO LIWÅNG AND KARIN FERM

ISBN 978-91-7673-562-6 | © ENERGIFORSK February 2019 | Cover photo OKG

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

Foreword

Starting in the 1990:ies, a series of modernization projects were initiated to change analogue instrumentation and control systems into computerized technology at the oldest nuclear power plants in Oskarshamn (O1 and O2) and Ringhals (R1 and R2). In this report, this process is documented mainly from the regulator point of view so summarize the experience from these projects.

The report is written by Bo Liwång former senior analyst and I&C expert at SSM and Karin Ferm senior management consultant at Evident, in close cooperation with the licensees represented, project team members from the projects covered by this report, Anders Johansson (Vattenfall), Hans Edvinsson (former Vattenfall employee) and Karl-Erik Eriksson (OKG). Stefan Persson, SSM has also contributed to the project. The authors would like to thank all persons involved in the report for taking their time to participate and for their contribution.

The activity is included in the Energiforsk Nuclear Safety Related Instrumentation and Control program – ENSRIC. The project is financed by Vattenfall, Sydkraft Nuclear/Uniper, Teollisuuden Voima Oy (TVO), Fortum, Skellefteå Kraft, Karlstads Energi and the Swedish Radiation Safety Authority.

Sammanfattning

Den här rapporten ger en historisk översikt av de genomförda moderniseringsprojekt som införde datoriserade I&C- system för säkerhet och säkerhetsrelaterade funktioner vid de svenska kärnkraftverken. Rapporten är skriven ur ett myndighetsperspektiv, SKI Svenska kärnkraftsinspektionens och SSM Strålsäkerhetsmyndighetens. Den innehåller samlade erfarenheter från myndigheten och tillståndshavarna erhållna under dessa projekt.

Fokus för studien är de stora moderniseringsprojekt som genomfördes vid Oskarshamn och Ringhals från slutet av 90-talet fram till 2015.

Konstruktion och implementering av datoriserade I&C-system kan inte verifieras i slutet av ett projekt. En förutsättning för att kvalitetssäkra datoriserade system är en dokumenterad utvecklingsprocess och en stegvis verifiering och validering (V&V). Införandet av den nya teknologin med datoriserade system tvingade både myndigheten och tillståndshavarna till att anpassa sina arbetssätt med avseende på kommunikation och rapportering samt genomförandet av myndighetens granskning av anläggningsändringen.

Kapitel 9, innehåller en sammanfattning av rapporten som bygger på den information som redovisas i kapitel 5 till 8 men kapitlet har även utökats med en sammanfattning av reflektioner från Bo Liwång, tidigare senior I&C expert och handläggare på SKI/SSM samt från tillståndshavarnas projektrepresentanter som framkom vid en genomförd workshop.

Huvudslutsatsen från rapporten är:

Enligt idag gällande relevanta standarder och forskningsrapporter om datoriserade system, rekommenderas en riskbaserad strategi där potentiella faror och händelser utvärderas som grund för nivån på den kvalitetssäkring och säkerhetsdemonstration som krävs för införandet. Dessa standarder kräver spårbarhet och en strukturerad verifierings- & valideringsstrategi under produktens hela livscykel. En dokumenterad konstruktions- och utvecklingsprocess samt en stegvis V&V-strategi är nödvändig för att kvalitetssäkra den här typen av system. För implementering av datoriserade I&C-system, är det inte möjligt att skriva en teknisk beskrivning i slutet av projektet som en utomstående person som ska kvalitetssäkra och granska en ny eller uppdaterad produkt kan nyttja och förstå. Detta gäller i synnerhet, när det datoriserade systemet ska användas för säkerhetsfunktioner. På grund av detta, krävs någon form av säkerhetsdemonstration som kontinuerligt under projektet, värderar, planerar, redovisar framdrift, verifikat och status mm. Det är viktigt att en dialog upprättas mellan myndigheten och tillståndshavarna tidigt i projektet, där man bland annat kommer överens om en planerad mötesserie, rapportstruktur och omfattningen på den information som kommer krävas för licensering av anläggningen.

Summary

This report is a historical overview of the completed modernization projects implementing computerized I&C systems used for safety and safety related functions, at the Swedish Nuclear Power Plants. The report is written from a Regulator perspective. The report also includes collected experiences obtained during these projects by the Regulator (SKI (Swedish Nuclear Power Inspectorate) /SSM (Swedish Radiation Safety Authority)) and the licensees.

Focus for this study are the large projects implemented at Oskarshamn and Ringhals from late 90's until 2015.

Design and implementation of computerized I&C cannot be verified in the end of a project. A documented design process and a stepwise verification and validation (V&V) approach is necessary to quality assure these types of systems. Due to that, both the Regulator and the licensees had to adapt their way of working when computerized I&C was to be implemented at the Swedish NPP's. The way to communicate, report project progress and the Regulators review was adapted to the new technology to be used in the NPP's. This report summarizes the experiences gained during these projects both from the Regulators perspective as well as from the licensees' perspective in terms of communication, accounting and the Regulator review. The Conclusion chapter 9, includes a summary of the report based at the information accounted for in chapter 5 to 8 but it is also extended with a summary of reflections from Bo Liwång, former senior I&C expert and analyst at SKI/SSM and the licensees project representatives, discussed at a performed workshop.

The main conclusion from the report is:

According to today's relevant standards and research reports regarding computerized systems, a risk based approach to evaluate potential hazards and events is recommended. These standards require traceability and a structured Verification &Validation approach during the complete life cycle of the product. A documented design process and a stepwise V&V approach is necessary to quality assure these types of systems. When implementing computerized I&C systems, it is not possible to write a technical description in the end of a project which someone outside the project can grasp, review or follow in a way that can quality assure a new or updated product. Especially not, when used for safety functions. Due to that, these types of projects require safety demonstration which is continuously accounted for during the project and also continues over the life cycle for the product or plant. Already in the beginning of the project a dialog between the Regulator and the licensee must be established, where the required information needed for quality assurance and licensing of the plant are identified and an agreement on how the accounting through the project shall be performed, must be made.

List of content

1 Introduction

This report is a historical overview of the completed modernization projects implementing computerized I&C systems used for safety and safety related functions, at the Swedish Nuclear Power Plants. The report is written from a Regulator perspective. The report also includes collected experiences from the Regulator (SKI (Swedish Nuclear Power Inspectorate) /SSM (Swedish Radiation Safety Authority)) and the licensees, obtained during these projects.

Focus for this study are the large projects implemented at Oskarshamn and Ringhals from late 90's until 2015.

1.1 PROBLEM AND BACKGROUND

During the period between the late 90's and 2015 there were 12 nuclear reactors in operation located in Sweden at the sites of Forsmark, Oskarshamn, Ringhals and Barsebäck. (the NPP's in Barsebäck were closed down in 1999 and 2005). Common for all of these reactors are that they were commissioned during the period from the beginning of-70's to the mid-80's and has served more than half of their intended life span of sixty years. Due to aging and to a sharpening of laws and regulations over the years, a need for modernization of the reactors started in the middle of the 90's.

Many Instrumentation and Control (I&C) systems have been in duty since the plant commissioning and are technologically old due to the swift development regarding I&C equipment since the first commissioning. The need for modernization of the plants required a decision where to continue with the old technology or invest in modern computerized I&C systems. The common decision for all the projects included in this study was to implement a computerized I&C platform for safety and safety related functions.

The processes and instructions for maintenance and changes of the NPP were adapted to the original set-up of used technology. In the same way, Swedish Nuclear Power Inspectorate (SKI) working methods for review and inspections were adapted to the usage of mostly analogue equipment in the NPP's. When performing an extensive modernisation program of an old plant including an introduction of a computerized I&C platform, a lot of new issues occur which were a challenge for both SKI as well as for the licensees, to handle and cooperate around.

1.2 PURPOSE AND RESEARCH QUESTIONS

The purpose with this report is to give a historical description and reflection of the large modernization projects implemented at the Swedish NPP's from the authorities' perspective. It also includes the likenesses' reflection of cooperation, required accounting and issues during the projects. The report must at least cover the large modernization projects where computerized I&C platforms were introduced into the old NPP's. These projects are:

- Oskarshamn: O1-Mod and O2-Plex
- Ringhals: R1-RPS/SP2 and R2-Twice

The Questions to be covered by the report but not limited to are the following:

1. What prerequisites did the Regulator (SKI/SSM) have when the modernization projects started to implement computerized I&C platforms
   a. Support by the regulations
   b. Knowledge of relevant standards
   c. Other standards, common positions and best practice
2. When in the project process was contact established between the licensee and SKI/SSM and to what degree was the Regulator involved during the project performance?
3. Important issues found during the projects and what impact did these issues have
4. How were requirements fulfilment, verification & validation and safety accounted for in the different projects? What conclusions did SKI/SSM and the licensee's draw from the used approach?
5. What research and branch cooperation has been performed as a result from the projects introducing computerized I&C platforms?
6. Current status at the NPP's and experiences received from the years of operation.
7. Future analysis

1.3 LIMITATIONS

This report is written in a technical level to suit the target group which is employees who are working within the nuclear industry or at the Regulator.

Focus is at communication between the licensee's and the Regulator, accounting and reporting from projects implementing computerized I&C platforms. Technical details of the solution for each platform are kept to a minimum. Furthermore, the licensee's perspective and the implemented projects have previous been documented in reports such as the Energiforsk report ref.[3]

2 Definitions and abbreviations

2.1 DEFINTIONS

2.1.1 Computerized system

Instrumentation and control (I&C) systems can be distinguished into many categories depending on what properties are used for the discernment. This report will focus on computerized system or equipment in contrast to analogue system which was to a large extent used in the original commissioning of the nuclear plants.

The term *computerized* is used rather than *digital* to avoid ambiguousness with terms. While the term digital may be interpreted as a binary state, e.g. on an electromechanical relay, the term computerized implies what is referred to as digital signal processing (DSP). However, the latter uses what is commonly referred to as digital signals, hence the ambiguity. A computerized system is defined to require software to perform some kind of programming at some point in the development, in order to obtain its function. It shall be noted that a computerized system is also required to work with *logical signals*, meaning that the signal can only take two distinct values (High or Low). This further requires the input signal to be interpreted to give it a useful meaning.

In contrast, an analogue system has its function defined directly from the ingoing components' relative connections to each other. As such, their function must not be obtained following programming of an integral component.

This report will due to this use the wording *Analogue* versus *Computerized* system/platform or *Programmable* equipment.

2.2 THE REGULATOR

The Regulator referred to in this report is the one responsible for governance of the nuclear industry. This report starts in the beginning of the 1980's and at that point in time, it was the Swedish Nuclear Power inspectorate (Statens Kärnkraftsinspektion, SKI) who had the responsibility. In 2008 a reorganisation was performed of the Swedish authorities and SKI was merged together with Swedish Radiation Protection Institute (SSI) into the Swedish Radiation Safety Authority (SSM). Due to that, the terms Regulator, SKI and SSM are all used in this report.

2.3 THE LICENSEES

The Licensee is the company which have the license and responsibility to operate a NPP in a safe way according to the current laws and regulations.

2.4 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 *(Safety demonstration plan guide, Energiforsk report 2018:512, ref [6].)*

2.4.1 Safety case

A collection of arguments and evidence in support of the safety of a facility or activity. This will normally include the findings of a safety assessment and a statement of confidence in these findings. *(IAEA Safety Glossary, 2016)*

2.5 ABBREVIATIONS

BWR	Boiling water reactor
CI	Configuration Item
CSNI	Committee of Nuclear Safety Installations
CNRA	Committee of Nuclear Regulator Activities
DPS	Diversified Protection System
DSP	Digital Signal Processing
EC	European commission
FKA	Forsmarks Kraftgrupp AB
FPGA	Field Programmable Gate Array
FSG	Independent safety review (Fristående säkerhets granskning)
HDL	Hardware Description Language
HW	Hardware
I&C	Instrumentation and Control
IFE	Institute for Energy Technology
KSAR	Supplemented (kompletterad) Safety Analysis Report
NPP	Nuclear Power Plant
O1	Oskarshamn 1
O2	Oskarshamn 2
OECD/NEA	Organisation for Economic Co-operation and Development where the Nuclear Energy Agency (NEA) is a specialised agency
OKG	Oskarshamnsverkets kraftgrupp
OTS	Off-the-shelf
PSA	Probabilistic Safety Analysis
PE	Programmable electronics
PLC	Programmable Logic Controller
PWR	Pressurized water reactor
QMS	Quality Management System
R1	Ringhals 1
R2	Ringhals 2
RAB	Ringhals Aktiebolag
RPS	Reactor protection system
SAR	Safety Analysis Report
SKI	Swedish Nuclear Power Inspectorate (Statens Kärnkraftsinspektion

SKIFS	Swedish Nuclear Power Inspectorate regulations (Statens Kärnkraftsinspektion Föreskrifts samling)
SSM	Swedish Radiation Safety Authority (Strålsäkerhetssmyndigheten) (former SKI,)
SSMFS	Swedish Radiation Safety Authority Regulations (Strålskyddsmyndighets författningssamling)
SW	Software
TBE	Tekniska Bestämmelser Elektrisk utrustning
V&V	Verification and Validation

3 Methodology

This report is based on Bo Liwång's experiences, working as an analyst at the Regulator SKI/SSM from 1982 to 2015. This is completed and combined with references to reports written by different staff members at the authorities from the beginning of the 1990's until 2015.

Interviews have been performed of present and former co-workers at SSM.

The licensees have been represented by project team members from the projects covered by this report, Anders Johansson (Vattenfall), Hans Edvinsson (former Vattenfall employee) and Karl-Erik Eriksson (OKG). A workshop with these former project members has been performed, where the challenges, gained experiences and the relation between the Regulator and the licensee's during performance of the projects were discussed. In a normal research report the conclusion chapter only includes summaries from the discussion chapters and no new information is added. Since the purpose with this report is to give a historical description and reflection of the large modernization projects, it differs from the normal set up of research reports. The Conclusion chapter is extended and contains reflections from the performed workshop where the participants accounted for their lessons learned and key to success factors based on their collected experiences. The topics for the workshop are included in Appendix A.

The project representative's roles during the projects:

- Karl-Erik Eriksson- was responsible for qualification of the I&C platform and speaking partner for supplier in both O1-Mod and in O2-Plex. Karl-Erik was the contact person for the Regulator regarding I&C questions.
- Hans Edvinsson- was the project client representative (the role who ordered the project) for Twice. Hans was responsible for the formal contact and dialog with the Regulator.
- Anders Johansson- was the project client representative (the role who ordered the project) for RPS & SP2. Anders was responsible for the formal contact and dialog with the Regulator.

4 Background

During the 90's, the Swedish licensees performed an overview and assessment of their modernization need. This assessment lead to modernization programs for the NPP's. In this report some of the largest projects implemented as part of each NPP's modernisation program will be accounted for. One aspect to consider was the need for modernization of aging equipment and since a computerized reform in the industry in general was on-going, it was natural also for the NPP's to evaluate if computerized platform could be one part of their modernization program. Different types of programmable equipment had been used in the plants size the 80's but no computerized platforms. These large scale projects including both process changes as well as the plan to introduce computerized platforms for safety functions gave SKI new challenges and they had to adapt their way of working.

4.1 BACKGROUND BO LIWÅNG

Bo Liwång is a former senior analyst at SKI and SSM.
Bo has a Master of Science in Reliability Engineering (graduation 74) from Royal Institute of Technology (KTH) in Stockholm and between 1975-79 worked as a lecturer and researcher at KTH. Between 1979 and 1982 he worked as a sub-project leader at Bofors, where Bo first came across computerized systems. In 1982, Bo started his career at SKI, continued over to SSM in 2008 and finally retired from SSM in 2015. During the years Bo has had a vast of different positions but from the early 90's he has been a specialist in electric and I&C systems with a focus at computerized systems

- Examination from Royal Institute of Technology in Stockholm (KTH) in Reliability Engineering 1974
- 1975-1979 Lecturer and Researcher at KTH in Reliability Engineering
- 1979-1982 Bofors Ordnance. Sub-project leader (reliability assessment and safety) within an anti-tank missile project.
- 1982-2008 Swedish Nuclear Power Inspector (SKI):
  - × 1982-1989 Deputy head of department of Research. Responsible for Safety Assessment Research.
  - × 1989-2008 Deputy Head section of Plant Safety Assessment. Special interest in assessment of Electrical and I&C systems.
- By July 1, 2008, Swedish Radiation Safety Regulator (SSM) was formed by putting together SKI with Swedish Radiation Protection Institute (SSI) to one organisation.
  - × 2008-2015 (retired) Senior Analyst, section of System Assessment, Electrical and I&C systems.
- From early 1990's to 2015 responsible for the strategies and assessment of Software based I&C systems important to safety

4.2 TIME LINE OVERVIEW

Here follows a time line overview including some important milestones from the middle of the 80's until 2015:

1985 Start of international cooperation regarding computerized I&C at SKI

1986 The Tjernobyl accident

1986 First issue of IEC 60880

1992 The Barsebäck event, the strainer incident

1998 SKIFS 1998:1, the first regulation for the nuclear industry published by SKI

1998 SKI require Millennium reports from the NPPs

1998 Re-start of project O1-Mod

1999 Project Twice starts

2002 Project O1-Mod completed

2003 Project RPS/SP2 starts

2004 Project Plex starts

2008 SKI is converted into SSM

2008 The regulations SKIFS is turned into SSMFS

2010 Project Twice completed

2010 Project RPS/SP2 completed

2015 OKG decided not to restart O2, and Project Plex is closed down.

2015 Transition Plan[1] implemented for all Swedish NPP's

In the middle of 1990's Sweden had 12 plants in operation. Two plants, B1 and B2, were taken out of operation due to political reasons, as they were close to Copenhagen.

[11] The NPP's generated a plan per plant, for how to fulfil the regulations, SKIFS 2004:17 and later on SSMFS 2008:17, the transition from one state of the plant to a modernized state.

Plant	Start operation	Decommissioned
Barsebäck 1 (B1) BWR	1975	1999
Barsebäck 2 (B2) BWR	1977	2005
Oskarshamn 1 (O1) BWR	1972	2017
Oskarshamn 2 (O2) BWR	1975	2015
Oskarshamn 3 (O3) BWR	1985	
Ringhals 1 (R1) BWR	1976	
Ringhals 2 (R2) PWR	1975	
Ringhals 3 (R3) PWR	1981	
Ringhals 4 (R4) PWR	1983	
Forsmark 1 (F1) BWR	1980	
Forsmark 2 (F2) BWR	1981	
Forsmark 3 (F3) BWR	1985	

4.3 OVERVIEW OF THE PROJECTS

During the 1990's international and national discussions on nuclear safety issues were on-going,(see 6.2.3 and 6.2.5). It was several reasons to this. Internationally, within EU was safety issues discussed with nuclear power plants in the Eastern Europe that were candidate countries to join the EU. In Sweden, it had also started evaluation of safety issues both at the licensees and at the regulator. Another impact of the safety analysis was the "Strainer incident" at B2 in 1992. SKI also published its first regulation in 1998. It resulted in a need for modernisation of the older plants (O1, O2, R1, R2). Furthermore, two plants (B1, B2) to be decommissioned due to political consideration. The main issues were separation and diversity in safety systems. The specific need for modernisation was different for each of the four plants. The other 6 plants (R3, R4, O3, F1, F2, F3) were considered not needing a modernization at this stage.

This report is focusing on the large projects at OKG and Ringhals where the complete or parts of the RPS functionality was transferred into a computerized system. The projects were:

- O1-Mod, OKG
- R2-Twice, Ringhals
- R1- RPS & R1-SP2, Ringhals
- O2-Plex, OKG

In chapter 7, a description of the projects and their scope are presented.

5 Overview of the Regulator

To give an understanding for the Regulator process in use at the time when the projects included in this report were performed, this chapter will give an overview of the Swedish regulator's organization and general principles for licensing of a Nuclear power plant (NPP) in Sweden.

5.1 THE ORGANIZATION AT SKI AND SSM

In 2008 the Regulator SKI was restructured and transformed into SSM. SKI was only responsible for governance of the nuclear industry and when put together with the Swedish Radiation Protection Institute (SSI), the scope for the new regulator SSM was enlarged to include all types of radiation usage e.g X-rays in hospitals and solariums. However, the organization of the Department of Nuclear Power Plant safety is kept more or less intact and is today organised in the same way.

The Regulator is divided into different types of business areas and for the nuclear power plants it is the area Radiation safe nuclear (VO1) who is responsible. The department of nuclear power plant safety, within this business area is performing the main part of the work related to radiation and nuclear safety. Other departments are responsible for other subjects in relation to the nuclear power plant within the business area e.g. control of core material, physical protection, information safety and inspection of the nuclear power plants readiness.

The department for nuclear power plant safety is divided into six sections which are specialized into different fields:

- Facility radiation protection
- Operations at Nuclear Plants
- Man Technology Organization (MTO)
- Reactor Technology and Analysis
- Structural Integrity and Event Analysis
- System Assessment

When large modifications are performed at a NPP, staffs from several sections are normally participating in the Regulator review, to ensure that the plant modification is fulfilling all aspects of the laws and regulations.

In most of the large plant projects the section of System Assessment has had a coordination role. The unit is responsible for supervision and investigations of the NPP's according to the following aspects:

- System technical design of barriers and defence of depth including electrical and I&C
- Components functions and functionality control, system functionality control and verification of operational readiness. (DKV)
- Fire and flooding analysis together with analyses for external events.
- Coordination of the department's work, supervision of the safety modernization and the NPP' safety analysis report (SAR)

The role Bo Liwång had at the authority is as a senior analyst and expert of I&C systems which belong to the Section of System Assessment.

5.2 PRINCIPLES FOR REGULATOR REVIEW OF PLANT MODIFICATIONS

A technical or organizational change of the plant which can affect the conditions that are accounted for in the safety analysis report (SAR) and principle changes of the safety analysis report of itself must be notified to the Regulator before the modifications are implemented.

Depending on the type of errand, the plant modification must be notified to the Regulator as soon as possible and in a reasonable time before it is planned to be implemented.

A modification notification shall include a clear description of the modification in relation to the earlier configuration and design, motive for the changes and an assessment of the safety consequences together with the verdict from the independent safety review (FSG) at the NPP.

For large plant modifications it is recommended to perform an early notification which comprises the plan for the modification, the prerequisites and what standards that are to be used.

Since 1998 with the publication of SKI's regulation, SKIFS 1998:1, has the formal safety reviews at SKI/SSM of major plant changes, such as power upgrade or modernisation of safety features, been based on review of the plants safety analysis report (SAR). The now valid regulation SSMFS 2008:1 specify that a preliminary safety analysis report (PSAR) shall be drawn up before a facility may be constructed and, for an existing facility, before major refurbishing or rebuilding work or major modifications are carried out. The safety analysis report shall be updated (FSAR) before trial operation of the facility may commence so that the report reflects the design of the facility. The safety analysis report shall be supplemented (KSAR), taking the experiences of such trial operation into account, before the facility is subsequently taken into regular operation.

The preliminary safety analysis report (PSAR), as well as the updated (FSAR) and supplemented (KSAR) safety analysis report, shall at all stages have been reviewed and approved by SSM.

When SSM receives a SAR (PSAR, FSAR or KSAR) from a licensee, an official in charge of the review is designated by SSM.

Depending on the scope and type of changes of the plant, a judgement is performed on what type of specialist competencies that needs to be incorporated in the review and if there are specific areas that shall be addressed in the review, such as separation, diversity, I&C-system, control room design or quality management system. In these selected reviews the licensees' activities on design, V&V, plant design etc. is scrutinised in general and is therefore more extensive compared to what is expressed in the SAR.

Due to the long project time for these modernisations and plant changes, and that the formal reviews of SAR (PSAR, FSAR, KSAR) is handle as separate review

errand, the official in charge and the personal participating in the review of the selected areas, can change over time for the different phases for a larger plant change.

For safety modernisations with introduction of software based safety systems, have complementary reviews, with different extent, been performed outside or within as a part of the formal review of SAR, which this report analysis and draw conclusions from.

6 Prerequisites

The use of computerized systems for I&C in the industry in general, are increasing and the nuclear power industry is no exception. As part of the modernization programs at the NPPs it was natural to evaluate and to implement computerized systems. Due to the high safety regulations in the nuclear industry, implementation of modern computerized systems to replace older systems is far from easy. Both the licensees as well as the Regulator had to adapt their way of working according to the new conditions. This chapter will describe the prerequisite both from the authorities and the licensees' perspective.

6.1 IMPACT OF THE TECHNOLOGY DEVELOPMENT

Back in the time of the first commissioning of the NPPs, the control systems were mostly analogue, meaning that the signals were processed using analogue electronics and logic was implemented using e.g. electromechanical relays. These I&C systems were generally custom built to serve a sole purpose, signals were hardwired and their function was locked once it was implemented and assembled on a component level. Many of these systems are still in operation in the NPPs today due to their robustness. Already from the beginning, the NPPs also were equipped with computerized I&C systems and equipment. At the time of the first commissioning, computers were vastly different from what we are used with today and the usage was used for a limited and dedicated function. The processes and instructions for maintenance and modifications of the NPP were adapted to this set-up of used technology. In the same way, SKI's working methods for review and inspections were adapted to the usage of mostly analogue equipment in the NPPs

During the 90's the evolution of computerized system was rapid. In the beginning the systems were small with a dedicated purpose which developed into multitasking systems which could be adapted to a vast of different usage areas. This development leads to an increasing amount of requirements for verification, validation and demonstration of the systems. The focus for qualification of a system moved partly from the HW and the base-SW to the complexity of functionality and features added to the systems. Due to this, the Regulator expectation on the safety demonstration and the extent of the V&V accounted for by licensees, increased over the years. The projects accounted for in this report were long and the rapid technology change of the chosen system did also have an impact on the actual performance of the project, e.g. version changes of HW/SW in the middle of the project. Apart from this, events around the world always effect the requirements and need of plant modifications e.g. Fukushima.

This rapid development of computerized systems is still on-going but it has slowed down a bit since the 90's where the whole industry made a huge development step.

Due to this, it is important to keep in mind that the prerequisites for the projects accounted for in this report differ a lot. The requirements from laws, regulation, standards and international best practices have increased a lot from the start of O1-Mod until 2015 when the last project was ended.

6.2 PREREQUIESTES FOR THE REGULATOR

In the beginning of the 90's there were few developed standards to support implementation of computerized systems in the nuclear industry. Neither was the regulation from SKI updated to include requirements for programmable equipment. Both the nuclear industry as well as the Regulator had to search for guidance and support from other parties.

There are three projects/activities at SKI that have had a great impact on the Regulator review strategy for programmable software systems, see 6.2.1 to 6.2.3.

Besides the activities presented below, there were several projects that have had an impact on the review strategies, such as the EU research projects as CEMSIS (www.cemsis.org) in the beginning of the 2000, and the later HARMONICS (www.harmonics.vtt.fi).

6.2.1 The Repac project

The very first project implementing a new computerized system was performed at R2 where some part of the equipment for signal treatment was installed as one part of the project changing the steam generators, in 1992. This project was called PAC. Later on, 1995-1996, a similar project was performed at R3 but changing all the signal treatment equipment, but the central safety logic (SSPS) was not changed. This project was called REPAC. Ringhals and SKI discussed how to find a feasible way of planning and executing the Regulator review process. Bo with his expertise in this field was involved in the project. There were no paragraphs in the regulation to support the decisions at this time and as few standards developed for the nuclear industry existed, SKI took support from the Halden Project, (see chapter 6.2.5).

On a research contract from SKI, Halden project developed guidelines, ref [1], which could be used by SKI in the review process for acceptance of computerized systems used for safety systems in nuclear power plants. The guidelines points out what should be expected from the licensee and what SKI should look for in the reviewing of the project.

The guidelines are divided into chapters and sections according to the different activities made during the development of the system, from "overall safety aspects", "specifications" to "installation", "maintenance", "operation". The text is divided into general explanatory information and a set of short recommendations to SKI

Based on this, a meeting plan was decided up on, following the development process, result and plans were presented and discussed. The experts from Halden Project participated in the meetings and also performed an assessment of selected parts of the application software.

The conclusion was that the meetings from early in the development process to the end treating different topics depending on where in the development process they were performed, was very effective for the Regulator review.

6.2.2 Preparations prior to the Millennium

Another important milestone and a prerequisite for how to work with computerized systems was the preparatory work performed prior to the Millennium (Y2K) In early 1998 the Government required from SKI reports at three occasions (autumn 1998, spring 1999 and autumn 1999) on the safety of the nuclear facilities in relation to the millennium shift. SKI should come up with a plan for the reporting to the Government. Before this request from the Government, the millennium shift was handled by SKI's IT department, but was now considered as a nuclear safety issue, and the section of Plant Safety Assessment at the Department of Nuclear Power Plant Safety should handle the issue.

The plan that was developed for the reporting from the NPPs was the following:

- First report- An analysis of the situation and a plan for the required actions
- Second report- The progress of the work and if any special problems areas detected.
- Third report- End report summarising the result and that the facility is safe.

The Swedish National Audit Office (Riksrevisionsverket)[2], performed an audit of SKI's work and was very satisfied with the established way of working with the working approach to follow the work progress from start to the end at licensees. It lead to a good confidence in the result, see ref. [5]). This approach has had a vital impact on the chosen way of working with Regulator review of the projects introducing computerized I&C platforms.

6.2.3 EU-Cooperation

The "Task Force-Safety Critical Software" was formed by EC , "Nuclear Regulator Working Group" (NRWG), in 1994. From the beginning participating countries were : Belgium, Germany, UK, France. In January 1996 Bo Liwång from SKI became a member of the task force. Later on new countries joined the task force, and a first report was published in 1998. During 1998 and 2000 a research project, financed by EC made a major contribution to the report, which was published in 2000 as EUR 19265, ref. [7].

The work has continued after that with several new editions of the report. For full information on the history of the work and the development of the report see "Licensing of safety critical software for nuclear reactors", SSM 2018:19 ref. [7], which is the latest revision of the report. Since the starting of the work several other countries outside Europe have contributed to the report, see SSM 2018:19, ref. [7], for full information. Bo stopped working in the task force in the beginning of 2015 as he retired but SSM is still participating in the work of the task force.

[2] The Swedish National Audit Office- The Swedish NAO is part of parliamentary control. They ensure that the Parliament receives a coordinated and independent audit of state work processes and finances. Furthermore, they contribute to the development of parliamentary control and the democracy of other countries through our international remit.

6.2.4 The support of the regulation and standards:

When the modernization projects introducing computerized systems started in the beginning of the 90's, the Swedish regulations was not updated. In 1998 the first Regulation for nuclear power plants were published by SKI. On the topic of assessment and approval of software based systems, it did however not give much advice. It is however one paragraph that has been useful in SKIFS-1998:1, see ref [1]:

"Chapter 3, Section 4 Structures, systems, components and devices shall be designed, manufactured, installed, inspected and tested in accordance with requirements adapted to their function and importance for the facility's safety."

It does not describe how to perform the assessment but indicates that something needs to be done and the proof of requirement fulfilment is central. This has been used in the dialog with the licensees.

Instead of the regulation, SKI had to find support in international forums, as expressed in chapter 6.2.1 – 6.2.3, and at the time available standards. The following standards have been used for support during the years:

- IEC 60880:2006 *"Nuclear Power Plants – Instrumentation and Control Systems Important to Safety – Software Aspects for Computer-Based Systems*", ref [8] is a functional safety standard which, together with IEC 62138, covers the software aspects of computer based systems used in nuclear power plants to perform functions important to safety. IEC 60880 provides requirements for the safety category A as defined by IEC 61226.
  - × In 1986 was the first edition of IEC 60880 regarding programmable equipment published and in 1996 a first addendum was added. In 2000 a new edition of 60880 was published
- IEC 61508 "*Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems*" ref. [10] is a basic functional safety standard applicable to all kinds of industry. It defines functional safety as: "part of the overall safety relating to the EUC (Equipment Under Control) and the EUC control system which depends on the correct functioning of the E/E/PE safety-related systems, other technology safety-related systems and external risk reduction facilities
  - × The first edition of IEC 61508 was published in 1998 and later on it was updated in 2000. This standard is not nuclear specific but is still frequently used by the NPPs especially in England
- IEC 61513 *(Nuclear power plants. Instrumentation and control important to safety*), ref. [9] *is* a derivate from 61508, adapted for the nuclear industry. It gives general requirements for computerized systems
  - × First edition of IEC 61513 was released in 2001
- IEC 61226- "Nuclear power plants - Instrumentation and control important to safety - Classification of instrumentation and control functions", ref. [11]
- IEEE 603 "Standard Criteria for Safety Systems for Nuclear Power Generating Stations", ref. [12]
- IEC 60987 "Nuclear power plants - Instrumentation and control important to safety - Hardware design requirements for computer-based systems", ref [16].

6.2.5 International cooperation and research

The Halden project

The Halden project is an international research program performing research on nuclear fuel, material, MTO and software safety for the nuclear industry. The Halden- program was started in 1958 as a part OECD/NEA. SKI/SSM have been a long time member of the project. IFE is the organiser of the program. The number of countries participating is around 19. The Halden project is performing research based on the three year period research program and besides that, the Halden project performs bilateral project, as the one for REPAC see chapter 6.2.1.

More information can be found at https://www.ife.no/en/ife/halden/hrp/the-halden-reactor-project

OECD/NEA

OECD/NEA is an international organisation in the area of nuclear safety: CSNI, Committee of Nuclear Safety Installations (the research part) and CNRA, Committee of Nuclear Regulator Activities (the regulatory part).

Within the OECD/NEA-CSNI there are working group (WG). One WG is the WG-Risk (former WG-5) that is working on the area of PSA-analysis, but also software safety issues. Bo has been a member of the WG-Risk since 1983 with his background in research of PSA at SKI.

OECD/NEA-CSNI organised a couple of workshop/conferences in the area of digital systems during the middle and end of the1990's

In 1995 it was formed an informal task force in WG-Risk, COMPSIS, for discussion of experience from computerized safety systems. This was in 2005 formulised as a research project, with 10 participating organisations where SKI was one, trying to draw conclusions from experience of the operation of these systems. The second period was between 2007 and 2011

For full information of the OECD/NEA activities see their webpage.

6.2.6 Conclusions related to the Regulator prerequisites

- The Halden-program help out with the knowledge regarding the importance of getting involved early and to continuously follow the development process
- The REPAC project became a role model for how communication during a project shall be performed and established a way of working.
- The Millennium (Y2K) report for the government gave a structured way of working with planning and reporting of modifications involving computerized systems.
- The European cooperation lead to the insight of the need for a Safety demonstration plan

This knowledge achieved in the beginning of the 90's, was used as the basis for the way of working and how to communicate between the licensees and the Regulator in the coming projects which were implemented from the late 90's until 2015.

One important lesson is that, it is not possible to verify the result in the end, there must be a proper analysis and plan in the beginning of an implementation project which is accounted for continuously through the project. This is also a "golden rule" for design of computerized systems in general which is described in most used standards today, e.g IEC 60880 [8], IEC 61513 [9]. The technical requirements need to be developed and followed up on continuously during the development process which has led to the use of the V-model for V&V in many projects. (see Chapter 5.3, IEC 60880, Second Edition 2006-05, ref [8]).

7 Description of the projects and the Regulator review

In this chapter the scope of the projects, the dialog between the project and the Regulator and Regulator review is presented.

For large plant modifications it is recommended to perform an early notification to the Regulator which comprises the plan for the modification, the prerequisites and what standards to be used. For project which includes I&C modifications, analysts with I&C competence from the section of System Assessments at the Regulator should be involved, at the latest, when the preliminary safety analysis report is sent to the Regulator. At that point the licensee shall have a clear conceptual solution for what modifications to be implemented, how it affects the plant configuration and the safety functions. The Regulator can at that point judge how much attention the project requires and assemble a suitable internal project. For the large scale project implementing computerized system the dialog regarding a Safety Demonstration plan started when the licensees presented their conceptual solution for the first time.

7.1 PROJECT O1-MOD

O1-Mod was re-started 1998 and finalized in 2002

In 1992 there was an incident where the strainers of the emergency core cooling system were plugged by isolation fibres at one of the Barsebäck reactors. The Barsebäck event led to an overview of the BWRs in Sweden to prevent similar events. At OKG the "project Fenix" started at O1 after the B2 "Strainer incident" with the main task to change the isolation and different mechanical parts in the O1 plant. In the permission to start the operation of the plant in 1995, SKI required that the plant must be modernized until 1999 to maintain the operation permission. In the end of 1998 most of the modifications of mechanical parts of the plant were completed but the issues regarding the I&C system was not solved. As a result of the safety analysis of the O1 plant in the middle of 1990's it was concluded that the plant needed a new safety concept. During the second half of the 1990's Framatom ANP and ABB Atom got contracts to develop the new safety concept. OKG performed an evaluation and concluded that they should use the safety concept from Framatom ANP but with ABB Atom as a supplier of the new I&C system. O1-Mod restarted in 1998 with a scope focusing at the safety concept and I&C changes.

7.1.1 Scope for O1-Mod

The main task for O1-Mod was to increase the separation and in the same time to modernize the I&C system. The new safety concept included improvements of the redundancy, diversity, physical separation, seismic requirements and separation of operational and safety functions. To diversify the reactor protection system (RPS) a parallel and separated system, the diversified protection system (DPS), was introduced. The DPS is realized with conventional technology. The amount of

safety functions was doubled due to this solution. The control room was modernized and a new turbine installed.

Safety system:

Reactor Protection (RPS), Diverse protection system (DPS) and all other Cat A functions in EKB (Emergency Control Building).

7.1.2 Project performance

Initially the computerized I&C platform ABB AC 110 was chosen to be used. When the platform was analysed it was found out it would be too complicated to qualify the platform according to the requirements in applicable nuclear standards e.g. IEC 60880 [8]. In 1998 OKG chose to make a restart of the project, O1-Mod, with the intention to use another I&C platform, ABB AC160, that later became the Westinghouse Common Q. The computerized platform AC160 had an already qualified application for traditional thermal power industry. The judgement was that this platform would be easier to qualify according to the nuclear standards than AC 110, since a documented structured development process had been used by the supplier when the platform was originally developed.

In the O1-Mod project, Westinghouse[3] performed the qualification of AC160 according to IEC 60880 [8]. When proof for fulfilment of criteria was missing, they performed an "Additional Qualification Demonstration" (AQD). In the project it was performed very deep technical reviews. There were regular meetings between Westinghouse Atom, that used TüV as independent reviewer, and OKG that besides its internal technical departments used Colenco (Switzerland) and ISTech (Germany) as reviewers. The purpose with this activity was to come to a common interpretation of the standards which were necessary to show the fulfilment of the standard requirements.

The qualification was divided into eight areas:

- Design Bases and Design Descriptions
- Codes and Standards
- Product Software Qualification
- Product Hardware Qualification
- Analysis
- Verification and Validation
- QA and QC
- General Qualification Support

7.1.3 The Regulator review of the project

Bo Liwång had god contact with O1, already in the project Fenix (1992-1995), as he was one of the reviewers of the Fenix project. At the restart of the O1-Mod project after the decision to use the AC160 platform, Bo was invited to participate to give a lecture of the expectations from the Regulator. Bo described the EU Regulators

[3] In 2000 ABB Atom was bought by BNFL and integrated in the Westinghouse Company. It became Westinghouse Atom AB

Task Force work (see chapter 6.2.3), he participated in and the key to success in this type of projects (EUR 19265 ref. [7]). The recommendations were:

- Transparency
- Clarity
- Traceability

O1-Mod had worked well in all these aspects and the delivered documentation followed a clear document structure where all documents had a clear presentation of the purpose and level of details.

The strategy for the Regulator review of this project is that it has been concentrated to three areas:

- Review of OKG's internal technical review
- Review of the project requirement capture process
- Review that the development process has been performed in a structured and documented way

SKI followed the progress in the project with regular meetings. At these meetings, presentations were performed within different areas such as:

- The technical computer platform
- The planning and performance of the design work
- The planning and performance of different safety reviews
- The documentation and the traceability

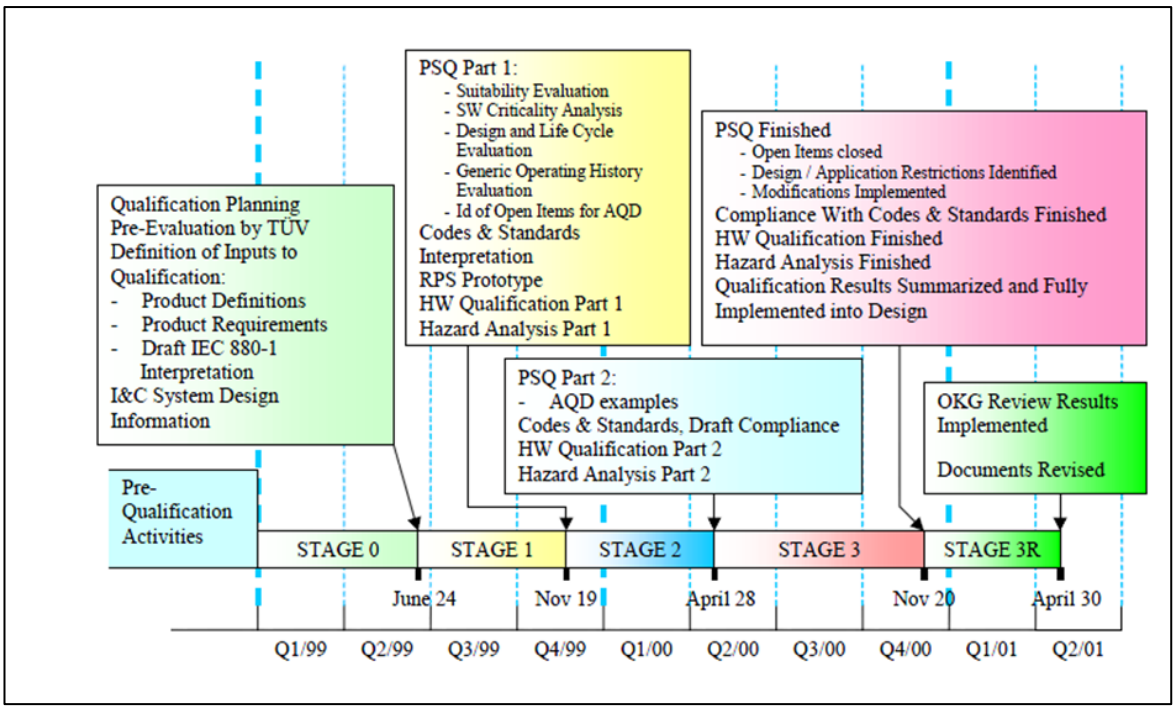


Figure 1: Qualification stages

An observation from a Regulator point of view, it was difficult to get a good knowledge of the total development process, due to limited available work resources at SKI. Based on the experience from the Regulator task force (TF-SCS) SKI wanted OKG to present an argumentation on four topics:

1. Give a description of how the design work has been performed following a clear sequential V-model.
2. Describe how the System Requirements was produced including the used strategy for handling different views of interpretation of the requirements.
3. Describe the work on primary safety review and internal independent safety review.
4. Describe the process for designing the test programmes. Show the coupling between the requirements and the test programmes and that the performed tests give a representative picture of the behaviour of the system.

Conclusion

The general conclusions from the regulator were

- that the documentation structure worked well
- that the regular meetings between the involved parties (OKG, ABB Atom (Westinghouse) and Framatom ANP (Areva)) ensured that all important issues were covered
- The meetings with the Regulator from early in the project made it possible for the Regulator to follow the development process
- The response from OKG on the four questions gave insights on the argumentations for that requirements were fulfilled

7.1.4 The licensee's perspective of the dialog and performance

In both O1-Mod and Plex there were uncertainties of the format, the formal relation to the SAR and the content level of the safety demonstration plan which lead to a lot of discussions and rework before approval. The uncertainties arise between all parties in project, Regulator-Licensee-Supplier.

7.1.5 The licensee's important issues and reflections

The platform was changed from AC 110 to AC 160 due to equipment qualification issues. At the time there were on-going qualification activities for AC160 in both Korea and in USA which OKG was promised by the supplier to benefit from. Those activities were delayed and instead of using their result, OKG was first out to qualify the platform which instead other parties could use. This lead to a very comprehensive and good documentation since Westinghouse was about to use the result in other countries.

7.2 PROJECT R2-TWICE

Project Twice (Two Instrumentation and Control Exchange) was started 1999 and ended in 2010.

The reasons for the modernization of R2 were mainly due to aging equipment, obsolescence, no spare parts and lack of technical support from the original vendors. The modernization also included improvements of the plant safety level in specified areas and separation between the subs. It was decided to include enough spare capacity in the system to accommodate modifications to safety systems due to expected modernisation of Swedish regulations. To estimate required spare capacity Ringhals 2 used information from the so called "Värnamo-gruppen", cooperation between Swedish utilities to develop modern requirements.

The Twice project chose to use the computerized platform AC 160/Common Q for the CAT A functions. The required diversified protection system (DPS) was also implemented in a computerized platform but of another type, the Westinghouse Ovation. The use of AC160 meant that the performed Qualification made in O1-Mod together with the Common Q qualification made in USA could be re-used but the qualification had to be completed with some new modules required for R2. For acceptance to use the Ovation platform for the diversified system it was demonstrated that it was diversified to the AC 160 platform.

The project meant an extensive re-design and modifications of the plant.

Scope for Twice:

The R2-Twice project involved modernization of most of the instrumentation and control functions, plants systems and the Main Control Room (MCR). The project also included the modernization of the Ringhals 2 full-scale simulator used for operators training and qualification.

A partially new requirement level was applied, for example an upgrade of the existing separation level. Functional classification was made in accordance with the IEC 61226.

Safety System:

Reactor Protection System (RPS), + PRM:

Included functions: Reactor Trip, Engineering Safety Features, diesel sequence, Post-Accident Monitoring System

Safety related and Non-safety systems:

Ovation is used for surveillance and control of non-safety systems and functions, electrical safety category CAT B, C, O.

7.2.1 Project Performance

The first presentation from the Twice project included an accounting for how the requirements from the standard IEC 60880 had been developed. It was performed in a similar way as O1-Mod had done it but no further analysis or planning was included. SKI pointed out that a more extensive presentation was required to show

how the project should quality assure this large scale project, where a computerized I&C platform for all the Safety functions was included.

The Twice project answered with a Plant Safety Assurance and Demonstration plan (PSADP), ref [13] and later on, corresponding reports (PSADPR).

7.2.2 The Regulator review of the project

Meetings were held on regular basis between the Regulator and Twice, approx. every fourth month. The regular meetings covered both high-level topics but also deep details on the tools that were used in the development. This and the different received PSADR's, gave the Regulator a good overview of the progress and project status.

An important issue in the review was the diversity between RPS (AC160/Common Q) and DPS (Ovation), as they were both based on computer platforms. In UK there was a rule stating that if the primary Reactor Protection System (RPS) is based on a digital platform, the Diversified Reactor Protection System (DPS) shall be a "hardwire" system. After evaluation, the conclusion was that the diversity was considered acceptable as:

- Different manufacturer, including programming tools
- Different processors
- Different operating system
- Different programming language

The validation and the demonstrated Safety case were of good quality and the Regulator was satisfied with the accounting. On the other hand, the formal SAR didn't follow the design solution and the presented reports (PSADR) in a distinct manner; it was not unambiguous and clear. R2 had to update the SAR after the project had completed the installation and commissioning.

The suppliers way of working was presented visually through link to the Westinghouse office in USA, e.g. was Configuration Management shown for SKI//SSM, which gave a good insight of their tools and way of working.

From SKI/SSM there was an internal team working with the project's different parts, with designated inspector, I&C expert, HFE expert etc.

The safety demonstration (PSADP/PSADR) included the following objectives:

1. To identify how (what – by whom – when – how) Ringhals is going to assure and demonstrate Plant Safety during and following the modernization/replacement of the Plant I&C system, including how Ringhals is going to document and demonstrate this in SAR and other reports and perform formal safety review
2. To identify what will be presented to SKI and when, both for information/review and for requesting formal permits.
3. To document the TWICE Total Safety Case grouped into Safety Subject Areas with Claims/Sub-claims and strategies for demonstrating compliance.
4. To elaborate on the approach for Plant Safety assurance and 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.

5. To allow for smooth transformation of the PSADP into the PSAR/SAR and Plant Safety Assurance and Demonstration Reports(PSADRs) and safety reviews, which will all together be used in the request for continued operating permit after the Plant I&C system modernization.
6. To document the philosophy, outline and plans for PSG in depth (=ISG) which is reported in the PSADRx.

This plan was agreed on between SKI and R2, by SKI acceptance.

In the Total Safety Case, which is a part of the PSADP, 14 Safety Subject Areas (SSA) was defined. For each of the SSA, claims and sub-claims, there are defined what shall be performed and who of the three parties (Westinghouse, R2-TWICE Project or R2 Plant) that is responsible for the performance of the activity. The 14 Safety Subject Areas are presented in Figure 2.

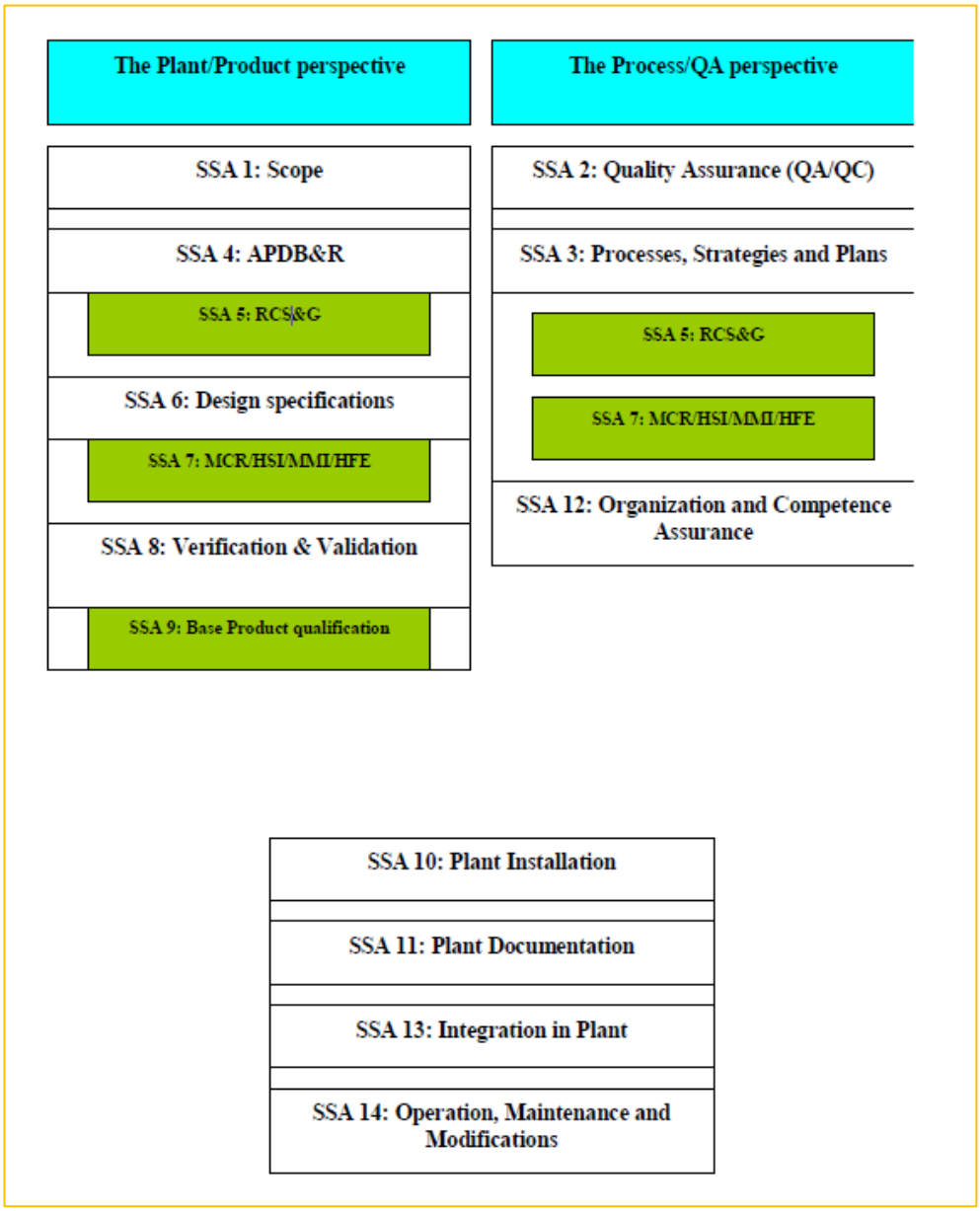


Figure 2: Picture of the 14 Safety Subject Areas (SSA)

Conclusion

- PSADP/PSADR with its clear structure was very good
- The objectives defined in PSADP/PSADR gave a clear overview of the purpose
- The regularly performed meetings on high level strategies and detailed performance together with presentations of used tools, gave the Regulator a good insight of the project performance
- The visual presentation of the suppliers' way of working with e.g Configuration Management gave the Regulator a better understanding of the documentation

7.2.3 The licensee perspective of the dialog and performance

The dialogue was good during the project but the prerequisites were not in place in the start. The expectation and agreement between the Regulator and the licenses was not clearly defined in the beginning. The final result was however the PSADP/PSADR which the Regulator was satisfied with. It was not only written for the Regulator but also for the project in itself and for governing of the supplier. The experiences and lesson learned from way of handling the Safety Demonstration in Twice has among other things been given input to Energifork's reports e.g. ref.[4].

It is of great importance that prerequisites are in place when starting the project and the expectations are clear for all included parties. Example of important prerequisites:

- Determine a Configuration management strategy and structure. Define the product structure and the hierarchy with its associate documentation early. (Preferable before the project starts, or during the conceptual design.)
- Ensure the QMS is up to date and includes instructions for e.g Configuration Management, Verification and Validation, a project governing and management model
- The level and purpose with reviews during the project must be agreed on between all parties, internally at the licensee, with the supplier and with the Regulator
- Clarify for all involved parties that the review is not primarily of the documents but of the safety case in total. Adapt the review process for the project's needs.
- Establish a licensing process at the licensee and appoint an ownership for the process and for the licensing per modification.

7.2.4 The licensee's important issues and reflections

Without the PSADP/PSADR, Ringhals 2 would not have been able to license the plant after project Twice.

The PSADP/PSADR included a safety demonstration which did not only focus at the product (the computerized platform) but also at the development process, organisation and required competence.

The insight that the supplier didn't have an up to date knowledge of the current state of the plant came during the project. Ringhals enforced the Westinghouse staff with their own project members to handle this shortage. A traditionally functional procurement is not to recommend for this type of project.

7.3 THE PROJECTS R1-RPS AND R1-SP2

The projects started: 2003 and ended in 2010.

More or less in parallel to Twice the projects RPS and SP2 was performed at R1 with the task to improve and diversify the RPS functionality. The background was similar with the other reactors need of modernization especially in respect of separation. A sister project to Twcie, called the Once project was planned for R1

with a similar scope as Twice, but when it was time for purchase of Once, Twice had run in to a lot of struggles e.g lack of current documentation for the plant. Due to that, Vattenfall didn't want to have another project in same scale running at the plant at same time and didn't approve a start of the Once project at R1. Instead R1 generated a first transition plan where the total need of modernization was divided in to several projects to be run in sequence at the plant, where the total scope of them all would solve the need for safety improvements. The largest project in the transition plan was the RPS project together with the parallel sister project SP2. The main focus for RPS moved from maintenance issues to pure safety related improvements. The first edition of the transition plan was released 2000-2001

For the RPS/SP2 projects, Ringhals chose Areva as supplier and introduced an Alliance concept for performance of the project. The Alliance concept meant that there was no traditional split between customer and supplier as in a functional procurement. Instead the design work and V&V were made according to a project developed Alliance Quality management system (QMS) in Ringhals regime, where the supplier was acting at different potions where they could contribute. The project was organized according to the development process, Plant design, System design and Detailed design. The programming, FAT and platform validation was made at the supplier's facility and according to their QMS but all other design (Plant/System design) and plant V&V activities were performed according to the Alliance QMS. In this way, a good cooperation between the supplier and the customer was obtained.

7.3.1 Scope for RPS/SP2:

The basic principle of the new RPS concept was to provide two physically and functionally separated "islands". Each shall cope with events requiring separation (e.g. fire, earthquake or CCF) considering loss of the other "island" as a consequence of the event.

The two parts of the new RPS system was:

- OPS (Original Plant Section). The existing part of the reactor protection system, which remained in principle unchanged
- DPS (Diversified Plant Section). A new part of the reactor protection system to cope with events including loss of OPS. Implemented in TXS.

The tasks were divided into two "sister projects", RPS and SP2 which was implemented in parallel with a unified installation and plant validation.

The RPS project implemented Reactivity Control, RCPB Integrity and Core Cooling in the DPS.

The task for SP2 (Safety Package) was to modernize the Containment Heat Removal by the cooling chains (322-711-715) and the associated power supply functions. SP2 was also responsible for providing emergency power supply with two new Diesel Generator sets.

The used platform was TXS which already was qualified by TÜF according IEC 60880.

7.3.2 Project Performance

The conceptual solution with an add-on to the existing plant with a computerized platform which is completely separated from the old plant was a robust solution which both Vattenfall and SKI liked. Focus moved from the I&C solution towards the process concept. R1 was presenting the conceptual solution, the safety demonstration and progress reports for SKI at approx. 15 times over the years for the project.

RPS was performed according to a project unique QMS where IEC 61513 and IEC 60880 were interpreted and applied to. The QMS included an extensive requirements development procedure with an associated verification and validation strategy following the V-model. SKI performed an audit before the project started the installation in the plant where the progress according to the QMS was accounted for. V&V reports were written in accordance to each project millstone accounting for the phase result which was presented to the Regulator. In the end of the project the complete Validation of both the computerized system as well as the complete plant was reported separately as a complement to the SAR.

7.3.3 The Regulator review

Ringhals presented early for SKI the chosen solution, which didn't include any modifications of the original reactor protection system (RPS) and with the additional system (DPS) totally stand-alone in its own separate building. SKI/SSM was mainly interested in the process changes and how to fulfil the requirements. SKI was also positive to the alliance model.

As the project was ongoing at the same period as the R2-Twice project, it was decided that the assessment of the new I&C system should be limited. The decision was to perform an assessment to get answer of two questions:

- Is there a development process that clearly specifies what V&V activities that shall be performed in the development stages and between the different phases?
- Is there an overall V&V strategy that controls the bigger activities?

The assessment was performed by meetings and review of a couple of documents:

- "R1 RPS Alliance – Document Review and Approval Principles" specify the principles for review and approval.
- "Overall specification – Overall system specification – I&C, electrical and mechanical systems, Baseline 2.3" specify generic solutions and interfaces between different systems. Includes couplings between chapters in IEC 61513 on requirements, system architecture and the use of developments tools.
- "Project Manual – Alliance Process Model" describes the development process, management, documentation etc. Is in two parts; Quality system and a more technical part with couplings to IEC 61513.
- "R1 RPS Alliance – V&V Strategy". This document is a high level document on V&V planning. It is divided in two parts: Equipment (TXS) and Functions (the application)

- "R1 RPS Alliance – Quality Management – V&V plan OPS/DPS Delivery within RPS". For each of the 12 milestones states the input, the purpose, used method and the documented result. It also states what type of documents (design and/or V&V document) that shall be produced, who is responsible, who approves and who is publisher.

This project differs from the others since not all safety functions were placed in the computerized platform. The TXS was an add-on to the existing analogue system which gave a lower safety risk for the project.

In the first presentation that Ringhals made regarding RPS, a safety demonstration plan including the V-model for validation of both the computerized system as well as the complete plant was presented. This was made on licensee's own initiative without any demands from SKI since R1 was aware of the discussions on-going at R2.

Conclusion

- The concept with an isolated I&C system lead to a much lesser complexity of the review
- The Alliance model that minimized errors in the mutual understanding between Ringhals-Supplier lead to a higher confidence that all important issues were covered. The use of a common QMS gave the Regulator a better overview of the total performance of quality assurance.
- The adaptation of the project QMS to the standards IEC 61513 and IEC 60880 gave confidence in the work processes

7.3.4 The licensee's perspective of the dialog and performance

Ringhals got an early acceptance for the chosen solution by the Regulator. SKI/SSM was mainly interested in the process changes and the I&C solution became secondary due the chosen solution with a stand-alone system.

The choice to run the project as an Alliance was a success factor which saved the project from a lot of responsibility issues between the supplier and Ringhals.

7.3.5 The licensee's important issues and reflections

- The chosen architecture of both the plant and for the computerized system has huge impact of the complexity of the safety case. Keep it simple and it will also be easy to review and communicate the safety impact.
- The Plant level design must be completed before the system design starts. When system design starts it involves a factor 10 in number of designers. If the plant design is not completed, the plant level designers will need to spend a lot of time to answer questions from all system designers. The project will slow down and the plant designer will not have time to finish the plant level design. Sooner or later the project will need to stop to catch up
- Modifications of the control systems structure will have a strong impact of the safety analysis. The conceptual solution could have a costly impact of the project. Sometime it can be worth to keep a proven design concept even if it will lead to more and expensive control equipment.

7.4 PROJECT O2-PLEX

Plex started 2004 and ended in 2015

The Plex project at O2 is the latest project to install a computerized I&C platform in Sweden (at this date and probably the last in Sweden). The pre-study for the project started in 2004 but the actual project start was in 2006. The project was on-going with the installations in the plant when the decision to terminate the plant was taken. The plant was never taken back in to operation and the project ended in 2015.

The choice of supplier was Areva and the used platform was TXS. Compared with R1, which also used the TXS platform, OKG chose to include the complete RPS (all safety functions) into the platform, which gave a more complex solution. A part from including the RPS in the platform, the Plex project also implemented modifications of the control room, of the process functionality and an increase of the electrical power out from the plant. This gives the far most complex project of all implemented in Sweden and there were a lot of challenges during the project. The final result was however not seen since the plant was never taken back into operation with the implemented modifications

Plex was performed in a traditional supplier/customer project.

7.4.1 Scope for Plex:

The scope included a new safety concept including a computerized I&C platform for the safety systems and modernization of the control room. Furthermore, a new turbine was installed to increase the electrical power out from the plant. Almost the complete plant was modernized.

Safety Functions:

Reactor Protection System (RPS) and DPS (Diverse Protection System)

Non Safety Functions

Operation and service functions were included.

7.4.2 Project Performance

In the end of September 2006 Bo had an informal meeting with the I&C specialist at OKG, and it was discussed that the safety demonstration for the new I&C would follow the basic concept of the R2-TWICE project. There were no formal agreements on the safety demonstration plan just information.

In 2007, OKG sent an “early notification” to SKI, covering the total modernisation including the power upgrade. SKI respond was a request for a formal “Independent Internal Review” from the licensee. After that the different technical issues (e.g. Digital I&C, New Control Room, New Separation) was reviewed separately at the Regulator with very little coordination between the reviewers.

In a discussion between Bo and the OKG I&C expert in late 2009, it was discovered that the planned safety demonstration will not be performed. The management of

the project had planned to use the structure of safety demonstration for I&C on the whole project. After some time the management realised that at this late time of the project it was impossible to perform such extensive demonstration. Since it was not required in SSM's regulation, the extensive demonstration plan was postponed. For the new I&C OKG therefor used the traditional qualification structure, with the top documentation K60 with the more detailed documents K40, see Figure 3

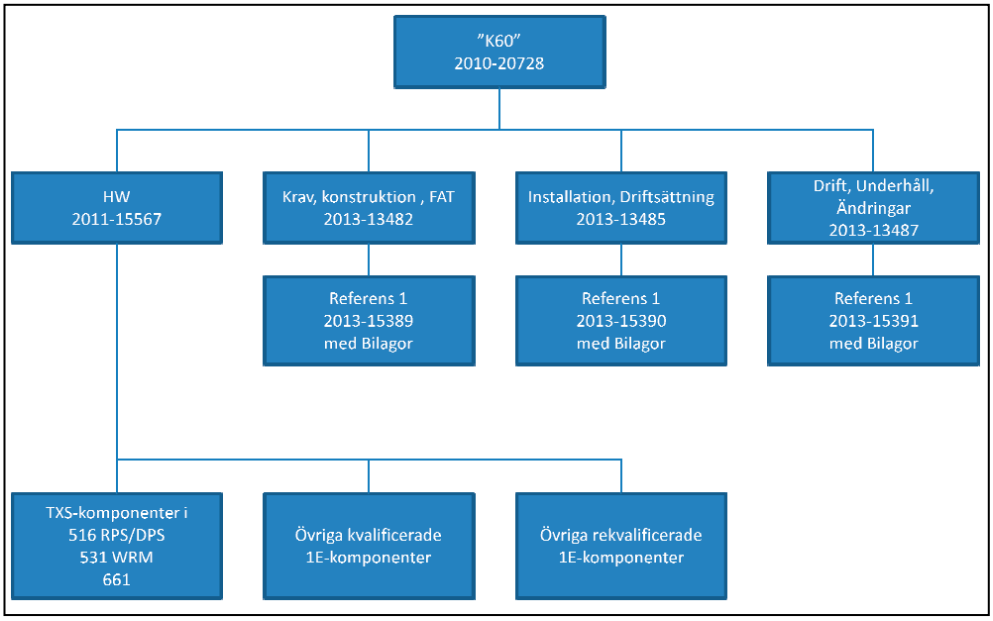


Figure 3: The qualification document structure

In January 2010 Bo open a review errand and a meeting between SSM and the Plex project was performed, the topic was regarding computerized I&C and a meeting plan for discussions regarding this subject was established.

The extended summarizing qualification report was called K60. This report didn't give the overview of the complete plant modification, how the quality assurance was supposed be performed and it was hard for SSM to get the big picture. The qualification report included only the modifications made in RPS/DPS and this was not enough for the Regulator. A report including a complete evaluation of the plant with the impact of all the 1E equipment was required by SSM.

SSM would like to have a presentation which included the complete design process which was not obvious according to the presentation and material received from the licensee. SSM would like part-reports presenting the progress during the project, which was performed within the planned series of meetings.

This was the most complex project which SSM had reviewed since the scope was so extensive, including a computerized I&C system for the safety systems, modification of the control room and modifications of process functions. Regarding the issue of the new computerized safety system, SSM felt that the presented accounting was not in party with the complexity of the project. The management at OKG didn't recognize the severity and didn't support the project in its need for presenting a coherent accounting apart from SAR.

Another difference between Plex and the other project was the collaboration with the supplier. R1-RPS had an alliance arrangement with Areva from the beginning and both R2-Twice and O1-Mod turned into a close collaboration between customer and supplier during the project. Plex on the other hand was performed in a traditional customer/ supplier relation, which was not beneficial from a transparency point of view.

7.4.3 The Regulator review

Compared to the previous projects (O1-Mod, R2-TWICE, R1- RPS/SP2), for O2 PLEX there were no analyst acting as the single point of contact at Regulator over the years, who had the total overview of the Plex project. The total scope of the review at the Regulator was spread out on different review projects, where the digital I&C was only one part.

The main issues discussed, were the structure and content of the high level qualification report, K60, and the separation between 1E and 2E, via the Gateway. The Gateway (2E) sends four types of telegram in to the TXS (1E) showing the status of the 2E part. If the TXS did not get the status of the 2E part an alarm was sent to the Main Control Room, but it was a communication from 2E into 1E. These two issues were discussed very much during the review period and resulted in an expanded content of the qualification report and a re-design where it became impossible to have signals from 2E into 1E. The signals for the status of 2E were instead simulated within the TXS (1E)

The regular meetings between O2 PLEX (and sometimes with the supplier) and SSM during the performance of the project was very good and gave a good insight of the different activities within the project

Conclusion

- It took a long time before SKI/SSM got a real insight of the project including the strategy for Safety Demonstration
- It was a long discussion of the scope and content of the qualification reports but at the end the Regulator was satisfied.
- The separation between 1E and 2E was also an important issue which lead to a re-design of the solution with a physical impossibility to communicate from 2E into 1E., by taking away the signal cable that could send signals from Gateway into TXS (1E)
- When the meeting series started in January 2010 it worked well with a clear structure and content covering all important issues, which gave the Regulator a good insight of both technical issues and work processes.
- It is important to have a single entry port at the Regulator that has the total overview.

7.4.4 The licensee's perspective of the dialog and performance

In both O1-Mod and Plex there were an uncertainties of the format, the formal relation to the SAR and the content level of the safety demonstration plan which lead to a lot of discussions and re-structuring of the format of the K60 report before approval. Plex was a much larger and complex project, in conjunction with general

development & improvement of computerized systems, it, lead to other focus areas compared with O1-Mod e.g. was the question regarding Cyber-security new. Cyber-security is an example of a requirement which occurs in the middle of the project which affects the project performance.

7.4.5 The licensee's important issues and reflections

As described in 6.1 the technology development of computerized systems had taken a great step between O1-Mod and Plex. These technical changes resulted in new and tougher requirement on accounting, traceability and V&V from standards and regulations.

TXS was qualified during the 90', in accordance with the document structure that was used in KTA (the German Guides for nuclear plants) at that time. The Qualification has since then been updated with new information, but within the same document structure. The KTA document structure doesn't match the Swedish licensing structure. This had an impact of the expectation on the accounting from Plex which differed from O1-Mod and also led also a lot of discussion with the supplier. Due to that, it would be more sufficient if the supplier delivers the assessment results and the licensee places the information in a structure that is applicable for the safety justification

These types of projects are so complex and thing needs to be verified during the development and design processes. All plants are unique and so are all projects. Equipment qualified and used for one specific NPP can't automatically be re-used at another plant without a thoroughly evaluation of the consequences, even if the usage seams similar. Each projects specific needs are unique and the extent of the safety demonstration, requirement management, V&V etc need to be evaluated case by case The Regulator needs due to that to be involved when these activities are planned and performed and not in the end of the project. A safety demonstration is a case by case activity.

8 Special areas of interest

8.1 ACCOUNTING

This chapter describes the different ways the safety impact of the plant was accounted for in the different projects.

The Regulator gives permission for an implementation and re-start after commissioning but they never approves a product such as the usage of a specific platform. It is the licensee's responsibility to guarantee a safe plant and to perform all required measures to prove fulfilment of the requirements and regulations. Due to that, the accounting must reflect how requirements management and V&V are performed to convince the Regulator that the plant is validated and safe. For projects including a computerized platform, where the whole or parts of the safety functions are implemented, it is not enough or convincing to only produce a SAR, what type depends on which phase the project is in (see chapter 5,3). Standards, research projects and experience point at the need of some type of quality plan, controlled design process, continuously follow-up and reporting, see examples in ref [1] [7], [8] and [9]. Due to that, the projects in this report all provided some kind of extended reporting besides the SAR.

As a minimum for all projects in this report the accounting consist of a plan, progress reports and a final report accounting for how the complete plant shall be verified and validated. It is not enough to only focus at the computerized system; the impact of the complete plant must be evaluated and accounted for. The used nomenclature, format and scope differ between the projects but the basic principles are the same. The maturity of each licensee's QMS, organization and available knowledgeable resources at the time has an impact of the required extent of the Safety demonstration plan and reports.

O1-Mod had a very clear document structure which made it easy to understand the purpose and level of each document.

R2-Twice- which was the next project to start after O1-Mod had a clear and more extensive Safety demonstration plan, compared with O1-Mod. It included a Total Safety case (TSC) with 14 Safety subject areas which were accounted for during the project.

R1-RPS/SP2 –was organized in an alliance model together with the supplier which was a key to success in terms of cooperation and transparency which was reflected in the reporting. Their Safety demonstration plan included a Validation strategy for the complete plant, not only the computerized system.

O2-Plex started with a plan for the licensing of the digital I&C reactor protection to use a safety demonstration plan that corresponded with one used for R2 TWICE. At a later stage the O2-Plex project considered to use the safety demonstration plan for the whole modernisation. The project management realised that to use the safety demonstration principal, it would be impossible to use that for the whole project. As it was not required by SSM regulation it was postponed for the whole project, including the digital I&C safety system. OKG used their traditional

equipment licensing structure that caused a lot of discussion in the meetings between O2-Plex and SSM, on the structure and content of the different reports.

All projects report that they experienced an uncertainty regarding the Regulator's expectation regarding the content and ambition level of the Safety demonstration. Furthermore, the relation between the Safety demonstration and SAR was not clarified and how the safety demonstration should be used in the SAR review. The relationship between the two types of accounting needs to be clarified by the Regulator if this is a way of working for the future.

8.1.1 Safety Demonstration and Safety Case

The usage of these two terms varies between the NPP's and there was no unified definition used or common interpretation made at the time for these projects. Today, there are several reports, guidelines and experience written on the subject. Most of them are from UK, as they have been using Safety Cases in all areas of the society. Some examples are:

- Office of Nuclear Regulation has published a guide (ONR, "The purpose, scope, and content of safety cases", NS-TAST-GD-051 Revision 4, 2016), ref. [14].
- The UK Nuclear Safety Case Forum Guide "Right First Time Safety Cases: How To Write a Usable Safety Case". In the "Safety Case Forum" are representatives from several companies and organisations, such as: EdF Energy, Imperial Collage London, and Ministry of Defence. In the introduction, they have also taken up criticism on how a safety case should not be used:
  - × The Safety Case regime has lost its way. It has led to a culture of 'paper safety' at the expense of real safety.'
  - × In reality, findings presented in 'The Nimrod Review' with respect to the Nimrod Safety Case may be just as applicable to other Safety Cases in other industries.

The Nimrod accident was a flight crash that was very deep investigated and the result very applicable to other industries with high safety requirements.

This is a direct quote from the report "The loss of RAF Nimrod xv230 - a failure of leadership, culture and priorities", undertaken by Charles Haddon-Cave QC. (ref:https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/229037/1025.pdf)

The UK Nuclear Industry Guide to "Peer Review of Safety Cases", published by "Nuclear Industry Safety Directors Forum (SDF), ref. [15] .The purpose of an Independent Peer Review is to review the safety arguments within a safety submission in order to both affirm the positive aspects and to identify weaknesses, errors or omissions, particularly those which could lead to a dangerous condition. (https://www.nuclearinst.com/write/MediaUploads/SDF%20documents/Safety%20Case/Peer_Review_of_Safety_Cases.pdf)

Due to the recommendations from e.g UK nuclear industry, as mentioned above, it is always important to evaluate the extent of the Safety Demonstration in relation

to the current project scope and its safety case. Before the start of a new modernization project or new build of a plant, including computerized system it is recommended to evaluate the maturity of the licensee's current QMS, how e.g. the design process including the V&V process is defined and how life cycle management is handled. If the existing process for e.g. "Requirements management & development" is weak or not fully implemented at the NPP, the project needs to take actions to solve the lacks. The safety demonstration plan needs then to be more extensive to make sure these aspects are handled within the project compared with a mature organisational and QMS.

Another lessons learned from the implemented projects is the importance of commitment from the top management team to the Safety demonstration. The projects are often running over long time, and the case also includes a life cycle perspective which needs to be kept when the plant is back into operation. This requires endurance from the management team and the plant staff.

As described in this chapter, a Safety Demonstration can not only focus at the technology aspects and the current QMS. It also needs to take in to account aspects as for example organization structure, available knowledgeable resources and culture behaviour at the plant. The recommendation from this report is to establish a checklist where the maturity level of different aspects are evaluated before the project starts to settle the content and extent level of the Safety Demonstration, se chapter 9.5 for an example of a checklist.

A further reflection is the yearly outage perspective. All the projects included in this report are large enough to manage the complete outage the year when the main parts were installed in the plant. The safety case, which is written for the project, then comprises more or less all modifications implemented in the plant that year. However, a "normal" year the modifications to be implemented in the plant often are divided in to several autonomous projects and in different maintenance activities with their own specific scope of modification. Even if the physical modification during outage is manage by one team, the responsibility for the modifications is divided into several parties with their own safety case. Due to that, is recommended to consider if there is a need for a cohesive accounting for all implemented modifications of the plant per year, to ensure validated state of the plant after commissioning. If the plant has installed a computerized platform, this is even more critical since the functional modifications are then divided on several parties which all affect the need for modifications in the platform. It is recommended to appoint one project or organisation part that has the total responsibility to compile and perform all modifications of the computerized I&C platform and to perform the system validation. A safety case needs then to be established for this activity/project as well as for the plant changing projects.

8.2 IMPACT ON THE REGUALATIONS, SKIFS AND SSMFS

The SKI/SSM's regulations were updated in 2004 and in 2008. No specific requirements regarding how to handle computerized systems or the required report structure for these types of systems were added in those revisions. However, a reference to the research work performed by the Task Force of

Regulators in Europe in which SKI/SSM participated, "Common position about licensing safety critical software" reference EUR 19265 ref[7], was added. A more comprehensive update of the regulations is on-going One suggested change in the regulation is to, with a graded approach, introduce the concept of Safety Demonstration (meaning a systematic approach to provide the arguments and evidence that a modification will support the overall safety of the facility or activity)for all modifications (also e.g. organisational changes) in the NPP's.

8.3 POST-PROJECTS AND FUTURE ANALYSIS

In this chapter the licensees and the Regulator are describing their lessons learned gained from the implemented projects, operational experiences and their plan forward.

Both Ringhals and OKG implemented most of their modernization needs until 2015. The amount and size of the current projects at the three sites in Sweden has reduced. None of the planned or on-going major projects are installing computerized I&C for safety functions.

Ringhals:

The operation of computerized system has worked well, they are stable. Both R1-RPS and R2-Twice contributed to updates and modernisation of Ringhals Quality Management System which was adapted to handle projects including programmable equipment.

When performing modifications of the plant, Ringhals has chosen to perform most of the design by themselves and to involve suppliers first in the detailed design (component level) and for purchased equipment. This requires a QMS to support the complete design and V&V process to be performed in-house. This differs from OKG who normally are purchasing functional deliveries from the suppliers, where the supplier is performing most of the design.

Ringhals has chosen per revision and plant, to dedicate the responsibility of all modifications of the computerized platform to one project, (or if the change need is limited, it is performed by the responsible line organisation). All other projects and planned maintenance activities need to interact with this platform project. How to organize the projects and settle their scope in a smart way is a challenge when the plant is equipped with a computerized platform including a lot of the functions cross the plant systems.

There is no plan to install more computerized platforms at least not for safety functions at Ringhals.

OKG:

The operational experience at O1 has been good after O1-Mod with few problems in the equipment. O2 was never taken into operation so no operational experience was made. At this date, both O1 and O2 have been taken out of operation due to other reasons.

The lesson learned from the implemented projects is that the required V&V activities are very extensive for computerized systems, especially when safety functions are implemented. Due to that, the usage of computerized systems will be limited preferably to be used as stand-alone equipment and only for operational functions. At OKG , O3 is still in operation and the plan forward for the plant is to continue with analogue equipment and change the circuit boards successively.

In relation to Plex a lot of new requirements turned up which was not in the same focus for the earlier project, one example is Cyber-security which is something all plants need to take into consideration for the future.

OKG is participating in a development of new provisions for HDL-technology and the usage of it, together with Ringhals and Forsmark. In the future this technology is something that might be relevant for O3 to use.

SSM:

As described in the chapter 8.2, the Regulator is working with a new release of the regulation. Since O1 and O2 are taken out of operation and Vattenfall's plan is to close down R1 and R2 in coming years, the total need and amount of projects has gone down at the NPP's which also leads to a new situation for the Regulator. This will affect the Regulator's plan and way of working for the coming years.

SSM is part of Energiforsk and are sponsoring the research projects to be performed by them. SSM is also participating in the international cooperation "Task Force-safety critical software", which recently released a new revision of , "Licensing of safety critical software for nuclear reactors", ref. [7]. SSM is also participating in a Working Group on Digital Instrumentation and Control (WGDIC) within NEAs Committee on Nuclear Regulator Activities (CNRA).

8.3.1 Summary

- The systems are stable, no severe problems since installation.
- The challenge for computerized I&C platforms in the life cycle perspective is the maintenance and changes of the HW, the base SW and application SW. The development pace in the computer field is making the HW and SW obsolete soon after installation. Even if just a small update is required, the licensee can be forced to modify both HW and base SW due to non-compatibility of the updates with the older versions. This is costly, time consuming and requires a risk evaluation of the safety system.
- A cohesive platform requires a dedicated project which performs all required modifications of the computerized system per outage year. All other projects and maintenance activities need to report their need of modification to this dedicated project (or to the line organisation responsible for the platform).
- The total amount of projects to be implemented during an outage year needs to be thoroughly planned for. An evaluation of the total impact of the plant needs to be accounted for. It must be possible to prove validated state of the complete plant after the outage. This is nothing new but the need is more obvious with a computerized platform. Consider how the total sum of all safety demonstrations shall be accounted for.

- Cyber-security is one important aspect to investigate further for the future. It might be an area of interest for Energiforsk to start a study within.
- Assurance of relevant competence over time is another critical area for the future. How to recruit and keep the competence over time. This is applicable for all technical fields but it is especially a problem for the computerized systems since the development pace is so fast.
- Participation in research programs:
  - Vattenfall, OKG and SSM are participating in a limited amount of research programs. It is mainly contributions via Energiforsk.
  - SSM is participating in the "Task Force-safety critical software", see section 6.2.3.

9 Conclusions

This chapter includes a summary of conclusions based at the information accounted for in chapter 5 to 8 but it is also extended with a summary of reflections from Bo Liwång and the project representatives discussed at the performed workshop. The answers to the research questions to be covered by the report (see chapter 1.2) are included in one or several chapters but the conclusions are not organized after them.

9.1 GENERAL

Design and implementation of computerized I&C cannot be verified in the end of a project. A documented design process and a stepwise verification approach is necessary to quality assure these type of systems. Due to that, all relevant standards are written in a way where they recommend a stepwise development approach where each step is accounted for along with the development as discussed in chapter 8.1. (The performance of the development process can be agile or iterative but all steps must be performed and all verification activities can't be made in the end)

Since most industries today are using and are dependent of computerized I&C systems, the need for some kind of safety demonstration is discussed in most industry developing products where a functional safety is required. For example was the standard ISO 26262-"Functional Safety for road vehicles "released in 2012 which put high and new demands on the automotive industry. ISO 26262 is an adaptation of IEC 61508,[10],and to this standard family the nuclear standard IEC 61513 [9] also belong. The trend is that a risk based approach to evaluate potential hazards and events, which has been required in the nuclear industry for a long time, is spreading. These standards also require traceability and a structured V&V approach during the complete life cycle of the product. In the end, all these requirements lead to a need of some kind of safety demonstration which is continuously accounted for during the project and also continues over the life cycle for the product or plant. The bottom line is, it is not possible to write a technical description in the end, which someone outside the project can grasp, review or follow in a way that can quality assure a new or updated product including computerized I&C. Especially not, when used for safety functions.

9.2 PREREQUISTES AND PREPARATION

During the 90's when the need for modernization of the plants accounted for in this report was evaluated, the era of computerized system had just started. The computer industry has made a great evolution from the 90's until today. The development is still fast but the knowledge regarding the systems behaviour, the risks and the advantages of them are much more spread in the society in large today. When these large modernization projects started, both the licensee's and the Regulator were to some extent pioneers when it comes to use computerized systems for safety functions. When O1-Mod started 1998, the guidance to support and give direction was mainly from the standard IEC 60880 [8], reports from the

Halden projects ref[1], the work within TC-SCS (see chapter 6.2.3) and standards from other industries such as IEC 61508 [10] and findings made in international studies from other industries.

Furthermore gave the reports and preparation work at the Regulator and the licensee's in front of the Millennium,(Y2K), a starting point for the scope and type of accounting to request from the licensee.

Even so, since there was to paragraph stating any extended accounting in the regulation, the expectations and ambition of the accounting was an uncertainty for the licensee s in all the projects, see the licensee's perspective in chapter 7.

If a project with the task to implement a computerized I&C system would start today, the support and guidance is much more developed. The expectations are clearer in the standards. However, there is no common definition for what a safety demonstration shall include. For example there is a new report from TF-SCS (see chapter 6.2.3) which includes recommendations but there is still no agreement between the Regulator and the licensees. The recommendation from this report is to agree on definitions, scope and ambition level of the accounting before a new project is started. This agreement must include all parties of the project; the Regulator, the licensees and the Suppliers.

The knowledge achieved in the beginning of the 90's, was used as the basis for the way of working and how to communicate between the licensee's and the authorities in the coming projects which were implemented from the late 90's until 2015.

These milestones lay the ground for the Regulator to start requiring a safety demonstration plan from the projects:

- The Halden-program help out with the knowledge regarding the importance of getting involved early and to continuously follow the development process
- The REPAC project became a role model for how communication during a project shall be performed and established a way of working.
- The Millennium report (Y2K) for the government gave a structured way of working with planning and reporting of modifications involving computerized equipment.
- The European cooperation lead to the insight of the need for a Safety demonstration plan

9.3 PREREQUISITES IN FORM OF TECHNICAL PLANNING AND CONCEPTUAL CHOICES

The chosen conceptual solution for modernization of a power plant must be transparent, graspable and easy to follow to get an acceptance for the safety concept and limit the extent of the V&V activities. This comprises all type of large modifications but are especially important when a computerized I&C system shall be used. Project portfolio management, where the technical planning, scoping of the projects and conceptual choices are made, has a huge impact of the licensing journey to come. The better the licensee is to generate a transparent technical

concept which is graspable, where the risks can be understood for all parties outside the project the easier licencing journey.

R1 chose to inforce the RPS-function with an add-on which limited the need of re-design of the existing functions. The I&C platform became a stand-alone equipment with no connections to the original plant. These early choices had a large impact of the acceptance from the Regulator, see section 7.3. Furthermore, R1 choose to split the total modernization need into several projects to be implemented over time instead of creating one large project. After the RPS/SP2-projects, a lot of minor projects followed, which were kept together by a program, to complete the total modernization task. These conceptual choices, the architecture and the split into several projects have served R1 well. The conclusion is to keep it as simple as possible. Don't add more tasks to a project than necessary, and don't include more functions than necessary into the I&C platform. Avoid, "nice to have" functions.

Furthermore, when a computerized I&C platform is installed and taken into operation, it gives the project portfolio management an additional dimension to plan for. It is of the outermost importance to plan for how modifications of the I&C platform shall be performed and by whom. The interfaces between the projects, planned maintenance activities and the I&C platform must be mapped and taken into account see chapter 8.

The chosen architecture of both the plant and for the computerized system has huge impact of the complexity of the safety case, e.g it is hard to prove full separation if all functionality is put in to the same CPU. Keep it simple and it will also be easy to review and communicate the safety impact.

All the licensees would like to emphasize the great importance that prerequisites are in place when starting the project and the expectations are clear for all included parties. Here follow some examples which are obtained lessons learned from Twice:

- Determine a Configuration management strategy and structure. Define the product structure and the hierarchy with its associate documentation early. (Preferable before the project starts, or during the conceptual design.)
- Ensure the QMS is up to date and includes instructions for e.g Configuration Management, Verification and Validation, a project governing and management model
- The level and purpose with reviews during the project must be agreed on between all parties, both internally at the licensee, with the supplier and with the Regulator
- Clarify for all involved parties that the review is not primarily of the documents but of the safety case in total. Adapt the review process for the project's needs.
- Establish a licensing process at the NPP and appoint an ownership for the process and for the licensing per modification.

9.4 PROJECT PERFORMANCE AND THE REGULATOR REVIEW

In the beginning of a project it is necessary that the Regulator and the licensee needs to agree on a safety demonstration plan and how it shall be followed-up on. All the licensees reported that there was an uncertainty regarding the expectation of the content and depth of the reports through the project, see chapter 7 and 8.1.

These large modernisations projects are complex and are due to that engaging a lot of different competences at the NPP as well as at the Regulator. One lesson learned is that the communication, follow-up and the Regulator review are facilitated if there is an appointed analyst who are acting as an internal project manager for the project also at the Regulator, who is keeping the complete review case together, see lessons learned from Plex chapter 7.4.3.

The Regulator must initiate the review process already from the beginning of the project. It is not possible to understand the full concept and the project journey only by reading the Safety Analysis report in the end.

The licensees also request that the Regulator must be able to express a verdict about the concept and chosen solutions along with the project. Of traditional principles the Regulator doesn't express any verdict until the complete modification and solution is presented which is right before the start of the installation in the plant. This is too late, especially when installing computerized I&C.

The contractual agreements and the way of working with the supplier involved in this type of project have impact of the transparency and cooperation climate. R1 performed their project in an Alliance concept and both O1-Mod and Twice turned into a more cooperative mode with the supplier during the project. The reason is that traditional functional procurement is more or less impossible when extensive modifications shall be implemented in an old plant. There are too much room for uncertainties and interpretations. The suppliers have too little knowledge about the current status of the plant and the licensee has too little knowledge about the latest technology. Due to that, some kind of cooperation agreement where both parties shares the risk is to prefer. A quote from Anders Johansson is worth to remember, "Independent of how good the procurement department at the licensee is at creating a solid contract, it is not possible to buy something no one can deliver"

Apart from the technical concept, there are three areas which all need to be treated equally to balance the project (or a complete company):

- Mature and updated Quality management system
- Available competences with relevant up to date knowledge and experiences
- Maturity of the organisation, management and culture behaviour

All three areas need to be up to date and ready for the tasks. This is why a Safety Demonstration plan not only can focus on the technical concept, it needs to cover other dimensions as well and it includes all involved parties, the Licensee, the Regulator and the suppliers.

Here follows the general conclusion from the Regulator review per project:

Conclusion O1-Mod

- the documentation structure worked well
- the regular meetings between the involved parties (OKG, (OKG, ABB Atom (Westinghouse) and Framatom ANP (Areva)) insured that all important issues were covered
- The meetings with the Regulator from early in the project made it possible for the Regulator to follow the development process
- The respond from OKG on the four questions gives insights on the argumentations for that requirements were fulfilled

Conclusion R2-Twice

- PSADP/PSADR with its clear structure was very good
- The objectives defined in PSADP/PSADR gave a clear overview of the purpose
- The regularly performed meetings on high level strategies and detailed performance together with presentation of used tools gave the Regulator a good insight of the project performance
- The visual presentation of the suppliers way of working with e.g Configuration Management gave the Regulator a better understanding of the documentation

Conclusion R1-RPS/SP2

- The concept with an isolated I&C system lead to a much lesser complexity of the review
- The Alliance model that minimized errors in the mutual understanding between Ringhals-Supplier lead to a higher confidence that all important issues were covered. The use of a common QMS gave the Regulator a better overview of the total performance of quality assurance.
- The adaptation of the project QMS to the standards IEC 61513 [9] and IEC 60880 [8] gave confidence in the work processes

Conclusion O2-Plex

- It took long time before SKI/SSM got a real insight of the project including the strategy for Safety Demonstration
- It was a long discussion of the scope and content of the qualification reports but at the end the regulator was satisfied.
- The separation between 1E and 2E was also an important issue which lead to a re-design of the solution with a physical impossibility to communicate from 2E into 1E., by taking away the signal cable that could send signals from Gateway into TXS (1E)
- When the meeting series started in January 2010 it worked well with a clear structure and content covering all important issues, which gave the Regulator a good insight of both technical issues and work processes.
- It is important to have a single entry port at the Regulator that has the total view.

9.5 ACCOUNTING

As describe in the introduction of this chapter, it is not possible to verify the result in the end, there must be a proper analysis and plan in the beginning of an implementation project which is accounted for continuously through the project. This is also a "golden rule" for the design of computerized systems in general which is described in most used standards today, e.g. IEC 61513 [9]. The technical requirements need to be developed and followed up on continuously during the development process which has led to the use of the V-model for V&V in many projects.

All interviewed parties for this report agree on that some kind of Safety Demonstration is required when installing a computerized I&C system.

The Safety Demonstration must be adapted to the current project. There is a difference between the projects in this report. O1-Mod is the only project where the full qualification of the equipment was included which settled a natural qualification focus in the safety demonstration. The other projects used an already qualified platform as the basis. Twice had the most comprehensive Safety demonstration with its 14 Safety Subject Areas which served them well in the licensing process of the complex project. Furthermore was the Safety demonstration in Twice a need for communication and quality assurance of the supplier.

The conclusion from the interviews and workshop made for this report regarding Safety demonstration is summarized below:

9.5.1 Safety Demonstration

The safety demonstration is necessary due to:

- A computerized I&C system needs to be verified and accounted for continuously during the development process and not in the end of the project.
- A computerized I&C system require a life cycle approach which does not end with the project.
- The purpose is to demonstrate for the Regulator that the suggested modification of the plant is safe. It is however, as important to be used internally at the licensees, both to quality assure the safety concept within the project and to explain for those not involved in the daily work of the project
- It is necessary for the cooperation, the relationship and the understanding between the licensee and the supplier(s).
- Catchword to include in the work:
  - × Early
  - × Clear
  - × Consequent

Safety Demonstration is often discussed from a project performance perspective when the product is installed for the first time but one challenge to take into account is the yearly required modifications and updates, see 8.1.1. All the projects in this report were large enough to more or less run the complete outage but a "normal outage year" many different projects and maintenance activities are on-

going in parallel. In the end there must be some accounting for the total impact on the plant and to ensure the plant is put into "Validated state" after each year's modifications. The planning work to get a feasibly split between the projects needs to be taken into consideration. The relation to SAR must be clarified. What expectations will the Regulator have on SAR contra on a Safety demonstration? What information shall be accounted for where? Review performance?

9.5.2 Safety Demonstration checklist

The parties ought to agree on a checklist which all licensees shall go through before a project is started. The result from the checklist evaluation set the content and extent level of the Safety demonstration plan and reports. Examples of areas to be included in the checklist:

- Impact of the plant and especially the safety functions
- Size of the project
- Complexity and/or introduction of new technology defined in the suggested conceptual design
- New laws, regulations and standards to be used and implemented by the project
- Maturity of the organisation
- Available competences
- Available and feasible suppliers
- Suggested procurement set-up of the supplier
- Maturity of the Quality Management system , with respect to (but not limited to), e.g.:
  - Requirements Management
  - Verification and Validation
  - Configuration Management
  - Document Management

9.5.3 Lessons Learned from the projects

Improvement suggestion in relation to a safety demonstration, obtained as lesson learned after the projects:

- Start early with Safety Demonstration planning and agree on what and by whom the demonstration shall be performed. All parties must agree on it.
- Establish a Configuration plan early where it is clear which information that is required for each Configuration Item (CI). Collect all relevant information and verifications continuously during the project and add it directly to the plant CI (documentation for the objects in the plant. Work in copies of existing plant documents (product information) instead of generating project document. This minimizes the document handling work in the end.
- Generate a demonstration report where the author needs to motivate why the requirements are fulfilled. Focus at conclusions and the basis for the conclusion, not so much at the performed activity. It is not enough to demonstrate what has been fulfilled but also answer to the question, "what is missing".

- Consider to write the Safety Demonstration in native language, at least partly. Those parts to be communicated to the supplier must still be in English but the rest is preferably in the native languish. The reason is that the communication with the Regulator is in native languish and when someone who doesn't have English as mother language it diminishes the nuances.
- Perform active choices regarding of what to categorize as product information which need to be updated through the product life cycle and what to categorize as project information that are obsolete after the project.

10 Recommendations

This chapter includes the collected keys to success factors from the workshop and a summary of the report.

- A Safety Demonstration is necessary and its extent must be adapted to the current project's needs.
- Agree on a definition and a way of working regarding Safety demonstration between the licensees and the Regulator. Establish a checklist to be used when starting a new project.
- Clarify the relation between the Safety demonstration and SAR
- Ensure all relevant perquisites are in place before the project starts, both at the Regulator as well as at the licensees.
- Involvement by the Regulator from the start is crucial; establish an early dialog between the licensee and the Regulator. It is necessary to take part of the reports written by the project continuously, since it is very hard to grasp the complete picture in the end of the project.
- The Regulator needs to appoint an internal project manager for large project, a single point of contact for the licensee.
- With the arrangement of a safety demonstration it must be possible for the Regulator to give a verdict of the chosen concept at an early stage.
- At an early stage identify and agree upon the required information which is needed for quality assurance and licensing, involving all parties; Regulator, Licensee and Suppliers. Focus at the information not the document and documentation format.
- Include the way of working with safety demonstration as a natural part of the licensees QMS.
- Keep the concept and architecture as simple as possible.
- Appoint a dedicated line organisation to own the computerized I&C platform overtime which shall be responsible for all modifications to be implemented per year in the platform.
- Consider and plan for the complexity when several projects are performed in parallel during the same outage year.
- Adjust the supplier agreement after type of project. Avoid Functional agreement when the scope and requirements are vague.
- Recommendation for new studies due to challenges for the licensee's
  - × Cyber security
  - × How to retain competence and/or handle the lack of it.

11 References

[1]. Guideline for Reviewing Software in Safety related Systems, SKI report 94:9, 1994

[2]. SKIFS 1998:1 Statens kärnkraftinspektions författningssamling, ”Statens kärnkraftinspektions föreskrifter om säkerhet i vissa kärntekniska anläggningar”

[3]. Experience from asset management of installed safety related programmable platforms/systems in Swedish NPPs, Energiforsk report 2015:147

[4]. Safety Demonstration Planning for Digital I&C Projects, Energiforsk report 2016:267

[5]. Riksrevisionsverket “Vad kan vi lära av 2000-säkringen i staten. En granskning av myndigheternas 2000 arbete” rapport 2000:19

[6]. Safety Demonstration Plan guide, Energiforsk report 2018:512

[7]. Licensing of safety critical software for nuclear reactors, 2018:19, published by SSM.

[8]. IEC 60880 Nuclear Power Plants – Instrumentation and Control Systems Important to Safety – Software Aspects for Computer-Based Systems

[9]. IEC 61513 Nuclear power plants. Instrumentation and control important to safety

[10]. IEC 61508 Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems

[11]. IEC 61226- Nuclear power plants - Instrumentation and control important to safety - Classification of instrumentation and control functions

[12]. IEEE 603 “Standard Criteria for Safety Systems for Nuclear Power Generating Stations”

[13]. “TWICE - Plant Safety Assurance and Demonstration Plan, PSADP”, Darwin ID 1704829, Ver 10.0

[14]. Office of Nuclear Regulation has published a guide (ONR, “The purpose, scope, and content of safety cases”, NS-TAST-GD-051 Revision 4, 2016

[15]. The UK Nuclear Industry Guide to “Peer Review of Safety Cases”, published by “Nuclear Industry Safety Directors Forum (SDF),

[16]. IEC 60987 “Nuclear power plants - Instrumentation and control important to safety - Hardware design requirements for computer-based systems”

12 Appendix A: Discussion topics for the Workshop

- Conclusions and reflections from each project, the Regulator view and the licensee view
- Cooperation: Regulator-Licensee-Supplier
  - × What worked well and where were the challenges
  - × Gained experiences
  - × Recommendations
- Key to success in these type of projects
- Long-term operation with computerized I&C platforms
  - × Experiences
  - × Handling of changes over time
  - × Handling of Configuration and Documentation Management
  - × Challenges for the future operation
- Safety Demonstration
  - × Your view and experiences of it
  - × What shall be the purpose and relation to SAR
  - × What shall it contain
- Research programs and cooperation initiative
  - × What have been performed during and after the projects
  - × What would you recommend for the future

13 Appendix B

Data for the Projects

NPP	Project	Years	Platforms	Functions	Supplier	Supplier/ Customer cooperation
O1	O1-Mod	1998-2002	AC160 and AC450, (installed by O1-Mod)	CAT A, CAT B and CAT C functions in the EKB are included in AC160. The CAT B functions in the "old electrical building" are included in AC450. Some of the CAT A functions in the old building remains in analogue equipment.	Westinghouse	O1-Mod was performed as a traditional functional procurement where the supplier performed the design and OKG review it. Areva was invited to perform a review of the conceptual solution as a second opinion Westinghouse performed the qualification but is was reviewed by OKG For changes made after O1-Mod, OKG hires Westinghouse for Detailed design, system verification and consultation.
R2	Twice	1999-2010	AC160 and Ovation	All CAT A functions are included in AC160 and all CAT B functions are included in Ovation.	Westinghouse	In Twice Westinghouse did all the design work. For the modifications made in the platform after Twice, Ringhals is performing all design and verification. Westinghouse is taking part only as a review instance for critical parts of the design
R1	RPS/SP2	2003-2010	TXS	RPS is divided in to a DPS and an OPS. OPS are the old part that still is in an analogue environment. DPS is the new part and an add-on to the existing plant where the computerized platform TXS is implemented.	Areva	The RPS/SP2 was performed in an Alliance cooperation where both the supplier and the customer worked in the same QMS. RPS/SP2 performed all the design according to the Ringhals project QMS but coding, system integration and system validation was performed according to Areva QMS at their site. In the projects performed after RPS/SP2 Areva is participating and are performing the verification in the test tool SIVAT. The rest of the design and verification is performed by Ringhals.
O2	Plex	2006-2015	TXS	The complete RPS and DPS is included in TXS. TXP is used for non-safety equipment)	Areva	Traditional Customer/Supplier relation. Functional procurement. The supplier performed the design but OKG performed the safety demonstration and updates the SAR. The equipment was never taken into operation but the

IMPLEMENTING COMPUTERIZED INSTRUMENTATION AND CONTROL SYSTEMS AT SWEDISH NUCLEAR POWER PLANTS

According to today's relevant standards and research reports regarding computerized systems, a risk-based approach to evaluate potential hazards and events is recommended. These standards require traceability and a structured Verification &Validation, V&V approach during the complete life cycle of the product.

A documented design process and a stepwise V&V approach is necessary to quality assure these types of systems. When implementing computerized I&C systems, it is not possible to write a technical description in the end of a project which someone outside the project can grasp, review or follow in a way that can quality assure a new or updated product. Especially not, when used for safety functions. Due to that, these types of projects require demonstration which is continuously accounted for during the project and also continues over the life cycle for the product or plant.

Already in the beginning of the project a dialog between the Regulator and the licensee must be established, where the required information needed for quality assurance and licensing of the plant are identified and an agreement on how the accounting through the project shall be performed, must be made.

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