EXPERIENCE FROM ASSET MANAGEMENT OF INSTALLED SAFETY RELATED PROGRAMMABLE PLATFORMS/SYSTEMS IN SWEDISH NPPS

REPORT 2015:147

NUCLEAR

Energiforsk

Experience from asset management of installed safety related programmable platforms/systems in Swedish NPPs

KARIN FERM & DAVID KLAMER, SEMCON SWEDEN AB

ISBN 978-91-7673-147-5 | © 2015 ENERGIFORSK

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

Preface

Elforsk ENSRIC is a research program focused on safety related I&C systems, processes and methods in the nuclear industry. The three focus areas of the program are emerging systems, life time extension and I&C overall. Information from the program will assist the nuclear industry and the Radiation Safety Authority when analysing how to replace systems and methods - choosing a new technology or finding a way to stay with the present solution - with maintained safety and promoting a low life cycle cost.
The program is financed by Vattenfall, E.On, Fortum, TVO, Swedish Radiation Safety Authority, Skellefteå Kraft and Karlstad Energi.

The research is performed by Karin Ferm and David Klamer from Semcon Sweden AB, in close cooperation with the responsible persons from the participating NPPs, Fredrik Bengtsson (Ringhals), Roger Granath (Forsmark) and Karl-Erik Ericsson (Oskarshamn). In total, 33 persons at the three NPPs have been interviewed and are participating in the survey. The authors would like to thank all persons for taking their time to participate and for their contribution to this report.

Reference group:

Fredrik Bengtsson, Ringhals
Roger Granath, Forsmark
Karl-Erik Ericsson, OKG
Harri Perhonen, Fortum

Sammanfattning

Den nordiska kärnkraftsflottan har idag olika tekniska lösningar för säkerhets I&C. En stor del av utrustningen är fortfarande av konventionell typ, men det finns också ny digital utrustningar, system och plattformar installerade. I många fall har implementeringen av ny digital utrustning introducerat högre komplexitet hos funktioner, men också i dokumentation och i licenserings-sammanhang. Projekt med påverkan på digitala system har i många fall eskalerat långt över budget.

Studiens syfte var att analysera erfarenheter från projekt som genomfört ändringar i programmerbara system i nordiska kärnkraftverk. Studien undersökte *design* och *arbetsprocesser* som påverkar *säkerhet, kvalitet* och *kostnadseffektivitet* hos Oskarshamn, Ringhals och Forsmark.

De undersökta kärnkraftverken har en stor spridning av I&C-produkter, konfigurationer, komplexitet av ändringar och valda strategier. Det gör det problematiskt att jämföra nyckeltal mellan de olika kärnkraftverken, eftersom informationen inte representerar homogen fakta.

Studien når slutsatsen att den största påverkan görs när utrustningen väljs och konfigureras för första gången. Desto mer funktionalitet som installeras i plattformen och desto mer kommunikation, både intern och extern, desto mer komplext blir det att göra ändringar och verifiera systemet över tid.

Från ett strategiskt perspektiv rekommenderar studien att vara selektiv vid acceptans av ändringar i PE-system. Det bör utvärderas om den efterfrågade anläggningsfunktionalliteten kan uppnås genom andra tekniska lösningar som inte leder till ändringar i PE-system. Om få ändringar planeras i PE-system är kärnkraftverken generellt mer nöjda vid användning av leverantören.

På det sätt som kärnkraftverken arbetar idag erhålls hög kvalitet vid ändringar i PE-system. Det är dock en utmaning att bevisa att ingen annan funktionalitet har påverkats, vilket kräver ett strukturerat arbetssätt och kompetenta resurser. Från ett kostnadsperspektiv finns det anledning att se över vissa arbetsmetoder som kärnkraftverken tillämpar. Aspekter att beakta för framtiden är framåttunga processer, kompetens (både internt och hos leverantören), estimering av kostnad för livscykel, leverantörsstrategi, projektomfattning och koordinering av I&C projekt. Vidare behöver kärnkraftverken tolka relevanta standarder och utgå från dem vid utveckling och effektivisering av processer. Slutligen rekommenderar studien att SSM ska involveras tidigare.

Följande lista är ett urval av rekommendationer till framtida studier för Elforsk:

- Hur regressionsanalys bör utföras.
- Att arbeta agilt men fortfarande uppfylla standarder och leverera kvalitetssäkrade ändringar.
- Utveckling av kravhantering och verktyg.

Summary

The Nordic nuclear fleet of today consists of a mix of technologies for safety I&C. A large portion of the equipment is still of conventional type but there are also new digital equipment's, systems and platforms installed. In many cases the use of new digital equipment has introduced complexities in the functions, but also in documentation and in licensing issues. Projects affecting these systems have in many cases escalated far beyond budget.

The research studies goal was to retrieve experiences from recent modification projects in programmable systems that have been implemented in the Nordic Nuclear Power Plants (NPPs). The study investigated *design* and *working processes* that affects *safety*, *quality* and *cost* efficiency at Oskarshamn, Ringhals and Forsmark.

The examined NPPs have a large diversity in I&C products, configurations, complexity of changes and chosen strategies. It makes it problematic to compare key figures between the NPPs, since the figures do not represent homogenous facts.

The study reaches the conclusion that the largest impact is made when the equipment is chosen and configured for the first time. The more functionality that are installed in the platform and the more communication, both internally and externally, the more complex it will be to change and verify the system over time.

From a strategic perspective, it is recommended to be selective when accepting changes in PE systems. It should be evaluated if the requested plant functionality can be achieved by other technical solutions that do not lead to changes in PE systems. If few changes are planned, this study indicates that NPPs are more satisfied using the supplier for changes.

In the way the NPPs work today they reach a high quality level in their modifications. Even so, it is always a challenge to prove that “nothing else” has been affected which requires a structured way of working and competent resources. From a cost effectiveness perspective there are reasons to look over the working methods the plants have. Some aspects to consider for the future are front loaded processes, competence (both in-house and supplier), life cycle cost estimations, supplier strategies, scoop and coordination of I&C projects. Furthermore, the NPPs needs to interpreted relevant standards and use them as basis for efficiency improvements. Finally, involve SSM more early.

The following is a selection of recommendations for Elforsk to perform future studies in:

- How to work with regression analysis.
- How to work agile but still comply with standards and deliver quality ensured changes.
- How to improve requirement management and tools.

Content

1 Introduction 11
1.1 Problem background ... 11
1.2 Purpose and research questions ... 11
1.3 Delimitations ... 12

2 METHODOLOGY 13
2.1 Research design ... 13
2.2 Methods ... 13

3 EMPIRICAL FINDINGS 15
3.1 General ... 15
3.1.1 Standards regulating safety systems and I&C ... 15
3.2 Strategy ... 17
3.3 Platform ... 19
3.3.1 Comparison; AC160, Oskarshamn 1 VS Ringhals 2 ... 19
3.3.2 Comparison; all platforms used for neutron flow measuring ... 20
3.3.3 Comparison; TXS, Oskarshamn 2 VS Ringhals 1 ... 20
3.3.4 Comparison; AC160 and TXS ... 21
3.3.5 Description of used platforms at R3/4 ... 21
3.4 Working Processes ... 21
3.4.1 Processes at Vattenfall AB (Ringhals and Forsmark) ... 22
3.4.2 Processes at Oskarshamn ... 24
3.4.3 Configuration and Documentation Management ... 26
3.5 Project ... 27
3.6 Summary of Interviews ... 28

4 ANALYSIS 30
4.1 General ... 30
4.2 Strategy ... 30
4.2.1 Resources and Competence ... 35
4.3 Platform ... 37
4.3.1 Functionality ... 37
4.3.2 Platform architecture ... 38
4.3.3 Platform capacity ... 39
4.3.4 Tools ... 39
4.4 Working Process ... 41
4.4.1 General ... 41
4.4.2 Administration, configuration and documentation management ... 41
4.4.3 Requirement process ... 42
4.4.4 Inherited processes ... 43
4.4.5 Roles ... 43
4.4.6 Verification ... 44
4.4.7 Licensing process ... 46
4.5 Projects ... 46
4.5.1 Packaging and Coordination of I&C projects ... 46

5 Conclusions 48
5.1 Safety and Quality ... 49
5.2 Cost and Efficiency ... 50

6 Recommendations 51
6.1 General ... 51

6.2 Strategy 51
6.2.1 Strategy life cycle 52
6.3 Platform 53
6.3.1 Platform tools 54
6.4 Working Process 54
6.4.2 Licensing process 55
6.4.3 Projects 55
6.5 Recommendation to Elforsk 55

7 References 56

Appendix

Appendix 1: Comparelse matrix NPPs I&C platforms

Appendix 2: Interview questions

Appendix 3: Graphs of multible choice questions

Appendix 4: Comparison: AC160,O1 vs R2 and TXS, O2 vs R1

Terms and abbreviations

DKV	Operational Readiness Verification (DriftKlarhetsVerifiering)
DPS	Diversified protection system
F1	Forsmark 1
F2	Forsmark 2
F3	Forsmark 3
FAT	Factory Acceptance Test
FKA	Forsmark Kraftgrupp AB
FPGA	Field Programmable Gate Array
GE	General Electric
HW	Hardware
I&C	Instrumentation & Control
KSU	Kärnkraft Utbildning och Säkerhet AB
KPI	Key Performance Indicator
NPP	Nuclear Power Plant
O1	Oskarshamn 1
O2	Oskarshamn 2
O3	Oskarshamn 3
OKG	Oskarshamnsverkets kraftgrupp
OPS	Original Protecting System
PE	Programmable Electronic
QMS	Quality Management System
R1	Ringhals 1
R2	Ringhals 2
R3/4	Ringhals 3 and 4
RAB	Ringhals AB
RHR	Residual Heat Removal
RPS	Reactor Protection System
PRM	Power Range Monitoring
SAT	Site Acceptance Test
SSM	Swedish Radiation Safety Authority
SW	Software
TXS	Teleperm XS
VPMM	Vattenfall Project Management Model
V&V	Verification & Validation
WEC	Westinghouse

Plant project	Project responsible for changes in plant design.
I&C project	Project responsible for I&C-platform changes.
Stand-alone platform	PE platform without communication to other PE platforms. (Normally Stand-alone is defined as a system without any interface to other systems, in this report it refers to no communication with other PE platforms)
Stand-alone processor	Processors without communication to other processors.

Definitions

Among the Swedish NPPs there is a mixed use of the available standards within IEEE (US) and IEC (EU). There is different use of definitions in IEEE compared with IEC and in this chapter it is described how the report has chosen to handle the differences and how to use some of the different terms.

In IEEE 603, *Safety System* [7] is defined. Some part of the Safety system can be realised by I&C, see Figure 1. IEEE 603 do not use the term I&C but when examining the definition for I&C from IEC 61513 [4], see definition below, it is comparable with what IEEE 603 states. Figure 1 is collected from IEEE 603 but the definition from IEC 61513 is added manually, to show the comparison between the two standards.

Definition of I&C system according to IEC 61513:

> *"**I&C system**, System, based on electrical and/or electronic and/or programmable electronic technology, performing I&C functions as well as service and monitoring functions related to the operation of the system itself. The term is used as a general term which encompasses all elements of the system such as internal power supplies, sensors and other input devices, data highways and other communication paths, interfaces to actuators and other output devices. The different functions within a system may use dedicated or shared resources".*

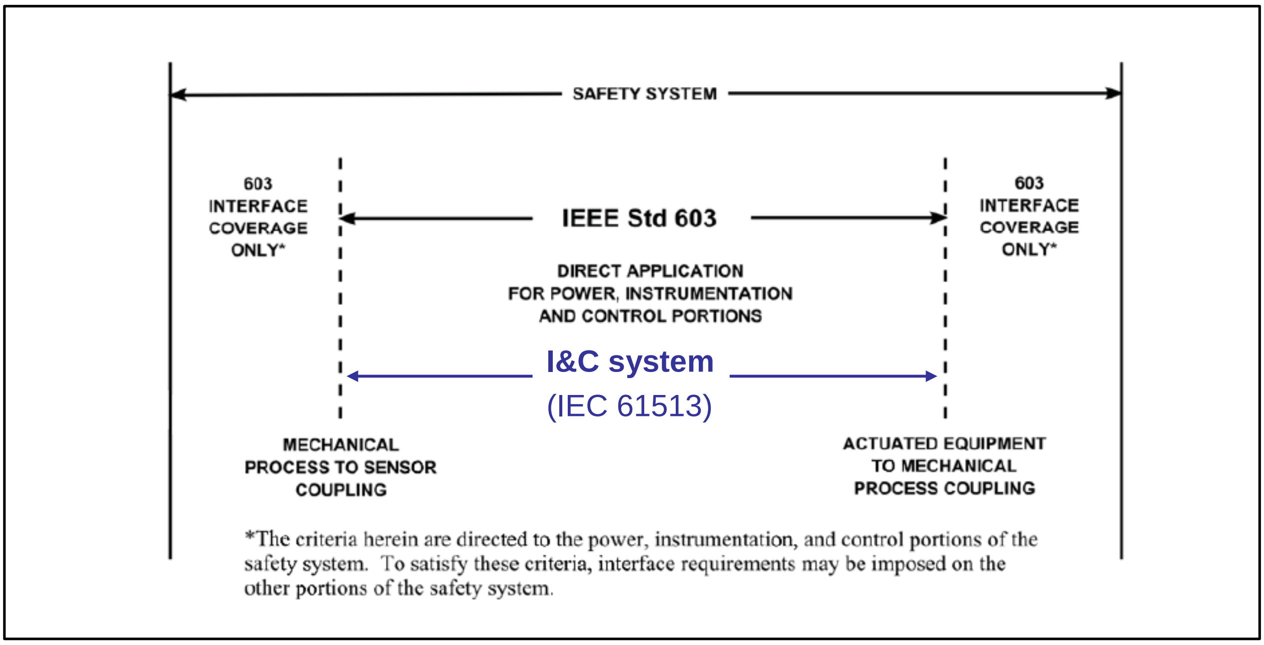


Figure 1: The figure is from IEEE 603 where the definition of an I&C system from IEC 61513 has been added.

The use of nomenclature differs and in this report the following definitions have been made:

Safety System

The definition of Safety System, according to Figure 1, comprises more than what is included in an I&C system. However, when referring to Safety System in this report, it is only referring to the part of the Safety System that is implemented in I&C.

Plant system

When plant system is used, it refers to the systems in the plant configuration such as system 531, 539 etc.

I&C system

An I&C system can be used for safety reasons as well as for non-safety reasons (and for safety related systems when the IEC categories are used). An I&C system contains the whole chain (from sensor to actuator of a component). The I&C system is often divided into several plant systems since e.g. the sensor and actuator belongs to different plant systems.

I&C platform / PE system

When the term I&C platform or PE system is used in this report, it refers to digital I&C implemented in a platform. Other programmable equipment, such as transmitters etc., is not a focus area in this report. When referring to analog I&C, it is clearly written.

Classification:

Since both IEC standards and IEEE standards are used at Swedish NPPs, a mix of classification is used.

O1, R2 are using the IEC classification which divides the functions into CAT A = Safety functions, CAT B = Safety related functions, CAT C = Non safety functions and Cat O = General purpose.

R2 has an additional classification which is "CATB^A" (CAT B rose to A). It is CAT B functionality with seismic requirements.

R1, R3 / 4, O2, F1 / F2 / F3 are using the IEEE classification which divides the functions into safety function and non-safety function. Equipment is classified as 1E, 2E and 3E.

This leads to a different set up and use of terminology at the different NPPs. The report reflects this situation.

1 Introduction

1.1 Problem background

The Nordic nuclear fleet of today consists of a mix of technologies for safety I&C. A large portion of the equipment is still of conventional type but there are also new digital equipment, systems and platforms installed.

In the coming years a considerable amount of systems and equipment must be replaced or upgraded because of different aspects of aging. This is a challenge and the experience from recent years is unfortunately mixed.

In many cases the use of new digital equipment has introduced complexities in the functions, but also in documentation and in licensing issues. On the other hand; the operating experience, availability etc., are in most cases excellent after the digital systems have been commissioned.

Regarding cost; new digital equipment has a reasonable price tag as long as only the products themselves are considered. However, when adding on the engineering hours required to implement the system in the nuclear power plant with verified safety the cost has in many projects escalated far beyond budget.

Hence, there is a need for research around these issues to achieve both safety and reasonable life cycle cost.

(Problem background from Elforsk, Strategy plan ENSRIC).

1.2 Purpose and research questions

The projects goal is to retrieve experiences from recent modification projects in programmable systems that have been implemented in the Nordic NPPs.
The project will answer the following research questions:

- Could a different approach in the design make the modification tasks easier with an increase in safety, quality and cost effectiveness?

- How do different approaches in the work processes for modifications influence the quality and cost effectiveness for the modifications?

The project will focus on modification projects in existing I&C platforms used in safety systems, at Oskarshamn, Ringhals and Forsmark.

The project will analyse *Platforms*, *Processes* and *Strategies* from the following aspects:

- Safety and Quality
  - Methods and processes
  - Available competent resources
  - Safety culture and behaviour

- Cost and Efficiency
  - Life cycle cost
  - Project cost / Efficiency within the projects
  - In-house versus supplier

1.3 Delimitations

The research study has investigated changes made mainly to existing I&C platforms used for safety systems, not implementation of new platforms. However O2 is part of the survey even if their I&C platform is not taken into operation yet.

Only Swedish NPPs are included in the study.

The research has focused in digital I&C used for safety systems, but the study also includes experiences from digital I&C used for safety related systems.

The technical level of this report is written to suit a target group with NPP and I&C competence.

The suppliers' strategies, working methods and tools have not been reviewed and are not part of the survey.

2 METHODOLOGY

2.1 Research design

The research has used a qualitative research approach. Qualitative methods are used when a deeper understanding is requested within a research area or a specific problem, and data are normally gathered through interviews.

Additional to the qualitative approach, a literature study has been performed where NPPs' documentation has been reviewed.

The examined NPPs have a large diversity in I&C products, configurations, complexity of changes in I&C and chosen strategies. It makes it difficult to compare key figures between the NPPs, since the figures do not represent homogenous facts. Because of the diversity and difficulties in comparing NPP 1:1 (conducting detailed comparisons), this study has focused in extracting and highlighting recommendations and good practices from all of the NPPs.

2.2 Methods

The project has interviewed altogether 33 persons at Oskarshamn 1-3, Ringhals 1-4, Forsmark 1-3 and the Swedish Radiation Safety Authority. The interviewed persons have the following positions:

- Line Managers I&C
- Product and System Owners I&C
- Process Owner Quality Management System
- Process Owner Verification and Validation
- Process Owner Configuration Management
- Project Managers I&C projects
- Lead Engineers and Developers I&C projects
- Test Leaders I&C projects
- Commissioning I&C projects
- Quality and Validation Managers I&C projects
- PSG executioners I&C projects
- Swedish Radiation Safety Authority I&C

All roles do not exist within all the NPPs, and then persons with similar responsibility have been interviewed. In this report *[“Interviews, 2015”]* is used when the interview material is referred to as a source.

The following types of documents and information has been supplied[1] from Oskarshamn, Ringhals and Forsmark (supplied partly during interviews).

---

[1] Due to confidential material these documents are only partly referred to directly in this report.

Generic processes and instructions:

- Project Management Process
- Quality Management System
- Verification and Validation Process
- Configuration Management Process
- Technical Processes I&C Safety System
- Platform Specifications

No project unique documentations have been supplied to the study.

Other types of documents that have been used in the study are presented in chapter 7 References.

3 EMPIRICAL FINDINGS

The empirical findings are collected from the references in chapter 7 and from the performed interviews.

3.1 General

From a general point of view, the NPPs choice of strategy and working methods are related to regulations in the standards for I&C, used for safety systems. To understand the NPPs strategic choices and to evaluate the potential of efficiency improvements, it is important to start from the standards. In the next section a selection of standards with impact on I&C has been listed and commented.

3.1.1 Standards regulating safety systems and I&C

Standards regulating the use of I&C systems contain requirements for management, working processes and quality management that shall be applied when changing in an I&C system (and installing the system for the first time).

In Table 1 a selection of standards with impact on safety systems and I&C systems are listed. The selection is made due to what SSM are referring to in combination with what the NPPs have used in their licensing. The scope and aim of the standards are different; some are dedicated for the nuclear industry, others are applicable for Systems or Software independent of branch (viewed in column *Scope* in the table). Due to this, it must be evaluated to what extent each standard must be applied and for which part of the plant.

Table 1. Table over a selection of standards with impact on safety systems and I&C.

IEEE	Scope	Main area	Details	Summary
IEEE 603	NPP	Safety systems	Standard criteria for safety systems in NPP.	IEEE is not using the term I&C system, see Figure 1.
IEEE 7-4.3.2	NPP	Digital computers	Standard criteria for digital computers in safety systems of NPP.	The standard is a complement to 603 with detailed requirements on computerized systems, including e.g. that a QA plan shall be conduct ed according to IEEE 12207 and 603. Requires independence. Used e.g. for licensing of R2.
IEEE 12207	System and Software Engineering Standards	Systems and Software Engineering - life cycle processes	Life cycle process for software (ISO/IEC 12207:2008, IDT).	The standard includes processes and activities that should be used during the life cycle of the Software (acquisition of Software, development, delivery, commissioning, operation, maintenance and decommissioning).
IEEE 1012	System and Software Engineering Standards	IEEE Standard for System and Software Verification and Validation	For Software	The scope encompasses V&V processes for System, Software and Hardware, and includes their interfaces.
IEEE 828	System and Software Engineering Standards	IEEE Standard for Software Configuration Management	For software	Standard for Software Configuration Management.
IEC 61513	NPP	Instrumentation and control important to safety	General requirements for systems.	Requires a life cycle perspective for I&C systems critical for safety. Compare with IEEE 603. The standard is pointed out in SSMFS 2008:1.
IEC 60880	NPP	Instrumentation and control systems important to safety	Software aspects for computer-based systems performing category A functions	Compare with IEEE 7-4.3.2. The standard is pointed out in SSMFS 2008:1.

All changes to a NPP require well defined regulated processes and instructions. Since validated state of the plant is affected by a change, a safety evaluation is necessary. Strategies for how to verify the change must be performed and a strategy for re-validation of the plant needs to be evolved. This is applicable for all plant changes but when programed equipment is installed to a NPP an even more structure way of working is required according to the standards in Table 1. The standards describe how a PE system shall be designed, installed and verified when it is used in a NPP. Each NPP owner needs to identify which standards those are applicable for their licensing. IEC and IEEE differ in nomenclature, classification etc., however the basic requirements are rather similar and some areas especially critical for PE systems are highlighted. Here follows some examples from the standards that relate to the working processes which the NPP owner needs to relate to:

- *A life cycle perspective is required. The life cycle for a computerized system starts in the concept phase of the development and ends when system/software is withdrawn from use.* IEC 60880 [5] and IEC 62138 [6]
- *The system safety life cycle described in IEC 61513 includes and places requirements on, but does not dictate, the project arrangements to be used for production of systems.* IEC 61513 [4]
- *The approach to software development should be based on the traditional "V" model as this approach has been reflected and promulgated in other standards, notably IAEA NS-G-1.3, but allowing necessary adjustments recognizing that some phases of the development can be done automatically by tools and that software development may be iterative*. IEC 60880 [5]
- *The verification activities undertaken as part of the software development are usually the responsibility of the supplier and are undertaken by staff independent of those performing the software production; the most appropriate way is to engage a verification team.* IEC 60880 [5]
- *The output of each software development phase shall be verified*. IEC 60880 [5]
- *Software tools used for verification and validation shall be qualified as required*. IEC 60880 [5]

These examples are from the IEC standards but similar requirements can be found in IEEE (e.g. IEEE 1012 [8]). These rules all argues for the necessity of a structured working process where the design is verified along with its development. They also indicated that a life cycle approach is necessary and that it starts already with the strategy choices made when deciding to use a PE system for safety systems and ends with decommissioning.

3.2 Strategy

The strategy starts during evaluation when an old equipment are about to be changed, due to e.g. age. Here follows some important strategic aspects to consider:

- Shall programmable equipment or traditional analogue equipment be used?
- Shall the platform and processors be in a network or stand-alone?
- What functionally shall be included?
- What kind of suppliers and platforms are available in the market?
- Maintenance strategies, what other equipment do the NPPs have today?
- Life cycle cost.
- Relation and involvement with the supplier.
- Test equipment and test strategy.
- Strategy for administration, configuration and documentation.

Most of these strategies are set when the PE system is acquired and installed for the first time, and the strategies then follows the equipment the whole life time. Table 2 summarizes some strategy decisions that the NPPs have made and it shows that they all have chosen different ways to solve their situation. The platforms listed in Table 2 are used for Safety functions and/or Safety related functions.

Table 2. Strategies for PE systems.

NPP	Platforms	Functions	Internal/External workload	Stand-alone platform / stand-alone processor	Internal test equipment
R2	AC160 and Ovation	All CAT A functions are included in AC160 and all CAT B and CATC functions are included in Ovation.	All design and V&V are done at RAB. WEC is taking part only as a review instance for critical parts of the design in AC160. WEC/KSU is used as an external part for verification for AC160.	Not stand-alone platforms (Communication AC160 -> Ovation)	LES (1 of 4 subs).
O1	AC160 and AC450	CAT A, CAT B and CAT C functions in the EKB are included in AC160. The CAT B functions in the "old main electrical building" are included in AC450.	WEC is performing all detailed design and is also participating in the system design to some extent. FAT is performed at WEC.	Stand-alone platforms (AC160 is separated from AC450)	Test tool (”Husmaskin”)
O2	TXS	The complete RPS and DPS are included in TXS. (O2 are using TXP for non-safety equipment)	The equipment is not taken into operation yet. However OKG is planning to have the same concept as for O1, meaning that the supplier Siemens/Areva in this case, are responsible for detailed design and verification of the changes in the PE system.	Stand-alone platforms (TXS RPS is separated from PRM)	No
R1	TXS	RPS is divided in a DPS and an OPS. OPS is the old part that still is in an analogue environment. Some of the safety functions were moved to the new part in TXS and is called DPS since it is diversified to OPS.	Areva is a part of the change projects and are performing the verification in the test tool SIVAT.	Stand-alone platforms (TXS RPS is separated from TXS RHR)	No
R3/4	Foxboro Spec 200 and WDPF	Spec 200 are used for some safety functionality, mainly limit value measuring and presentation of safety function in the control room. The execution of the safety functions is done by an analogue system.	R3/4 are performing all design and verification on their own (without involvement from the supplier).	Stand-alone platforms (Spec 200 is separated from WDPF) Stand-alone processors in Spec 200 and WDPF	1 Spec 200 Electrical enclosure for testing 1 WDPF Electrical enclosure for testing

Neutron flow measurements					
F1, F2, F3	NUMAC	Neutron flow measurements (stand-alone platform) (531)	All detailed design and verification is performed by GE.	Stand-alone platform	Test tool (1 sub)
R1	TXS	Neutron flow measurements (stand-alone platform) (531)	Areva is a part of the change projects and are performing the verification in the test tool SIVAT (same as for RPS).	Stand-alone platform	No
O1	TXS	Neutron flow measurements (stand-alone platform) (531)	The supplier is performing all changes to the equipment.	Stand-alone platform	No
O2	TXS	Neutron flow measurements (stand-alone platform) (531)	The supplier is performing all changes to the equipment.	Stand-alone platform	No
O3	TXS	Neutron flow measurements (stand-alone platform) (531)	The supplier is performing all changes to the equipment.	Stand-alone platform	No

3.3 Platform

In Appendix 1, a comparison matrix between the Swedish NPPs' I&C platforms is included. It includes facts such as technical data, configurations and strategies acquired during the study. In the following chapters, parts from the large comparison matrix are broken out for a more easily comparison between relevant aspects of the I&C platforms, these tables are included as Appendix 4.

The following comparisons and descriptions are made:

- Comparison between O1 and R2, since both NPPs are using AC160 for safety functions including RPS.
- Comparison between all platforms used for neutron flow measuring.
- Comparison between O2 and R1 since both NPPs are using TXS for safety functions including RPS.
- Comparison between AC160 and TXS, to compare the platform equipment used for similar type of tasks in the NPPs.
- Description of the used platforms at R3/4. The configuration and application of the platform differs from the other NPPs.

3.3.1 Comparison; AC160, Oskarshamn 1 vs Ringhals 2

See Appendix 4 table 1 for detailed description of AC160 at O1 and R2. Below is a summary of Appendix 4.

Both O1 and R2 have AC160 from Westinghouse in the safety system. Both the NPPs have the platforms deeply integrated and use it for RPS. However, O1 has implemented more functions in AC160 (including CATB and CATC functions) than R2. Notable is that O1 has almost twice as many processors in AC160 as R2 has, which partly can be explained by R2's use of Ovation for CAT B functions. Both the NPPs have made functional changes in the platform since installation. An important difference in the strategy is that O1 use Westinghouse for both parameter and functional changes in AC160. R2 performs all the changes in-house which results in more in-house competence for AC160 at R2 than at O1.

Ovation is not seismic classified and due to that CAT B functions with seismic requirements are included in AC160. ("CATB^A")

3.3.2 Comparison; all platforms used for neutron flow measuring

Table 3. Comparison all platforms used for neutron flow measuring.

	O1	O2	O3	R1	R2	R3/4	F1/2	F3
Platforms used for neutron flow measuring (531, Safety System)	TXS	TXS	TXS	TXS	AC160	Analogue system	Numac	Numac
Dedicated for neutron flow measuring.	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes

R2 is the only NPP that do not have a dedicated I&C platform for neutron flow measuring (Nimod at R2, an analogue system 531, sends signals to AC160 for signal processing). Numac, used for neutron flow measuring at FKA, is the only PE system that FKA are using for safety. Few changes have been made in the neutron flow measuring systems at the examined NPPs (mostly parameter changes). At R3/4, an analog system is used for neutron flow measuring and O1 has a diversified analog system to TXS for neutron flow measuring.

3.3.3 Comparison; TXS, Oskarshamn 2 vs Ringhals 1

See, Appendix 4 table 2, for detailed description of TXS at O2 and R1. Below is a summary of Appendix 4.

Both O2 and R1 have TXS in the safety system. R1 has three separate TXS platforms, one for RPS, one for RHR and one for PRM. The RPS functionality is divided into two parts, DPS (included in TXS) and OPS (the old analog system). O2 has two platforms, one for RPS and one for PRM. O2 has twice as many processors in TXS compared to R1, since O2 have more functionality included in the platform. O2 has not yet taken the RPS platform into operation (the platform is being installed by project PLEX). R1 has made functional changes in TXS and the changes are made in-house (testing is performed by Areva).

3.3.4 Comparison; AC160 and TXS

See Appendix 1 for detailed description of AC160 and TXS in O1-3, R1-2 and F3. Below is a summary of Appendix 1 regarding AC160 and TXS.

The great difference between AC160 and TXS are not in the PE systems basic architecture, it is in how the PE systems are configured. At e.g. R2, there are a lot of internal communication in AC160 (communication between the processors), while the communication is more limited in TXS at R1.

Interviewed engineers with knowledge about both AC160 and TXS state that there are a few differences between the two PE systems. E.g. visual coding at TXS (which makes it easy to review and perform changes) is an advantage compared to AC160. An advantage with AC160 is the reliability of the platform.

3.3.5 Description of used platforms at R3/4

The configuration and application of the platforms at R3/4 differs from the other NPPs. Only a limited amount of the safety functions are implemented in the platforms. See Appendix 1 for detailed description of used platforms at R3/4. Below is a summary of Appendix 1 regarding platforms at R3/4.

R3/4 has Spec 200 and WDPF for safety system. Both the I&C platforms have stand-alone processors, which makes it difficult to compare them to other I&C platforms in Swedish NPPs. Spec 200 is only used for value measuring and do not actualize the safety functions (an analog system does this), which is another difference from other NPPs. Smaller changes in Spec 200 and WDPF are made in-house (for Spec 200 supplier competence is not available). Both the platforms will most likely need to be replaced near year 2023.

3.4 Working Processes

The standard states requirements on working processes (as described in section 3.1.1) which the NPPs needs to comply with. In this chapter the NPPs working processes for plant changes including changes of the PE systems are accounted for.

Note: The pictures in this chapter are collected from the NPPs' instructions and are due to that in Swedish.

3.4.1 Processes at Vattenfall AB (Ringhals and Forsmark)

At a Project Management level both Ringhals and Forsmark are using the same process, VPMM, since they both are a part of Vattenfall AB. However, the Operative parts of the process (product/plant development) are separately developed at each NPP over the years. The instructions for design, programing and test of PE system are part of the operative process and due to this the approach to do changes in programmable equipment differs between the two NPPs.

Explanation to VPMM process in Figure 2:
Red process - Governance process
Blue process - Project Management
Yellow process - Operational Process (product/plant development)

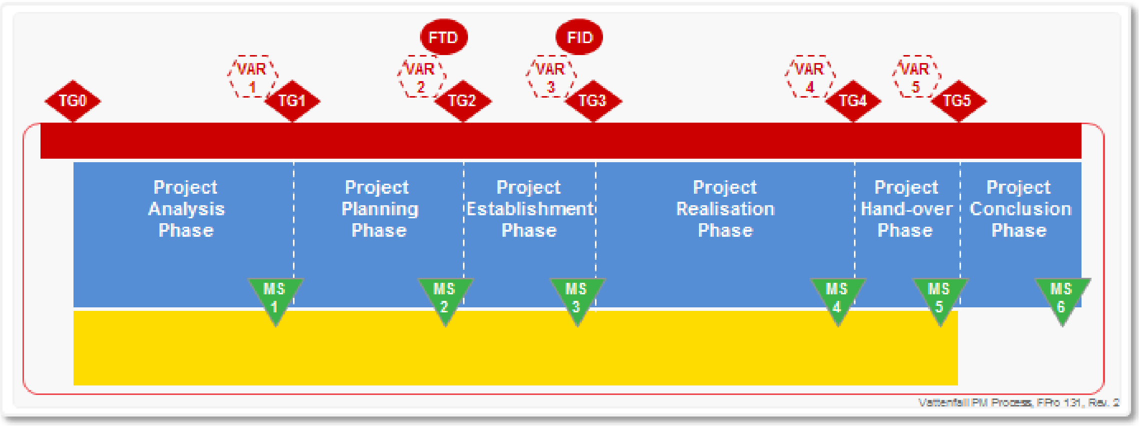


Figure 2: Generic VPMM process, ref. [13].

Within the operational process where all the design is performed, RAB is using the V-model for design and verification which is recommended in the standards. The design is broken down in Plant, System and Detailed design. Most of the design of the PE system is performed between ÄK3 and ÄK4, shown in Figure 3. The design of functionality is made in the earlier phases of the process and the input to the I&C platform design comes from a plant and system level. The functionality is thereby finally verified in the plant together with the complete plant system verification. All design guidelines for the PE systems are included in the Operational processes. Since RAB has the strategy to perform more design and verification in-house compared with FKA and OKG, RAB also has a more extensive set up of instructions on a detailed design level. The top level design instructions for detailed design of PE systems are generic, but each platform also has their specific set of instructions, design guidelines and test recommendations.

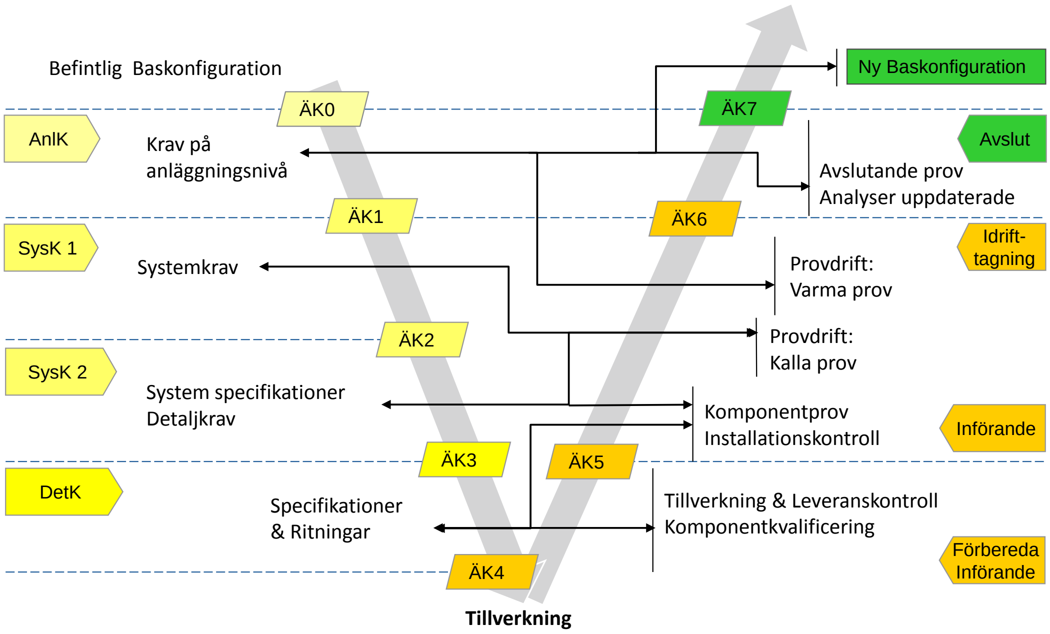


Figure 3: V-model used at Ringhals, ref. [12].

FKA's top level process is similar to RAB and FKA is also working accordingly to the V-model, see Figure 4. Since FKA is using the supplier for all design, test, installation and documentation of the PE system, FKA do not have detailed instructions for changes of the PE system, in-house. The focus is instead on the communication and interface towards the supplier from a quality assurance perspective. Plant and system design are performed in-house by FKA while detailed design for the PE system is performed by the supplier.

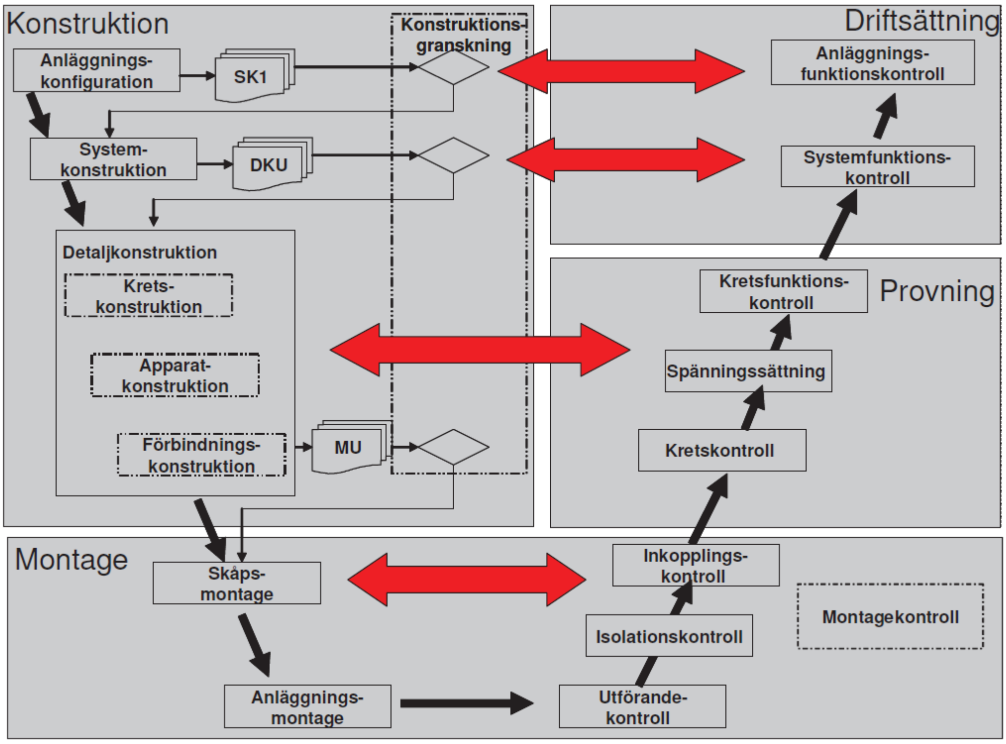


Figure 4: Forsmark V-model, used for all types of plant changes, ref. [14].

3.4.2 Processes at Oskarshamn

OKG has an own developed project model, see Figure 5. The green swim lane is the Operational process for product/plant development, (to be compared with the "yellow part" of VPMM in Figure 2).

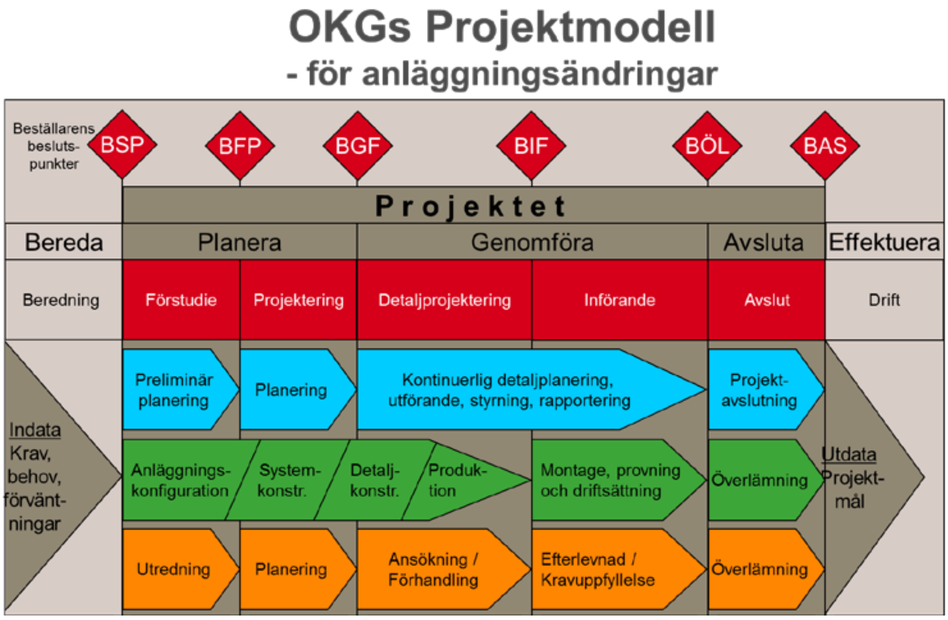


Figure 5: OKG project model, ref.[16]

Also OKG are working accordingly to the V-model which is shown in Figure 6. As Figure 6 shows, the verification of the PE system is integrated with the verification and the final validation of the plant systems (the top box on the left leg is stating System requirements and is referring to Plant system). OKG let the supplier do all the changes in the PE system and due to that they do not have detailed instructions regarding design or testing of the PE platform. The complexity of the change decides when the supplier shall be included in the process. If it is a complex change, affecting the functionality, the supplier is involved from system design. If it is a simple change, e.g. text faults, it is given as a direct specification from OKG.

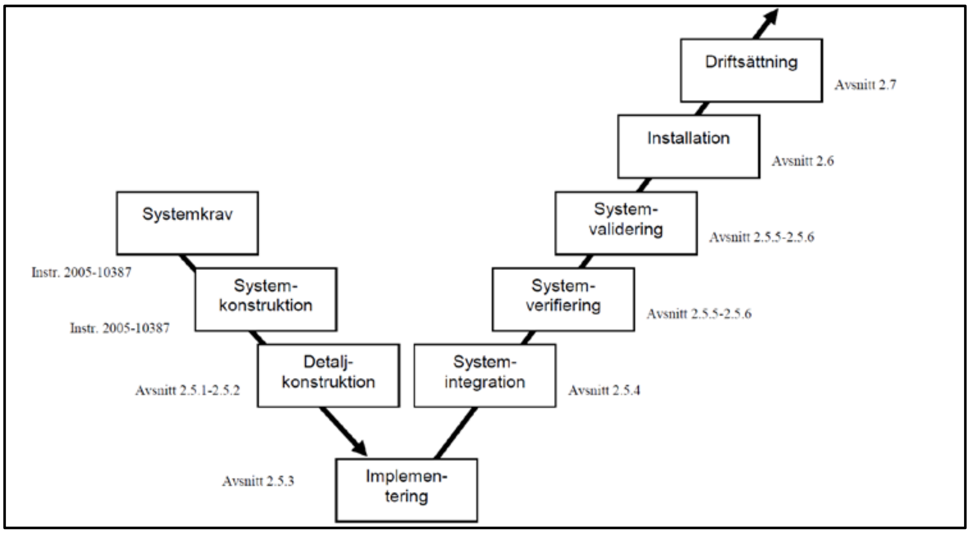


Figure 6: OKG V-model used for changes in SW (the numbers are references to sections in the NPP's instruction), ref. [15].

3.4.3 Configuration and Documentation Management

Both IEEE 12207 [8] and IEC 61513 [4], states requirements regarding the importance of Life cycle plans for PE systems. Due to that, it is not enough to only have development processes and focus at the projects changes. There most exist a plan and process for administration over time, where configuration and documentation management are important support processes. It must be visual and easy to find the latest baseline for both the PE system and the whole plant. All NPPs have well-defined regulations regarding how to store information over time, the Plant register (anläggningsregister).

Even though there exist a Plant register with a define documentation regulation, there is a complexity when handling I&C system since it stretches over more than one Plant system. Therefore, a strategy for handling the documentation which addresses requirements, design documents and test results to the most logical plant system is required. Also the PE platform in itself can be divided into several plant systems, e.g. 505, 516 etc. FKA has chosen to keep the PE systems' documentation together and refer to it from other place in the Plant register, this makes it easier for the supplier to up-graded it after a change.

OKG has not indicated any problems regarding handling of documentation over time.

RAB, mainly R2 which have had most changes since installation, reports that they spend a lot of time in documentation handling due to inherited configuration and documentation structures from the supplier.

3.5 Project

The NPPs where asked to estimate the costs at different activities/phases during I&C projects. Their answers are just rough estimations but give an overview over where most of the cost/time is spent. In these types of projects which include only a limited amount of hardware, cost and spent hours are strongly related.

Table 4. Table over estimated cost/time consumptions at different project activities.

<table>
<tr><th></th><th colspan="2">Ringhals 1</th><th colspan="2">Ringhals 2</th><th colspan="2">Forsmark</th><th colspan="2">Oskarshamn</th></tr>
<tr><th>Project activities:</th><th>% of project cost</th><th>Internal or by supplier</th><th>% of project cost</th><th>Internal or by supplier</th><th>% of project cost</th><th>Internal or by supplier</th><th>% of project cost</th><th>Internal or by supplier</th></tr>
<tr><td>Project Manage-ment and Admin</td><td colspan="2">Is included in the other figures</td><td>25</td><td>Internal</td><td>15</td><td>Internal</td><td>15</td><td>Internal</td></tr>
<tr><td>Plant/System design</td><td>25</td><td>Internal</td><td>10</td><td>Internal</td><td>15</td><td>Internal</td><td>10</td><td>Internal</td></tr>
<tr><td>Detailed design</td><td>20</td><td>Internal</td><td>23</td><td>Internal</td><td rowspan="3">50</td><td rowspan="3">Supplier</td><td rowspan="3">50</td><td rowspan="3">Supplier</td></tr>
<tr><td>Coding</td><td>20</td><td>Internal</td><td>5</td><td>Internal</td></tr>
<tr><td>Verification, incl FAT</td><td>25</td><td>Supplier</td><td>33</td><td>Internal</td></tr>
<tr><td>Installation & Commissioning, incl SAT</td><td>10</td><td>Internal</td><td>4</td><td>Internal</td><td>20</td><td>Internal</td><td>25</td><td>Internal</td></tr>
</table>

The NPPs estimates that between 50-65% of the cost/time are spent during Detailed design, coding and verification (including FAT). This is natural for a project with the task to change in PE systems. However, it is also in this area where most efficiency efforts can be made, see analysis in section 4.4 and 4.5.

R2 spends only 4 % at installation and it refers only to the time spent on the PE system during installation and commissioning.

Graph 1 in Appendix 3 shows that most NPPs are of the opinion that they do not work cost effective with I&C changes.

3.6 Summary of Interviews

In this section the answers to the quantitative interview questions are presented. The answers to the qualitative interview questions are not included due to integrity reasons. All question forms are presented in Appendix 2. The results from the qualitative interview questions are used as background for the analysis and are referred to in the Analysis chapter.

The multiple choice questions are transformed into graphical views which are presented in Appendix 3. The colors represent:

Dark red - Strongly disagree
Light red - Tend to disagree
Green - Neither agrees nor disagrees
Light blue - Tend to agree
Dark blue - Strongly agree
Grey - No opinion

When analyzing the result the amount of persons at each Plant needs to be taken into consideration, R1=6, R2=8, R3/R4=3, OKG=8, FKA=9, some persons are doubled since they have experience from more than one plant.

The following multiple choice questions were asked to detect problem areas for the study to investigate and all the resulting graphs will therefore not be discussed in chapter 4 Analysis (only the graphs with distinctive results are discussed). A short summery to each result (graph) is presented below:

1. **Does the I&C projects work efficiently. (Graph 1)**

   RAB is general more negative than OKG and FKA in this question. RAB has performed more complex projects after installation than OKG and FKA, which could be one explanation to the result.

2. **The NPP has sufficient I&C competence internally including consultants (without help from suppliers). (Graph 2)**

   The OKG staff is more worried about the access to I&C competence than the other NPPs.

3. **The NPP have well-developed processes/instructions for implementing I&C modifications (execution of I&C modifications internally without much supplier involvement). (Graph 3)**

   At all NPPs there are a un-satisfaction regarding the processes. However, there are also some staffs that are positive, especially at R3/R4.

4. **We have satisfactory safety thinking when implementing I&C modifications. (Graph 4)**

   Overall, the NPPs' staffs are satisfied with the safety thinking and attitude.

5. **I feel very confident in the quality of the I&C modifications. (Graph 5)**

   Overall, the NPPs' staff are satisfied with the quality of the I&C modifications.

6. **We should let the supplier perform more work during I&C modifications. (Graph 6)**

   Red in the graph means that the persons do not like more involvement by the supplier; they are satisfied or would prefer less involvement. R2 that has least involvement from the supplier are the most positive to involve the supplier more.

7. **We have sufficient emphasis on management and lifecycle when performing I&C modifications. (Graph 7)**

   The answers are widely spread and at RAB there are a lot of persons without an option.

8. **We create a technical debt while performing I&C modifications. (Graph 8)**

   At R1, the opinion is that a technical debt is created. This is not the perceived situation at the other plants.

9. **Our I&C documentation is managed and established in a good way. (Graph 9)**

   R2 is most negative and the opinion is that there is a lack in documentation management.

10. **We have a good working method for requirement management at I&C modifications. (Graph 10)**

    Overall, the NPPs' staff believes that the requirement management is good.

    Note: This is interesting since the study also has received suggestions for improvements of requirement handling during discussions with several of the interviewed persons.

11. **We have a good working method for verification and validation during I&C modifications. (Graph 11)**

    General, all NPPs are satisfied with how V&V are working.

12. **I think the following areas work well during I&C modifications (Graph 12 to Graph 29)**

    The question lists activities to be performed during a project.

    The areas that have the most negative responses are:

    - Project order and scope
    - Project Management
    - Purchase of HW (mainly RAB)

4 ANALYSIS

4.1 General

The standards applicable for I&C systems and software used for safety systems gives requirements and prerequisites for how the quality assurance must be performed when changing in an I&C platform, as described in chapter 3.1. Some of the requirements are summarized below:

- A life cycle perspective is required.
- The approach to software development should be based on the traditional “V” model but some phases of the development can be done automatically by tools and software development may be iterative.
- For the verification activities undertaken as part of the software development it is common to engage a verification team.
- The output of each software development phase shall be verified.
- Software tools used for verification or validation shall be qualified as required.

The standards give the basis for all improvement that can be introduced in the QMS at the NPP. The NPP must be clear about which standards they have interpreted and have traceability to where in their QMS the standards are implemented. If this is done in a structured way it is easier to evaluate any suggested change of efficiency improvements.

The NPPs are not comparable in a homogenous way. They all have chosen different strategies in terms of technical solution, implemented functionality and use of supplier. Furthermore, the amount and complexity of changes that have been performed since installation, differs widely between the NPPs. It is problematic to compare key indicators between different NPPs’ strategies since the extent of changes and circumstances are widely spread, and the figures are therefore not comparable. In the analysis chapter the report will account for the differences but also present best practise from the different NPPs.

4.2 Strategy

The strategy starts during evaluation when an old equipment are about to be changed, due to e.g. age. Here follows some important strategic aspects to consider:

- Should programmable equipment be used or should traditional analogue equipment be used?
- Should the platform and processors be in a network or stand-alone.
- What functionally shall be included?
- What kind of suppliers and platforms are available in the market?
- Maintenance strategies, what other equipment do the NPPs have to day?
- Life cycle cost.

- Relation and involvement of the supplier.
- Test equipment and test strategy.
- Strategy for administration, configuration and documentation.

These strategic decisions set the prerequisites for all coming changes of the I&C platform and some of them are hard to change later on, e.g. the use of the platform. This means that improvements that a NPP can perform are to some extent limited to the prerequisites that was set during the installation of the platform, see Figure 7. Figure 7 show the changeability over time, from acquiring to operation.

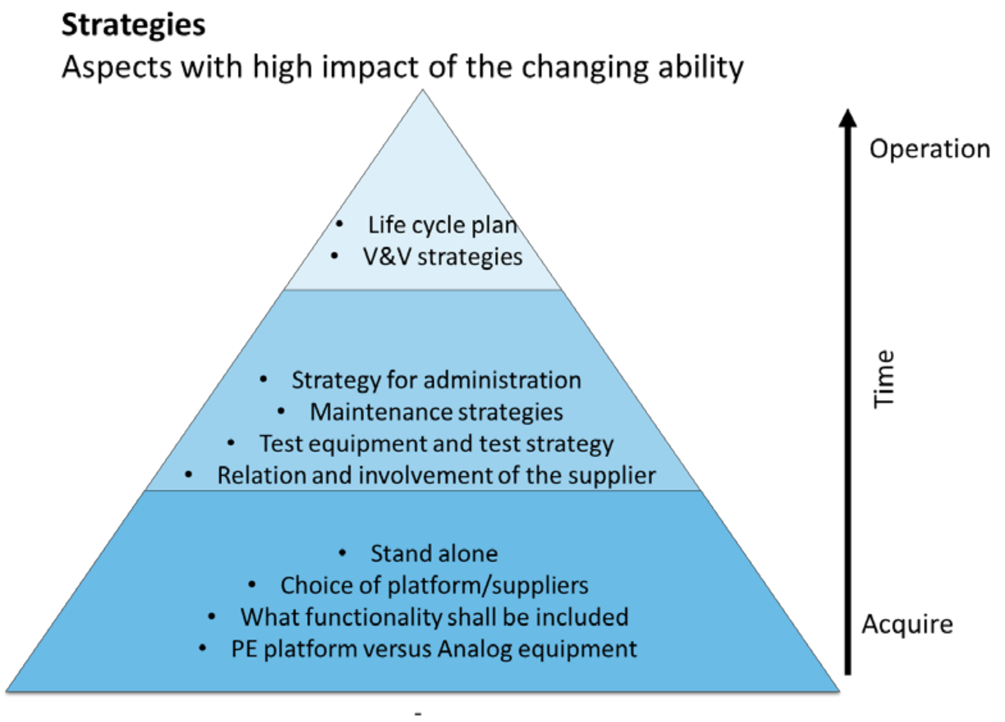


Figure 7: Changing ability in relation to time

In Chapter 3.2 it is accounted for some of the strategies that the NPPs have chosen, including all platforms used for safety functions and safety related functions. Table 5 is based on the Table 3 from chapter 3.2 but the *analysis* column and *complexity* column are added. The grades of complexity are based on a combination of the functions that are included in the platforms and the amount of work performed in-house. Table 5 gives an overview of the situation at the Swedish NPPs and the analysis in this chapter are made with this table as a basis.

Table 5. Summery over the platforms used for safety and safety related functions.

NPP	Platform	Functions	Internal/External workload	Analysis	Complexity
R2	AC160 and Ovation	All CAT A functions are included in AC160 and all CAT B and CATC functions are included in Ovation.	All design and V&V are done at RAB. WEC is taking part only as a review instance for critical parts of the design in AC160. WEC/KSU is used as an external part for verification for AC160.	R2 has the most complex situation of the NPPs since all CAT A and CAT B functionality is included in a PE platform and R2 has chosen to do all the design, coding and verification by them self. This requires a complete working process to be able to quality ensure the change. Furthermore, since R2 are doing the tests by them self they also need to quality ensure the test environment that is used for verification of code. Of all NPPs, R2 has done most changes in the PE systems since installation. Even if it is no CAT A functions in Ovation the total amount of functionality that are included in PE systems, and the fact that AC160 is communicating with Ovation, leads to a very high complex situation for R2.	Very High
O1	AC160 and AC450	CAT A, CAT B and CAT C functions in the EKB are included in AC160. The CAT B functions in the "old main electrical building" are included in AC450.	WEC is performing all detailed design and is also participating in the system design to some extent. FAT is performed at WEC.	O1 has a high complex situation since the entire CAT A functionality is included in a PE platform together with CAT B and CAT C functions. OKG has on the other hand chosen to use the supplier in a much larger context than RAB. One advantage with involving the supplier in this way is that it creates a natural independence and that OKG do not need to have detailed instructions for changes and tests in the PE system. OKG do not need to maintain the test environment that is used for verification of code, which R2 needs to do. In total this gives OKG an easier situation compared to R2.	High
O2	TXS	The complete RPS and DPS are included in TXS. (O2 are using TXP for non-safety equipment)	The equipment is not taken into operation yet. However OKG is planning to have the same concept as for O1, meaning that the supplier Siemens/Areva in this case, is responsible for detailed design and verification of the changes in the PE system.	The complexity of functions is comparable with O1. Compared with R1, which also is using TXS, O2 has chosen to include the complete RPS including DPS in the PE system. R1 have divided RPS in two part (OPS and DPS) and kept some of the safety functions in analogue systems. Since O2 is choosing the same supplier set up as for O1, no detailed instructions for changes in the PE systems and verification tools are required.	High

NPP	Platform	Functions	Internal/External workload	Analysis	Complexity
R1	TXS	RPS is divided in DPS and OPS. OPS is the old part that still is in an analogue environment. Some of the safety functions were moved to the new part in TXS and is called DPS since it is diversified to OPS.	Areva is a part of the change projects and are performing the verification in the test tool SIVAT.	R1 has a less functional complex situation compared with both O1 and O2 since not all safety function are included in the PE system. R1 is on the other hand performing all design by them self but not the verification of the code. This means that R1 needs working processes for design but does not need to maintain and administrate the verification tool SIVAT.	High
R3/4	Foxboro/ Spec 200 and WDPF	Are used for some safety functionality, mainly limit value measuring and presentation of safety function in the control room. The execution of the safety function is done by an analogue system.	R3/4 are performing all design and verification on their own (without involvement from the supplier).	R3/4 are using PE system for some of the safety functions but not to the same extent as R2, R1, O1 and O2. The use of the equipment is very limited to a few functions which make it easy to change. On the other hand, the equipment is old and R3/4 are doing all the changes on their own. Risks in the future are available competence and spare parts.	Medium
			Neutron flow measurements		
F1, F2, F3	NUMAC	Neutron flow measurements (stand-alone platform) (531)	All detailed design and verification is performed by GE.	PRM is a safety function but the PE system is stand-alone equipment dedicated to this task which makes it easy to control and change. Functional changes are rare; it is mostly correction of faults and parameter settings that are made. FKA has chosen to let the supplier do all the changes in the PE system.	Low
R1	TXS	Neutron flow measurements (stand-alone platform) (531)	Areva is a part of the change projects and are performing the verification in the test tool SIVAT (same as for RPS).	It is stand-alone equipment; see the comment for F1, F2, F3. The difference compared with FKA is that RAB are conducting changes in-house. There have only been minor corrections since installation.	Low
O1	TXS	Neutron flow measurements (stand-alone platform) (531)	The supplier is performing all changes to the equipment.	The same system is used for all three NPPs at OKG. However, O1 also has a diversified analogue system connected. It is stand-alone equipment with a limited amount of functionality included. The supplier is performing all changes to the equipment and only minor corrections have been done since installation.	Low
O2	TXS	Neutron flow measurements (stand-alone platform) (531)	The supplier is performing all changes to the equipment.	It is stand-alone equipment with a limited amount of functionality included. The supplier is performing all changes to the equipment and only minor corrections have been done since installation.	Low
O3	TXS	Neutron flow measurements (stand-alone platform) (531)	The supplier is performing all changes to the equipment.	It is stand-alone equipment with a limited amount of functionality included. The supplier is performing all changes to the equipment and only minor corrections have been done since installation.	Low

Since a lot of the initial strategic decisions sets the prerequisites for the complexity that the NPP will have during the life time of the I&C platform, the strategic decisions need to be based on a well thought out business case with a life cycle perspective. Today, decisions are sometimes made without having a profound analyse of different alternatives, costs estimations and life cycle consequences. Decisions are made successively which steers the orientations of the strategy until few alternatives becomes the only option. It is important to have a broad discussion regarding different kinds of alternatives, and to be careful focusing on only exciting and thrilling alternatives (often technical solutions that the engineers finds interesting, but that may lead to high life cycle costs). For instance, instead of replacing an old I&C system that the supplier may no longer support, it could be more cost effective to keep the old system and spend the money in training in-house personal for maintenance of the I&C system. *[Interviews, 2015*] A business case where different alternatives, cost estimations and life cycle consequences are being analysed must be developed before strategic decisions are made. If the analysis states that an exchange of an old I&C system is necessary, it is recommended to replace it with a system that is adapted to the task. It should be considered if other technology then fully adjustable programmable equipment could suit the requested purpose, e.g. FPGA technology.

R2 has developed a life cycle plan for Ovation including costs for each activity in the system until decommissioning year 2027. *[Interviews, 2015]* It gives R2 valuable knowledge when steering their operation and helps them make sustainable decisions from a life cycle costs perspective. The NPPs are recommended to develop a life cycle plan for I&C systems, with a profound analyse of the I&C systems status and coming activities. The following information should be included in a life cycle plan (but not limited to):

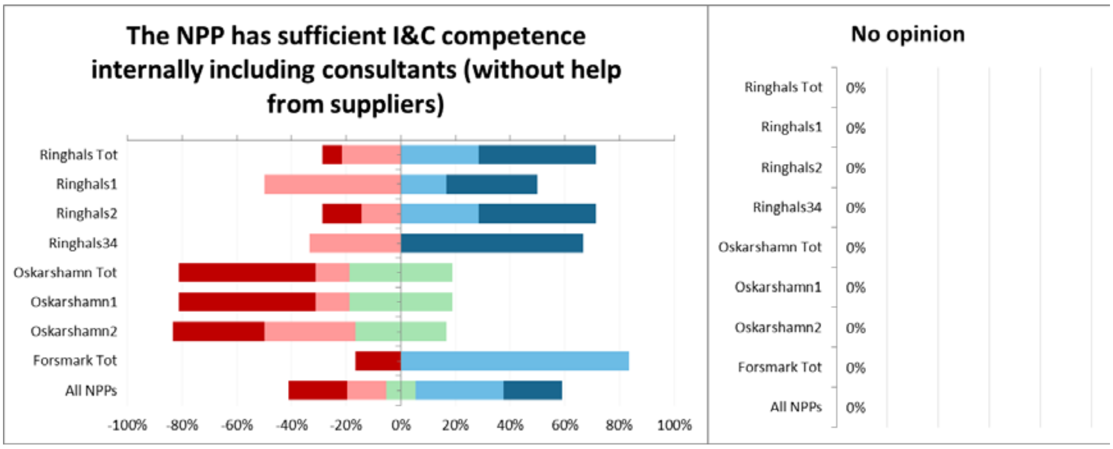
- Coming updates of the software.
- Replacement of hardware.
- Planned changes in the system (backlog, plant changes etc.).
- Regression strategy (how to handle regression analysis and tests).
- Lifecycle Verification and Validation.

The activities should relate to a business case and be planned in time. With this information the NPPs can make sustainable decisions from a life cycle costs perspective.

All investigated NPPs have expressed difficulties when performing changes in I&C systems. Several of the senior engineers and system managers have stated the need of a strategy that limits changes in I&C systems. When functional changes are made in NPPs (e.g. change of process function in the plant), the changes' effect on the I&C systems are often neglected. *[Interviews, 2015]* A more selective approach towards changes in I&C systems are wished for, and it should be evaluated if the requested functionality can be achieved by other technical solutions. It is desirable to have an established strategy where changes (in existing I&C systems) are limited to changes of absolute necessity.

Graph 7 in Appendix 3 shows that the NPPs are unsatisfied with the lifecycle emphasis during I&C modifications.

4.2.1 Resources and Competence



Graph 1 Report. The NPP has sufficient I&C competence internally including consultants (without help from suppliers).

OKG and FKA have expressed a difficulty in recruiting and maintaining resources for I&C, much because of the geographical position of the NPPs. Even though OKG from the beginning made a strategic choice to have enough competence to make I&C changes in-house, OKG has not been able to follow their strategy. OKG and FKA have partly because of the situation with lack of competences, chosen to involve the supplier for changes in I&C. *[Interviews, 2015]* (Graph 1 Report)

RAB has expressed a better recruiting situation then OKG and FKA. The resource situation at RAB is better because of the geographical position of the NPP (more and larger cities are within commuting distance). Also, many of the participants involved during project RPS (R1) and project TWICE (R2) are still employed by RAB and a lot of the consultants are still at assignments at RAB. *[Interviews, 2015]* (Graph 1 Report)

Since R1 does not have test equipment for TXS, their strategy has been to use Areva for testing but to perform the I&C changes (design and coding) in-house. *[Interviews, 2015]*

R2 took at strategic decision during project TWICE to have development and testing of I&C changes in-house. *[Interviews, 2015]*

R3/4 are vulnerable when it comes to competence for Spec 200 that is no longer supported by the supplier. *[Interviews, 2015]*

4.2.1.1 Supplier

Oskarshamn, Ringhals and Forsmark have all expressed a willing to involve the supplier when making changes in I&C systems. *(Appendix 3, Graph 6)* A majority of the participants in this study have expressed the supplier as a more cost effective alternative when making changes in I&C systems, instead of in-house development. *[Interviews, 2015]* The opinion among the interviewed participates (all NPPs) are that there are cost benefits in using the supplier for changes. It is believed to be cheaper for the NPPs to use suppliers since all I&C competences do not need to exist in-house. Even though, the cost for the supplier is expensive and it is hard to achieve a competing situation since the platform is strongly connected to a certain supplier, it is still believed to be cheaper for the NPPs to use the supplier in the long run.

Several of the NPPs have expressed a concern regarding the suppliers' possibility to support installed I&C systems. An example is Spec 200 at R3/4, where the supplier does not have enough competence to support the system (not even international competence). *[Interviews, 2015]* This leads to a risk for R3/4 since they are forced to have all necessary Spec 200 competence in-house, and cannot get any support from the supplier. A strategy to avoid this situation is to continuously use the supplier for I&C changes, to let them have a business interest in the NPP so that they keep competence. This is an unspoken strategy used by several of the NPPs, to prevent the supplier from stop providing support.

Having a good collaboration and communication with the supplier during I&C changes is expressed as a success factor at all the interviewed NPPs. The complexity when making changes in I&C systems makes communication vital. Too only have formal or little communication between NPPs and suppliers leads to a more inefficient collaboration and risk for quality problems. Even though a certain degree of independence is important for questioning and reviewing, the benefits of a close collaboration is expressed as crucial among the interviewed persons. *[Interviews, 2015]*

4.2.1.2 Strategy regarding number of platform types at site

As discussed in 4.2.1, the studied NPPs have expressed difficulties in recruiting and retaining personal for I&C platforms. Having different types of platforms at site forces the engineers' to have knowledge in and keep up to date with more than one platform type. Maintenance engineers at especially O1 and R3/4 have expressed vulnerability in competes if problem arises in certain I&C systems, since the resources are limited. *[Interviews, 2015]* Having fewer types of I&C platforms makes it easier to have necessary competence in-house.

Forsmark 1-3 all have Numac in the safety system (WRNN & PRNN) and in the non-safety system (ATIP). *(Appendix 1)* It gives Forsmark the possibility to use the same personal for all three plants, which makes them less vulnerable if problem arises in the systems.

4.3 Platform

When comparing platforms at the NPPs there is no situation that is completely comparable with another, se summary in 4.2. However some conclusions can be made from a platform perspective, see 3.3 for background information, that will be accounted for in this chapter.

When comparing TXS with AC160, there are some advantages that are highlighted by the interviewed software engineers. E.g. TXS have visual coding which makes it easy to review and perform changes compared to AC160. An advantage with AC160 is the robustness of the platform which makes it very reliable during operation. However, according to participants in this study, it is not the label of the equipment that matters most when performing changes in the PE system. It is the choice of configuration and included functionality that have most impact on the complexity. *[Interviews, 2015]* To some extent, this is set by the configuration of the plant such as diversity, number of subs etc.

There are strategic platform choices and prerequisites that have large impact on the changeability of the platform. In the following chapters, the most important aspects that have been found during the study will be presented (from a platform perspective).

4.3.1 Functionality

Safety functions are in its basic design very simple. Safety systems used to realize safety functions shall be robust, transparent and reliable. *[Interviews, 2015]*

When a PE system that has a full adjustable programing environment is used for safety functions a complexity arises. It is easy to add functionality and communication, which makes it temping to add more functionality then necessary for the task. When used to supervise and steer safety functions which are simple in their basic design, the adjustable programing environment creates an unnecessary complexity. When implementing the safety functions in a PE system, a higher complexity arises compared to when an analogue system is used. For analogue systems, it is easier to physically limit the area of changes. For digital systems, changes can affect nearby functionality which makes it hard to argue that everything in the system is complete and correct verified. *[Interviews, 2015]*

This states that few functions implemented in a PE system makes it easier when performing changes. Do not add “extra” functions if not necessary, se next section.

4.3.1.1 No “extra” functions

The safety related system Ovation at R2 has “extra” functions implemented that are not safety related functions (e.g. alarm instructions). This type of function does not have to be in the safety related system, but has been implemented as a help for the operators (instead of storing the information in the primary documentation tool “Darwin” at Ringhals). When changes are made in the alarm instructions, the changes needs to go through the whole Ovation developing, release, test and installation process, which leads to higher costs and longer lead times. *[Interviews, 2015]* Having this kind of “extra” functions in a PE system is positive from an operative perspective, but it is costly when changes are required in the system.

O1 have CAT A, CAT B and CAT C in their AC160 platform. *(Appendix 1)* They have not indicated that there is a problem with this, but it is something to consider when new equipment shall be installed. Do not add more functions in the same platform then necessary.

4.3.1.2 Diversify digital I&C platforms with analogue technology

At R1, TXS are used for safety system (DPS) together with a diversified analogue system (OPS). *(Appendix 1)* Having different technologies for the safety system, one analogue and one digital part, gives both diversity and redundancy that has been appreciated by the Radiation Safety Authority. It is believed to increase safety and confidence. *[Interviews, 2015]* Diversified/redundant system is a strategy important for R3/4 to consider since they need to exchange I&C systems before decommissioning.

4.3.2 Platform architecture

4.3.2.1 Stand-alone Platform

Having isolated PE systems, which do not communicate with other PE systems, makes it easier to perform changes. The potential side effects when performing a change are then physical limited. *[Interviews, 2015]* R2 has integrated AC160 and Ovation deeply in the power plant, and Ovation receives signals from AC160. At e.g. O1, where the AC160 system and AC450 are more isolated from each other than AC160 and Ovation at R2, changes are less complex. To what level the systems are communicating with each other has consequence when making changes. PE system for neutron flow measure is an example where most NPPs have stand-alone platforms, see Table 3.

4.3.2.2 Few functions per PE system

Having few functions implemented in an I&C platform makes it easier when performing changes. The changes potential side effects are limited to affect fewer nearby functions. At e.g. FKA, where three separate Numac platforms are used for neutron measure (WRNN, PRNN and ATIP, see *Appendix 1*), it is easier to performing changes than if all the functions where in the same Numac platform (in this reasoning the aspect of diversified system is ignored). Another example is R1 that has three stand-alone TXS platforms for the Safety System, which simplifies changes compared to R2 where one I&C platform (AC160) is used in the Safety System *(Appendix 1)*.

4.3.2.3 Stand-Alone processors

R3/4 has configured Foxbora Spec 200 and WDPF with stand-alone processors. *(Appendix 1)* Stand-alone processors make changes easier since potential side effects of the change are limited to the affected processor. At Oskarshamn 1-3, Ringhals 1-2 and Forsmark 1-3, where stand-alone processors are not used in the same extent, verification of changes becomes more complex. If the numbers of functions in each stand-alone processor are few, the potential side effects are even more limited.

4.3.3 Platform capacity

It has been notices by several participants in the study that the systems built in functionality are not fully used. The systems often have e.g. self-monitoring functions that are not used. Using the systems build in functionality could simplify changes. *[Interviews, 2015]* These built in functionality is an advantage compared with analogue systems and if it is not used, the full potential in having a digital system disappears. A reason why NPPs are not using built in functionality optimal, is that the functionality has not been qualified and there is an uncertainty in how trustable the results from the systems are. This is an area that Elforsk is recommended to investigate more, and give suggestions in how this kind of functionality could be used in a quality ensured way.

4.3.4 Tools

Suitable tools are of great importance when making changes in a digital system. It directly affects the developing and testing process and has a large impact on quality and cost during changes. Suitable tools reduce the risk of introducing errors during changes and increase the possibility of finding errors early in the process. The earlier errors are detected, the less it costs to correct it. [1], *[Interviews, 2015]*

Tools that accordingly to this study have a large impact on NPPs' quality and cost during the change process in PE systems are discussed below.

4.3.4.1 Code comparing tool

Suitable software tools when comparing differences in released code are of importance from a quality and cost perspective. *[Interviews, 2015]*

With a suitable code compare tool it is easier for engineers to compare the code releases. It leads to A) more detected errors in the code and B) less time spent in comparing the code. To have a good process and quality when comparing differences in the code release is important for being able to argue that no changes have been made to any other functionality than the one intended (code comparison is a part of the argument). Several of the interviewed software developers have mentioned that R1 have a good tool for comparing the code in TXS which makes it visible and easy to review.

If large in-house projects are to be realized in NPPs in the future, it is highly recommended that the NPPs invest in suitable tools for comparing code differences. Several tools exist on the market.

4.3.4.2 Requirement tool

None of the examined NPPs uses a software tool designed for requirement handling. Several engineers have expressed the need of such a tool to be able to effectively handle requirements during developing and testing. Much administrative time is today spent on handling requirements and verifications. *[Interviews, 2015]* A suitable requirement tool can increase the development and verification process as well as delivering better quality.

A requirement tool is recommended for those NPPs that are performing large changes in software as well as for plant systems and complete plant.

4.3.4.3 Test tools

For more "simple" PE systems (stand-alone processors or PE systems with little communication, e.g. WDPF and Spec 200 at R3/4), a simple test tool consisted of one electrical enclosure with processors are to prefer. It is a cost effective tool that can be used for testing in an early stage of development. It can also be used for training. At R3/4, this strategy has led to great results when handling changes in WDPF and Spec 200. *[Interviews, 2015]*

For more complex digital I&C platforms (with much communication, e.g. AC160 at O1 and R2), a more complex test tool is needed. R2 has solved it with an advance replica of the plant called LES (1 of 4 subs), while O1 are using Westinghouse for testing. *[Interviews, 2015]* Both strategies are functioning well and there are no arguments suggesting that any of the NPPs shall change strategy regarding test tool. However, if a new digital I&C platform with a high complexity are acquired by a NPP, it is recommended to secure the suppliers ability to test changes instead of acquiring an advanced testing tool to have in-house. A test tool needs to be maintained and it needs competence. There is a risk that it will be expensive to have the test tool in-house in correlation to the number of changes that are being tested. Furthermore, it gives a natural independence between design and test if the supplier is performing the code testing (including FAT).

4.3.4.4 KSU

Several of the NPPs have stated KSU's review of code changes as a much appreciated activity. In KSU's simulator, tests are often performed differently from most FATs. *[Interviews, 2015]* Even though the opinions differ in whether KSU can be used for official testing or not, using KSU for in-official testing can still contribute with valuable information. KSU has a powerful simulator that should be used for controlling the correctness in I&C changes.

4.4 Working Process

4.4.1 General

Standards that NPPs must comply with when introducing PE systems for safety functions points out the importance of having a structured way of working from concept to end of use, se chapter 3.1.1. The working process has phases where verification activities need to take place and be documented after each phase. It means that all verification cannot be performed as commissioning's tests in the plant.

The standards also require a life cycle perspective that forces the NPPs to look beyond the projects that are performing the changes. There must exist a plan and strategy for administration of the platforms and documentation over time.

Graph 3 in Appendix 3 indicates that the NPPs do have improvement potential of processes/instructions for I&C changes. For enabling improvements to the processes, it is suggested to derive KPIs for optimization.

All NPPs have established QMS and project management methods for performing changes in the PE systems. However, there are some areas that have impact on the efficiency and quality over time that the NPPs are recommended to look into. Those aspects are discussed in this chapter.

4.4.2 Administration, configuration and documentation management

To be efficient over time a life cycle process is essential, not only focusing in the performance of projects. The administration over time is an essential part, se chapter 3.4.3. To store the documentation in a structured way that makes it easy for future projects to find and understand the design concepts saves time. A project is not only documenting for their own benefits, but also for coming projects to understand their strategic decisions and conceptual choices. Since an I&C system is complex and is covering more than one plant system, it is of importance to have a configuration strategy regarding the handling of product information for the involved plant systems (where to find requirements, design and verifications). From a lifecycle perspective, projects are encouraged to work in plant documentation instead of project documentation when possible. Graph 7 in Appendix 3 indicates that there are insufficient emphases in lifecycle among all NPPs, and Graph 9 indicates issues in documentation.

Participants in this study have expressed an irritation in how the suppliers' documentation is received and managed at the NPPs (especially a problem at R2 after project TWICE). *[Interviews, 2015] (Appendix 3, Graph 9)* Not having a clear and well planned strategy in how to maintain and update suppliers' documentation leads to inefficiency when new changes are made. Having a documentation strategy and clear interfaces supplier/NPP are recommended for all future changes where a supplier is used.

Strategies for how to package projects, what scope to give them and how to coordinate them over time is essential for efficiency and to minimize misunderstandings and design collisions (see chapter 4.5.1 for examples). A program management process could be applicable if the NPP are planning to perform many projects, both over time and per outage. Project order and scope is perceived as problematic among most of the NPPs, see Graph 12 in Appendix 3.

4.4.3 Requirement process

According to Standish group, 24 % of all failed projects depend on incomplete requirements and specifications or by changes of the requirements and specifications. Good requirement management has a significant role in the success or failure for a project. [3] The examined NPPs all have expressed weaknesses in their requirement handling. Project managers and Engineers have expressed requirement handling as an important factor for success in I&C projects. *[Interviews, 2015]*

4.4.3.1 Front loaded requirement process

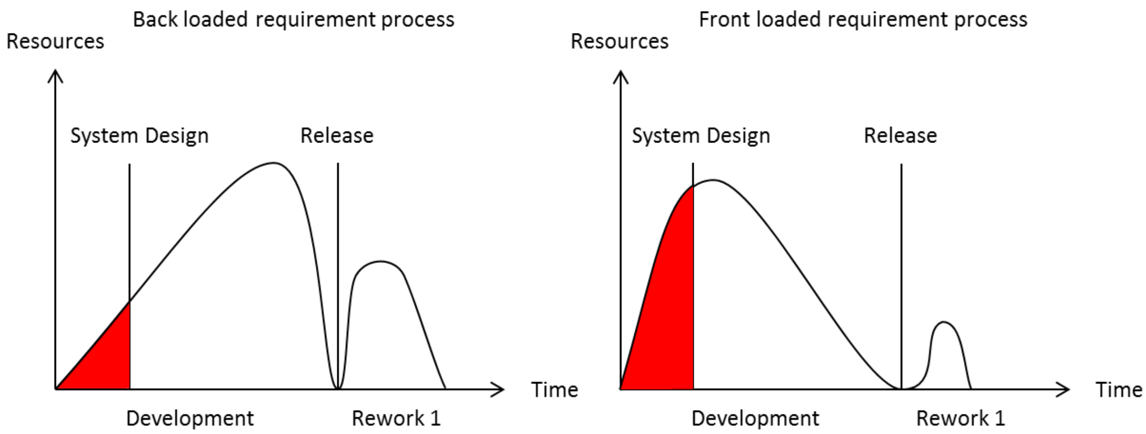


Figure 8. Back loaded VS Front loaded requirement process.

Studies show that poor decisions early in the development process have an exponential impact as the project develops; costs and time might increase drastically. In Lean development, the front loaded approach is promoted. [2]

A majority of the examined NPPs have expressed a willing to involve more I&C competence early in the development process*. [Interviews, 2015]* This strategy enables 1) more cost effective solutions for I&C and 2) get it right from the beginning (less changes).

At R2, Project PICUP has been responsible for all I&C changes during the last years. Plant projects at R2 have delivered input requirements for PICUP to realize in I&C at different time points. It has created difficulties for PICUP since the scope has changed constantly. The focus on I&C in early phases has been inadequate (phases where the plant projects have been responsible) which lead to changes that are discovered late in the process. Changes are costly since they might require rework in the code, new release and additional testing. *[Interviews, 2015*] According to chapter 3.5 Projects, most time can be saved in the phases of detailed design and code verification. To make this possible, input requirements and specifications must be correct.

A front loaded development approach may be even more important at OKG and FKA since the supplier is used to a large extent. Several of the interviewed engineers at OKG and FKA have expressed the importance of a well-made requirement specification when using a supplier. Changes are expensive and the later insufficient requirements are discovered, the more expensive they are to correct. The need of a complete plant/system level design (process design) before starting with I&C design is requested by several of the interviewed. *[Interviews, 2015]*

4.4.4 Inherited processes

I&C development at Oskarshamn, Ringhals and Forsmark all have experienced consequences from inherited processes, mostly from the NPPs' process for changes in *electrical equipment* and the *suppliers' process*. The inherited processes for *electrical equipment* are not always adjusted to fit system/software engineering in an ideally way. *[Interviews, 2015]* When inheriting processes, it is important to ensure how it is value adding and to eliminate existing equivalent processes.

The inherited process for changes in *electrical equipment* creates heavy processes that do not utilize the agile potential with software development fully (e.g. first coding on paper instead of directly in the development system). *[Interviews, 2015]* However, such a change of the QMS must be quality ensured before taken into operation. There is a study [10] comparing Scrum and IEC 60880 [5] that can be used for inspiration regarding this subject. RAB is performing a business development project, for improvement of process and instructions for changes in PE systems (how to manage changes more efficient, how to work according to standards etc.).

The inherited *supplier processes* are difficult to map towards the NPPs' existing processes (QMS etc.) and less traceability exists towards standards and guidelines. *[Interviews, 2015]* When inheriting processes from the supplier, it is important to ensure that the processes support the life cycle perspective of the systems, and not only focus in new development.

4.4.5 Roles

Several of the interviewed I&C project members have expressed overhead project roles as costly (e.g. roles for time planning, quality, project management etc.). *[Interviews, 2015]* This is not a unique situation for I&C

projects, but a general balance for all NPP projects. The necessity of certain overhead roles should be reviewed for more cost effective projects. However, this must be done with the life cycle perspective in mind. Cost benefits from a project perspective can be costly from a life cycle perspective, e.g. cutting resource for document management could be costly for the next coming project.

When changes are made in I&C systems it is important to have a certain degree of independents between the different roles. *[Interviews, 2015*] Development and Test shall be independent, enabling the roles to create a fresh viewpoint of problems and to encourage questioning. Many of the relevant standards for software development support this (e.g. IEC 60880 [5], IEEE 1012 [8] and IEEE 12207 [9]). When major decisions are made, because of the complexity in PE systems, it is recommended to involve several different roles.

4.4.6 Verification

Changes in PE systems cannot be limited to verification and testing of the end product, i.e. the computer code. Factors such as the quality of the processes and methods for specifying, designing and coding have an important impact on the result. [1]

The later an error is detected, the more expensive it is to correct it. Discovering an error after installation, e.g. during SAT, is very expensive since the development process normally needs to be iterated (if not live coding in the PE system is allowed). *[Interviews, 2015]* It is recommended to perform as much verification as possible early.

Verification of PE systems consists of several activities (reviews, analyses, testing etc.) during all phases. Test is often the verification activity requiring most resources and it is time consuming. The study has therefore focused in test strategies and test processes.

4.4.6.1 Testing

Testing requires much time in I&C projects (see Table 4). In order to create independence between Development and Testing, it is recommended that both teams base their input on the same specification. It is recommended that the requirement specification is designed to suit both development and testing's needs (design specifications are in general formulated conservatively, and therefore focus mostly in the needs of Detailed Design). Requirements shall be stated in a verifiable way and involving test resources early can help improving the verifiability of the requirements.

Several of the interviewed NPPs are attempting to reuse test cases from earlier projects when performing FAT and SAT. However, it is difficult to find earlier tests since they generally are not saved in a proper "test library". New tests are then often designed solely to test the implemented change.

[Interviews, 2015] If tests where to be saved in a “test library”, clearly describing what functionality they are made for, it would be easy to e.g. reuse tests, write new tests or to re-validate the whole platform. R3/4 have in a successful way saved all tests for WDPF and Spec 200 in a “test library”, making future changes and re-validation easy.

Other opinions are that the complete test set-up, from verification of code to DKV is not optimized. *[Interviews, 2015]* Testing must be overlapping but each test must have a clear purpose to avoid unnecessary repeating. Make sure that the test set up is beneficial. To start early in a project with a complete V&V strategy and plan is recommended to optimize the testing activities.

For test equipment, see chapter 4.3.4.3 Test tools.

4.4.6.2 Regression analysis and testing

IEEE 1012-2012 *Standard for Software Verification and Validation* [8] defines regression analysis and testing as follows:

> ***“Regression analysis and testing.*** *Determine the extent of V&V analyses and tests that must be repeated when changes are made to any previously examined software products. Assess the nature of the change to determine potential ripple or side effects and impacts on other aspects of the system. Rerun test cases based on changes, error corrections, and impact assessment, to detect errors spawned by software modifications.”*

The NPPs needs to have a strategy for how to handle regression analysis and testing when performing changes in PE systems. Ringhals 1 and 2 have started reasoning about the concept of regression during the in-house projects TXS and PICUP.

Having a test library (see previous chapter), that enables tests to be repeated after changes are made to the system, is one way to handle regression (performed by R3/4). Conducting deep code analysis and tests to detect potential side effects of changes is another strategy to handle regression (performed by R2). R1 is using DKV (hardware and software are tested together) in the regression argumentation*. [Interviews, 2015]* The strategies for regression depend on the changes made to the system as well as the technology and configuration of the system. Having a strategy for how to handle regression analysis and testing is important to optimize the need of testing and further studies in the subject is recommended.

4.4.7 Licensing process

NPPs have during interviews described vagueness in what kind of material that SSM requires from I&C projects. Graph 29 in Appendix 3 also indicates an uncertainty among the NPPs regarding contact with SSM. Oskarshamn, Ringhals and Forsmark all have a willing to have a closer dialog with SSM regarding I&C changes. Also SSM sees the potential in having a closer dialog with I&C projects, enabling SSM to observe more during the development process. *[Interviews, 2015]* Both the NPPs and SSM sees the potential in having discussions about requirements, standards and reporting material, which could save time for both parts by initiating an early dialog.

The NPPs need to have a more pedagogic documentation structure, from incoming requirements to validated I&C platform. With a clear documentation structure, the NPPs have better control and SSM can follow changes in I&C more easily, se section 4.4.2. *[Interviews, 2015] (Appendix 3, Graph 9)* It is important to plan the documentation structure before starting with I&C changes, enabling a clear structure. To produce documents costs time and a non-pedagogic documentation structure creates confusions which could lead to quality flaws.

The NPPs need to argue for the total change of the PE system and the complete plant, what have been done and how is it ensured that all functionality is according to specification (no unwanted changes has been performed). Elforsk has released recommendations related to this topic in report 13:86 [11].

4.5 Projects

Most possibilities to save time and money during development are in the phase from detailed design to performed FAT (since this is where most engineering hours are spent, see Table 4). For OKG and FKA this part is performed within the suppliers' QMS and their processes but the input is generated by the NPPs. The more accurate the specifications used as input for the supplier are, the less changes are required (changes takes time and costs money). The interviewed NPPs have expressed the need of more time during the specification phases (Plant and System design) to avoid rework. *[Interviews, 2015]*

4.5.1 Packaging and Coordination of I&C projects

The project or line organisation responsible for I&C changes should have total responsibility for re-validation of the system (including hardware, system software and application software). The project or line organisation should have a well-defined scope of their changes and responsibilities. *[Interviews, 2015]* This is a best practice expressed by several project managers. Dividing or sharing the responsibility of changes in the platform is not recommended.

At R3/4, each plant project is responsible for their own changes in I&C, which makes it more difficult to coordinate changes. At R1 and R2, one project (project TXS and project PICUP) is responsible for all I&C changes. *[Interviews, 2015]* If changes are made in-house, it is recommended to have one project or line organisation responsible for handling <u>all</u> the I&C changes, since A) changes should be made by few well informed resources to avoid misunderstandings and B) one actor needs to take full responsibility to re-validate the I&C platform.

R2 initiated a program management team for steering and coordination of 56 projects that were performing changes in R2 during 2014 and 2015. Around a third of the projects were having impact on I&C and even thought a specific project for handling all the I&C changes existed (project PICUP), steering and coordination from a program where necessary to succeed. *[Interviews, 2015]* Depending on the number of projects and the complexity of the changes, a program (steering the projects) or a coordinating role (supporting the projects) is recommended for the NPPs. An experience from R2 is that much effort need to be spent on interfaces and coordination between projects to succeed with I&C changes.

R1 made an early plan for all coming changes related to SSMFS 2008:17. A Program was established creating the complete conceptual design and packaged the projects (establishing the scope for them) and coordinated the projects during performance over the years. The Program gave R1 a good plan for all coming changes that had an impact on the PE systems, and R1 avoided e.g. design conflicts both for the PE system and for the plant in large.

These are two examples of how NPPs used Program Management for packaging and coordination of projects. It had positive effects, especially when a lot of changes where planned for. Graph 12 in Appendix 3 indicates that most NPPs find project order and scope for I&C projects problematic.

Even though no large amount of changes are going to be performed by the NPPs, or if the supplier is used for I&C changes, it is recommended to have a coordinating role for I&C even if it is not as comprising as a whole Program.

5 Conclusions

The project will answer to the following research questions:

- *Could a different approach in the design make the modification tasks easier with an increase in safety, quality and cost effectiveness?*

  Yes, however the largest impact is made when the equipment is chosen and configured for the first time. Aspects that have a huge impact for the future are such as:

  - Prerequisite
    - Chosen functions and concept (analogue/digital)
    - Choice of platform from a maintenance and competence perspective
  - Design constrains
    - Platform architecture, amount of processors etc.
    - Communication between platforms and between processors
  - Efficiency
    - The use of built-in functionality
    - Platform tools

  The more functionality that are installed in the platform and the more communication, both internally and externally, the more complex it will be to change and verify the system. Perform technical risk analysis when planning to introduce new functionality into an existing platform.

  According to this study, it is not the label of the equipment that matters most when performing changes in the PE system. It is the choice of configuration and included functionality that have most impact on the complexity.

- *How do different approaches in the work processes for modifications influence the quality and cost effectiveness for the modifications?*

  In the way the NPPs work today they reach a high quality level. They find a very small amount of faults in SAT and commissioning. Even so, it is always a challenge to prove that “nothing else” has been affected which requires a structured way of working and a competent staff. Even if the suppliers are performing all changes or part of it, the NPP is always responsible for the result and needs to be able to review the design and test results. Furthermore, they need to be able to argue for the rationales, nothing has been affected that should not be affected. From a cost effectiveness perspective there are reasons to look over the working methods the plants have today. None of them have a perfect set-up of working methods. RAB is performing a lot of the work in-house compared to FKA and OKG. However, FKA do not have as complex systems as RAB and OKG. Neither have FKA performed that many changes since installation. Neither O1 has made that much changes since AC160 was installed compared to what R1 and R2 have done. Therefore, it is hard to compare which strategies that are most cost efficient. None of the plants are working agile today, and therefore there is no best practise regarding if this is a possible and effective working approach. Some aspects to consider for the future from a quality and cost effective perspective are:

- Life cycle management
    - Create life cycle cost estimations when considering buying new equipment.
    - Create Life cycle strategy plans for the existing PE system.
    - Packaging of project
    - Administration and documentation
- Project management
    - Front load the process (RM approach)
    - Consider a more agile approach This must however be more investigated and quality assured before it is taken in use
    - Optimize the V&V and test set up
    - Coordination of projects
- Strategies
    - Supplier strategy
    - Secure competences both at supplier and in-house
    - Licensing process

5.1 Safety and Quality

Methods and processes

All the NPPs have processes suitable for their task from a quality perspective, but they all have indicated that there are potential for improvements from an efficiency perspective. For enabling improvements to the processes, it is suggested to derive KPIs for optimization.

Available competent resources

All NPPs have available resources for the moment but for some roles they indicated that they are vulnerable for absence, retirement and ending of position. It is also important that their suppliers can keep competent resources for support over time.

Safety culture and behaviour

All NPPs indicate that their safety culture is well and that working processes are followed. When performing efficiency improvements of the processes, it is critical to balance the efforts in a way so that the safety culture is not jeopardized.

5.2 Cost and Efficiency

Life cycle cost

The NPPs have generally not taken into account what the life cycle cost for administration and changes in PE systems costs over time.

Project cost / Efficiency within the projects

All NPPs indicates that there are efficiency improvements that can be done in their processes. Their working methods are not optimal for changes in PE systems and the full potential of the software is not used.

In-house versus supplier

The NPPs are using the supplier differently. RAB are performing most of their work in-house compared to OKG and FKA that are using the supplier for all detailed design and testing. All NPPs are positive in using the supplier. To what extent the supplier should be used need to be evaluated in relation to the amount of changes that needs to be performed during the coming years.

6 Recommendations

6.1 General

A starting point for the NPPs is to:

- Identify which standards to apply and interpret them according to the NPPs' need.
- Implement the interpretation of standards in the QMS and keep traceability to where different parts have been implemented.
- Be strict about nomenclature, especially when both IEC and IEEE are used at the NPP.

This gives the basic requirements for the processes and needs to be handled before efficiency improvements can be performed.

6.2 Strategy

For an I&C platform, many strategies are established in early stages of the life cycle and it is hard to change the strategies later on. The NPPs are recommended to thoroughly investigate the business case before making strategic decisions and from the beginning create a life cycle plan, see 6.2.1.

When changing existing I&C-platforms the following aspects should be considered:

- From a strategic perspective, it is recommended to be selective when accepting changes in PE systems. It should be evaluated if the requested plant functionality can be achieved by other technical solutions than implementing into an existing PE system.
- If few changes are planned, this study indicates that NPPs are more satisfied using the supplier for changes. It is believed to be cheaper for the NPPs to use suppliers since all I&C competences do not need to exist in-house.
- It is recommended that the NPPs regularly provide the supplier with assignments, for the supplier to have a business interest in the NPPs and to keep up-to-date with competence. It is a risk if the suppliers lose competence or interest to support the installed I&C systems.
- It is recommended to have a close collaboration and communication with the supplier during changes.
- It is recommended for the NPPs to have strategies for how to receive the suppliers' documentation and how to administrate it over time.

- If changes are made in-house, it is recommended to use the supplier for independent reviews.

Several NPPs in Sweden have a great difficulty in recruiting and maintaining competence for digital I&C. The following competences are vital for the safety of the I&C systems over time:

- Competence for plant design shall exist in-house. The supplier can never have equivalent knowledge in the plant design as the NPP.
- Competence for purchasing and reviewing I&C system design shall exist in-house. The NPP need to have sufficient competence when evaluating the suppliers I&C solutions and test results.
- Competence for integration of I&C systems shall exist in-house. The supplier is expert in I&C systems, but the NPP need to have the knowledge in how to integrate I&C systems into the plant.

6.2.1 Strategy life cycle

The NPPs are recommended to develop a life cycle plan for I&C systems, with a profound analyse of the I&C systems status and activities until decommissioning. The activities should be costs estimated and planned in time. With this information, the NPPs can make sustainable decisions from a life cycle costs perspective. The strategy should as a minimum include the following information:

- Coming updates of the software.
- Replacement of hardware.
- Planned changes in the system (backlog, plant changes etc.).
- Regression strategy (how to handle regression analysis and tests).
- Lifecycle Verification and Validation.

6.3 Platform

This research study indicates that strategic decisions (chapter 4.2) combined with the configuration of the digital I&C platforms affect the ability to perform changes more than the choice of product (label of PE platform).

The following strategies are important when acquiring and configuring a new digital I&C platform:

- Standardized product type.
- Several separated and isolated I&C platforms rather than few large and joint.
- Diversify digital I&C platforms with analogue technology.
- Stand-alone processors.
- Minimum number of functions per processor.
- No "luxury" functions that are not necessary for the primary task of the I&C system.
- Purchasing of spare parts when acquiring a digital I&C system.

The following strategies are important when making changes in an existing digital I&C platform.

- Not making changes in the I&C platform that are not of great necessity.
- Not adding "luxury" functions that are not necessary for the primary task of the I&C system.
- Start to use of the systems built in functionality, e.g. self-monitoring of the systems operating status, if the functionality can be quality ensured.

6.3.1 Platform tools

Having suitable platform tools are of great necessity for an effective change process. The following tools have been highlighted by interviewed personal in this research study:

- Suitable code comparing tool (leads to higher quality and more time effective process).
- Requirement tool for requirement handling (especially recommended for those NPPs that are performing many changes in the software, and for the complete plant).
- Testing tool (in correlation with the NPPs supplier strategy).

6.4 Working Process

The following aspects are recommended from a process perspective:

- Establish life cycle processes, including administration process and packaging of project (scope optimization)
- Adapt inherited processes to suite development of system/software.
- Investigate if and how an agile working approach can be used.
- Front loaded I&C development, including requirement management.
- Involve I&C competence early in the change process (plant level), to choose cost effective solutions for I&C, avoiding costly I&C design and late changes.
- Evaluate how resources are used to create most value, both within the projects and for the whole life cycle.
- Evaluate where independence between roles is applied and necessary. Design versus Test.

6.4.1.1 Requirements

Correct requirements from the beginning to avoid changes during the development process have a significant impact on the result.

Have a single point of delivery for all I&C requirements that are to be implemented in the coming software baseline. It decreases the number of changes during software development.

6.4.1.2 Testing

- Perform as much tests as possible early in the process.
- Advocate large scale FAT instead of SAT.
- Evaluate the complete set of test to be perform and try to optimize, are all tests contributing and in what way. Can DKV be used more efficient, etc.

- Design requirement specifications and design specification to fit also for testing.
- Save test cases as plant documents and structure test cases per function, enabling a test library for future tests in I&C.

6.4.2 Licensing process

Initiate a dialog between I&C projects and SSM early in the change process. Discuss perception of requirements, standards, licensing material etc.

Pedagogic documentation structure, from incoming requirements to validated I&C platform would be beneficially in the communication both internally and externally, with e.g SSM.

6.4.3 Projects

If several projects effects the I&C system with their changes, have one I&C project responsible for validation of the I&C-platform. If a supplier is responsible for performing I&C changes, someone at the NPP still needs to be responsible for validation of the I&C platform. Depending on the number of projects and the complexity of changes, a program (steering the projects) or a coordinating role (supporting the projects) should be introduced at the NPP.

If I&C changes are performed by a project, it is recommended to define a clear project scopes which includes responsibility for hardware, system software and application software.

6.5 Recommendation to Elforsk

These are areas of interest that are suggested for future investigations by Elforsk:

- How to work with regression analysis and test? What is recommended from a test library perspective?
- How to work agile but still comply with standards and deliver quality ensured changes?
- How to improve requirement management and use of tools?
- How to derived KPIs for methods and processes, enabling improvements to be made?
- How to use system built in functionality in a quality ensured way?
- Benchmark with NPPs around the world?
- Collaboration between Nordic NPPs regarding I&C strategies and processes?

7 References

[1] 2013:08 Licensing of safety critical software for nuclear reactors – Common position of seven European nuclear regulators and authorized technical support organisations. Revision 2013

[2] Morgan, J.M., Liker, J.K., 2006. The Toyota Product Development System Integrating People, Process, and Technology. Productivity Press, New York

[3] 2014, The Standish Group Report, CHAOS

[4] IEC 61513 ed2.0, 2011, Nuclear power plants - Instrumentation and control important to safety - General requirements for systems

[5] IEC 60880, 2006, Nuclear power plants – Instrumentation and control systems important to safety – Software aspects for computer-based systems performing category A functions

[6] IEC 62138, 2004, Nuclear power plants – Instrumentation and control important for safety – Software aspects for computer-based systems performing category B or C functions

[7] IEEE 603, 2009, Standard Criteria for Safety Systems for Nuclear Power Generating Stations

[8] IEEE 1012, 2012, Standard for System and Software Verification and Validation

[9] IEEE 12207, 2008, ISO/IEC/IEEE Standard for Systems and Software Engineering - Software Life Cycle Processes

[10] Scrum and IEC 60880, 2013, Stålhane Tor, Katta Vikash, Myklebust Thor.

[11] Safety Demonstration Plan Guide, Elforsk Rapport 13:86, 2013, Axenborg Marie-Louise, Ryd Pontus

[12] RAB-Processbeskrivning för V&V inom processen Ändra Anläggning, Darwin ID 1946414

[13] AB/FKA, VPMM on-line

[14] FKA- Anläggningsförnyelseprocessen, F-I-2873

[15] OKG - Konstruktionsstyrmodell (KSM), Konstruktion av system innehållande Programerbar teknik, 2005-10151 (V'et)

[16] OKG - Oskarshamnsverket - Beskrivning av faser och besluts-punkter för Anläggningsändringsprojekt, 2007-02994

Appendix 1
Comparison matrix NPPs I&C platforms

	O1 – Safety System	O1 – Safety Related System	O1 – Non Safety System	O2 – Safety System	O2 – Non Safety System	O3 – Safety System
Platforms	AC160 from WEC TXS from Areva (for system 531)	AC450 from ABB. Operator interface constructed with ABB Advant OS (UNIX) Block computer ABB SPIDER.	Different advant systems (ABB system)	TXS from Siemens	TXP from Siemens Here the old TXP or SSAP/T2000 (new name for TXP) is used together with Siemens S7	TXS from Areva
I&C platform application and functions	Reactor Protection (RPS) and all other Cat A functions in EKB (backup control building). Neutron flow measurements PRM WRM, SRM, IRM, APRM, LPRM, SIRM system 531	ABB450 CAT B functions in the "main electrical building" are implemented in AC450, all other in AC 160. For SRS there is a big difference between the O1/R2 platform extent. The O1 platform is comparable to the R2 block computer function.	All operation and service functions	Reactor Protection (RPS) including DPS Neutron flow measurements PRM WRM, SRM, IRM, APRM, LPRM, SIRM system 531	All operation and service functions.	Neutron flow measurements PRM WRM, SRM, IRM, APRM, LPRM, SIRM system 531
I&C platform insertion year	Project MOD installed 2001-2002. Neutron flow measurement installed 1997.	Project MOD installed 2001-2002.		PLEX ongoing. Neutron flow measurement installed 2000 but will be updated during PLEX.	Project Turbic (turbine I&C) installed 2007.	
Projects that have been done on the platform. Scope of project.	The Autobor project has done the only function change (that were outside the qualification). Some smaller logic changes (alarms/measurement points) and parameter changes have been made. HW (CPU card changed), SW new version (high speed link).	Some smaller logic changes (alarms/measurement points) and parameter changes have been made.	Only smaller changes in operation system have been done in O1, changes in service functions.	No changes in neutron flow measurements besides corrections of errors. Otherwise PLEX.		
Architecture basics (number of subs, processors, communication links etc.)	Number of subs: The logic is built in four subs where AC160 is used for CAT A, B and C functions. All that belongs to EKB is found in AC160. Number of electrical enclosures: 12 Cat A and 16 Cat B Number of Processors: AC160 has 174 processors Communication Communication between the subs in Cat A is done via High Speed Link while all other communication is done via Advant Fieldbus 100 Other: O1 has no ODP or MTP screens (R2 has) There is a diversified RPS system (516-DPS) that is realised with electronic cards from Foxboro.	AC450 approximately 40 processors		There is approximately 60 TXS electrical enclosures and 60 TXP electrical enclosures in total. Processors: approximately 140 TXS (531 is in same platform)		
Spare parts	Available	Available	Available	Available		Available
I&C changes conducted in-house / by supplier.	Supplier conducts parameter modifications Supplier conducts functional modifications Tests are made in TUSS by WEC.	Supplier conducts parameter modifications Supplier conducts functional modifications	Supplier conducts parameter modifications Supplier conducts functional modifications	Supplier conducts parameter modifications Supplier conducts functional modifications	Supplier conducts parameter modifications Supplier conducts functional modifications	Supplier conducts parameter modifications Supplier conducts functional modifications
Supplier strategy	Important to give WEC assignments so they do not lose interest in O1. O1 have signed a contract between OKG/WEC regarding minimum hours to be used for modifications at OKG each year. O1 believes it to be more cost effective to bring in WEC. The collaboration is currently very well-functioning. Important to have internal competence that knows the integration towards the plant. Supplier knows their product but it needs to be correctly implemented at OKG. O1 believes the supplier will be involved further on.	Same as for safety system	Same as for safety system	Important to have internal competence that knows the integration towards the plant. Supplier knows their product but it needs to be correctly implemented at OKG. O2 believes the supplier will be involved further on.		
Resources in-house	O1 would like to conduct more modifications in-house, but do not have enough competence. O1 uses the supplier. O1's strategy has been to have sufficient I&C competence internally and to do changes without involvement from the supplier. It has been problematic to get enough resources. Now when O1 is starting to be old there are no longer any incentive to build up the internal competence. O1 will decommission in year 2032.	Could be more resources. O1 is vulnerable if staff disappear. O1 makes changes in the system now and then. Not enough to conduct a few modifications to retain competence.		Could be more resources. O2 is vulnerable if staff disappear. O2 makes changes in the system now and then. Not enough to conduct a few modifications to retain competence.	Could be more resources. O2 is vulnerable if staff disappear. O2 makes changes in the system now and then. Not enough to conduct a few modifications to retain competence.	

	R1 – Safety System	R1 – Non Safety System	R2 – Safety System	R2 – Safety Related System	R2 – Non Safety System
Platforms	TXS from Siemens/Areva	Masterpiece 200/1 from ABB AC800 from ABB AC450 from ABB AC450 from ABB AC450 from ABB	AC160 from WEC	Ovation from WEC	N/A
I&C platform application and functions	RPS - Diversified reactor protection system (DPS). One part of RPS is included in TXS and one part is still in OPS (analogue) RHR - Diversified rest effect cooling RPM-Neutron flow measurement surveillance. R1 has divided RPS in to two part, a new part DPS run by TXS and an old part OPS which still is analogue. HVAC - Safety ventilation for control electrical enclosures in V-building.	Masterpiece 200/1 system: Turbine controller/Pressure control AC800: Safety system on turbine and several smaller stand-alone units. Masterpiece 200/1 : Water feed system control level in reactor tank. Masterpiece 200/1 : Effect control system AC450: Rod Control system AC450: Alarm system 517A131	Reactor Protection (RPS) + PRM (Reactor Trip, Engineering Safety Features, diesel sequence, Post-Accident Monitoring System)	Ovation is used for surveillance and control of non safety systems and functions, electrical safety category CAT B, C, O. Ovation is deeply integrated in the plant.	
I&C platform insertion year	PRM installed 2006. RPS/RHR/HVAC installed 2009.	Masterpiece 200 installed 1991. AC800 installed 2012. AC450 installed 1994. AC450 installed 1996. AC450 installed 1999. AC450 installed 2005.	1999-2010 Project TWICE	1999-2010 Project TWICE	
Projects that have been done on the platform. Scope of project.	The two coming outage after installation were clean up project performed at R1, where remaining open items were closed, such as parameter changes, text changes etc. After that, projects including functional changes have been performed: Autobor and the change of 314 valves. 2015 the last ÖGP project will be implemented which include functional changes.		PICUP 2011 was only remaining points from TWICE and DCRs. PICUP 2012 conducted smaller changes. PICUP 2013 changed baseSW in AC160. PICUP 2014/2015 included changes (HW/applSW) in AC160 and Ovation.	PICUP 2011 was only remaining points from TWICE and DCRs. PICUP 2012 conducted smaller changes. PICUP 2013 changed baseSW in AC160. PICUP 2014/2015 included changes (HW/applSW) in AC160 and Ovation.	
Architecture basics (number of subs, processors, communication links etc.)	Number of subs: Three subs, S1, S2 and S3. Two main subs (S1 and S2). Number of electrical enclosures: 55 Number of Processors: Approximately 70 processors in TXS. There are a few stand-alone processors. Communication: Processors communicates via fib (five data bases).	Number of subs: Three subs, A, B and C. Two main subs (A and B) Number of electrical enclosures: 60 Number of Processors: 70 Communication: Ethernet, MB200, MB300, AF100, Profibus.	Number of subs: Four subs, A, B, C & D Number of electrical enclosures: Division A and B have 14 electrical enclosures and division C and D 12 electrical enclosures. Number of Processors: In total 96 processors, 4 MTP and 4 Operator Display Panels (ODP). Communication: Communication between subs in Cat A is done via High Speed Link.	Number of subs: Four subs, A, B, C & D (built with redundancy for network and power supply (AC, CA, BD,DB)) Number of electrical enclosures: about 165 Number of Processors: 67 redundant processors Communication: Fast Ethernet Other: Ovation 1.6, Solaris 8 42 work stations (Operator stations, Engineering stations, Calculation server etc.)	
Spare parts	Available	Available	Available	Some parts are critical. WEC has delivered a report that claims R2 can run with Ovation to planed shutdown year 2027.	
I&C changes conducted in-house / by supplier.	Collaboration R1/Supplier when modifying parameters and functions.	R1 conducts changes in-house.	R2 conducts parameter changes in-house. R2 conducts functional changes in-house (WEC is partly used for reviews and council). Tests are made in R2's test tool LES (1 of 4 subs).	R2 conducts parameter changes in-house. R2 conducts functional changes in-house.	
Supplier strategy	R1 is positive in using the supplier for TXS changes.	R1 is positive in using the supplier for changes in ABB systems.	R2 have another supplier strategy compared to the other NPPs. It was a condition when starting TWICE that R2 should be able to perform changes in I&C without help from the supplier. R2 consider it to be risky when to much responsibility is put on the supplier since the NPP will lose competence and it will make the NPP more vulnerable. There could have been several benefits if WEC had been involved more in the2014/2015 modifications in AC160 and Ovation. In that case it should have been important with internal competence which could have questioned the Supplier. R2 shall be able to evaluate errors in plant by them self. R2 has a lot of internal competence available. Therefore, the supplier contributes most if used for basic design criteria. WEC will have AC160 competence further on.	R2 have another supplier strategy compared to the other NPPs. It was a condition when starting TWICE that R2 should be able to perform changes in I&C without help from the supplier. R2 consider it to be risky when to much responsibility is put on the supplier since the NPP will lose competence and it will make the NPP more vulnerable. There could have been several benefits if WEC had been involved more in the2014/2015 modifications in AC160 and Ovation. In that case it should have been important with internal competence which could have questioned the Supplier. R2 shall be able to evaluate errors in plant by them self. It is important to keep Ovation competence internally since R2 is running on older version of Ovation.	
Resources in-house	Lack of in-house competence is an upcoming risk.	Lack of in-house competence is an upcoming risk.	R2 have sufficient resources to conduct functional modifications in-house.	R2 have sufficient resources to conduct functional modifications in-house.	

	R3/R4 – Safety System	R3/R4 – Non Safety System	F1/F2 – Safety System	F1/F2 – Non Safety System	F3 – Safety System	F3 – Non Safety System
Platforms	Spec 200 from Foxboro WDPF from WEC	AC 800 from ABB WDPF from WEC	NUMAC-system from GE	Advant system AC450 from ABB NUMAC (ATIP) from Siemens (KWU)	NUMAC-system from GE.	SINDAC - Block computer TXS - from Siemens TXP- from Siemens. Master Piece from ABB Procontrol from ABB NUMAC-system (ATIP) from GE
I&C platform application and functions	Spec 200 part of the safety system. Spec 200 is used for limit value measurements. Takes signals from transmitter, analyses, sends signal to analogue system (SSPS) to initiate function. Parts of the five SSM safety functions are realized in Spec 200. Spec 200 is used for presentation of safety functions in control room. WDPF 1E for regulation and control. WDPF is used for regulation and control of process data. Not valves (like Ovation on R2). WDPF is the interface between control system and operator. Plant data in presented to the operator. WDPF has no images. Neutron flow measurement system is in a separate analogue system.	AC 800: Turbine regulator, turbine protection and alarms. Sending signals to BIS and PIS WDPF 2E for regulation and control. WDPF is used for regulation and control of process data. Not valves (like Ovation on R2). WDPF is the interface between control system and operator. Plant data in presented to the operator. WDPF has no images.	Neutron flow measurement PRNM system 531. Three different units of Numac system 531 (Safety system and Operation System). NUMAC WRNN- Measure middle effect (Safety system) NUMAC PRNN (>8%) - measure normal effect (Safety system)	NUMAC ATIP - Every forth week a detector is submerged to compare values to PRNN and WRNN (Operation systems)	Neutron flow measurement PRNM system 531. Three different units of Numac system 531 (Safety system and Operation System). NUMAC WRNN- Measure middle effect (Safety system) NUMAC PRNN (>8%) - measure normal effect (Safety system)	TXS: Rod control system (not SS system). Numac: ATIP - Every forth week a detector is submerged to compare values to PRNN and WRNN (Operation systems) TXP-OM from Siemens, 592, Turbine protection Master Piece from ABB, 535/537, Effect and level regulation Procontro from ABB, 592, Turbine regulator SINDAC, 520 Block computer
I&C platform insertion year	Spec 200: 1994-97 Project Repac WDPF: 1994-97 Project Repac	AC 800: 2010 R3 and 2011 R4 (NICE) WDPF: 1994-97 Project Repac	WRNM - Installed in F1/2 1996-1997. PRNM - Installed in F1/F2 2005/2006.	Advant system AC450 - 1995	NUMAC PRNM - 2007	Master Piece - Block computer - 1985 (in operation). Procontrol - TXS - 2001 TXP - 2000 ATIP - 1996
Projects that have been done on the platform. Scope of project.	In Spec 200 and WDPF 1E parameter changes, changed alarm limits, changed functions (added and removed) have been made.	AC 800 Only smaller changes In WDPF 2E Parameter changes, changed alarm limits, changed functions (added and removed) have been made. Processors have been removed.	Have conducted parameter changes in Numac.	Have conducted parameter changes in Numac.	Have conducted parameter changes in Numac.	Have conducted parameter changes in Numac.
Architecture basics (number of subs, processors, communication links etc.)	Spec 200 Number of subs: 4 subs. Number of electrical enclosures: 12 Number of Processors: 47 Stand alone processors. WDPF Number of subs: 4 subs Number of electrical enclosures: 6 Number of Processors: 18 Stand alone processors.	WDPF Number of subs: 4 subs Number of electrical enclosures: 10 Number of Processors: 32 Stand alone processors.	Separated units of Numac system 531. Number of subs: 4 Number of electrical enclosures: 1 electrical enclosure/sub Number of Processors: 1 CPU/Chassis. 2 Chassis in one electrical enclosure. Communication: Fibre and regular signal cable.	Advant system AC450 can not be described in a simple way. Several electrical enclosures and distribution from two central electrical rooms to control equipment and relay electrical enclosures in plant.	Separated units of Numac system 531. Number of subs: 4 Number of electrical enclosures: 1 electrical enclosure/sub Number of Processors: 1 CPU/Chassis. 2 Chassis in one electrical enclosure. Communication: Fibre and regular signal cable.	
Spare parts	WDPF platform will need to be changed before R3/4 shutdown. Old functional HW will be difficult to find (HW accessories as HW drives). Platform upgrade is planed to 2023-2025. Some support from supplier (WEC) is possible for WDPF. Not possible to get support from the supplier for Spec 200. Platform upgrade is planed to 2023-2025. Spare parts available (taken from R2 during TWICE).	Available WDPF platform will need to be changed before R3/4 shutdown. Old functional HW will be difficult to find (HW accessories as HW drives). Platform upgrade is planed to 2023-2025. Some support from supplier (WEC) is possible for WDPF.	Numac should be able to run until shutdown. GE has several other plants running on the same HW. GE has regulations to follow consequently, they cannot stop producing HW. They have promised NRC to have HW available.	Numac should be able to run until shutdown. GE has several other plants running on the same HW. GE has regulations to follow consequently, they cannot stop producing HW. They have promised NRC to have HW available.	Numac should be able to run until shutdown. GE has several other plants running on the same HW. GE has regulations to follow consequently, they cannot stop producing HW. They have promised NRC to have HW available.	Numac should be able to run until shutdown. GE has several other plants running on the same HW. GE has regulations to follow consequently, they cannot stop producing HW. They have promised NRC to have HW available.
I&C changes conducted in-house / by supplier.	Spec 200: R3/4 conducts parameter changes in-house. Supplier has conducted function changes (no longer possible to use supplier help for Spec 200). WDPF: R3/4 conducts parameter changes in-house. Supplier conducts functional changes (WEC)	AC 800 Can perform changes in-house, but supplier is available if necessary WDPF: R3/4 conducts parameter changes in-house. Supplier conducts functional changes (WEC)	F1/2 conducts parameter changes in-house. Supplier conducts functional changes and HW changes (GE).	Numac: F1/2 conducts parameter changes in-house. Supplier conducts functional changes and HW changes (GE).	F3 conducts parameter changes in-house. Supplier conducts functional changes and HW changes (GE).	TXS/TXP: Supplier conducts parameter changes. Supplier conducts functional changes. Numac: F3 conducts parameter changes in-house. Supplier conducts functional changes (GE). Block computer: Minimal in-house competence, management outsourced to Cap Gemini to coordinate etc. Master Piece: Supplier conducts changes but lack of competence. Procontrol: No in-house design competence. Only competence within maintenance.
Supplier strategy	Some support is possible for WDPF from supplier (WEC). No longer possible to get supplier support for Spec 200. Not even available internationally.		F1/F2 uses NUMAC for system 531 WRNM and PRNM. For modifications in NUMAC FKA rely on supplier. Important that Forsmark participates in changes since supplier do not know the plant design.	F1/2 upgrades Advant platform (project VAPP) with ABB partner.	F3 uses NUMAC for system 531 WRNM and PRNM. For modifications in NUMAC FKA rely on supplier. Important that Forsmark participates in changes since supplier do not know the plant design.	Block computer: Upgrade performed now (Emulated) in operation 2014/2015. Retain TXS/TXP with upgrades.
Resources in-house	WDPF: Lack of in-house competence is an upcoming risk. Spec 200: Lack of competence within Spec 200, not even available internationally by the supplier.	WDPF: Lack of in-house competence is an upcoming risk.	NUMAC - The need of in-house competence is not that large. F1/2 specifies changes and they are conducted by GE. There is a challenge in retaining the competence since there are many retirements. Applies both in-house and for the supplier.	Advant system AC450 - F1/2 needs to be involved in development since F1/2 have a lot of competence in existing design and solutions. NUMAC - The need of in-house competence is not that large. FKA specifies changes and they are conducted by GE. There is a challenge in retaining the competence since there are many retirements. Applies both in-house and for the supplier.	NUMAC - The need of in-house competence is not that large. FKA specifies changes and they are conducted by GE.	TXS - F3 have some competence but cover up via service agreements and upgrades regularly. TXP - F3 have some competence but cover up via service agreements. NUMAC - The need of in-house competence is not that large. F3 specifies changes and they are conducted by GE. Block computer - minimal in-house competence, management outsourced to Cap Gemini to coordinate etc. Procontrol - No in-house design competence. Only competence within maintenance. Masterpiece - No in-house design competence. Only competence within maintenance.

Appendix 2. Interview questions.

Note. The first three pages include standard questions that were used in all conducted interviews. The following pages presents interview questions for each specific role.

Appendix 2. Interview questions.

ID	Select the option that most closely matches the claim.	1. Strongly disagree	2. Tend to disagree	3. Neither agree or disagree	4. Tend to agree	5. Strongly agree	6. No opinion	Comment
SM1	I&C projects works cost effective							
SM2	The NPP has sufficient I&C competence internally including consultants (without help from suppliers)							
SM3	The NPP have well-developed processes/instructions for implementing I&C modifications (execution of I&C modifications internally without much supplier involvement)							
SM4	We have satisfactory safety thinking when implementing I&C modifications							
SM5	I feel very confident in the quality of the I&C modifications							
SM6	We should let the supplier perform more work during I&C modifications							
SM7	We have sufficient emphasis on management and lifecycle when performing I&C modifications							
SM8	We create a technical debt* while performing I&C modifications *Technical debt is future negative consequences due to previous flaws in design/code/documentation							
SM9	Our I&C documentation is managed and established in a good way							
SM10	We have a good working method for requirement management at I&C modifications							
SM11	We have a good working method for verification and validation during I&C modifications							
K1	The platform design makes it easy to implement changes and to verify them in a quality safe and cost-effective way?							

Appendix 2. Interview questions.

ID	I think the below areas work well during I&C modifications	1. Strongly disagree	2. Tend to disagree	3. Neither agree or disagree	4. Tend to agree	5. Strongly agree	6. No opinion	Comment
SM12	Project order and scope							
SM13	Project Management							
SM14	Plant Design							
SM15	System Design							
SM16	Detail Design							
SM17	Purchase HW							
SM18	Purchase SW							
SM19	Configuration Management							
SM20	Verification and Validation							
SM21	Technical risk management							
SM22	Human Machine Interface HMI							
SM23	Factory Acceptance Testing FAT							
SM24	Site Acceptance Testing SAT							
SM25	Installation							
SM26	Maintenance							
SM27	Operation							
SM28	PSG							
SM29	Contact with Swedish Radiation Safety Authority							

Appendix 2. Interview questions.

ID	Background	Comments
S1	Is the term "I&C" (Instrumentation & Controll) used in the NPP or do you use another terminology? What is your opinion on what is included in I&C?	
S2	How long have you been working with I&C in the nuclear industry?	
S3	Describe your role and the I&C related projects/departments that you are/have been involved in?	
S4	What I&C platforms are you working with?	
S5	Did you participate in the original installation project of the platform?	
	Challenges	
S6	In what area do you see the biggest challenges for modification projects in I&C? (E.g. platform, processes, competence etc.)	
S7	What do you think are great contributors to success in I&C modification projects? (E.g. platform, processes, information, communication, competence, technical tools etc.)	
S8	What would you do to improve to possibility to conduct successful I&C modification projects? (E.g. choice of platform, development of processes, information, competence, technical tools etc.)	
S9	What do you think are the largest cost drivers in I&C modification projects? (E.g. complex platform, steered processes, information, communication, competence, technical tools etc.)	
S10	Do you believe that the organization is supporting I&C modification projects with enough support? (E.g. processes, competence, technical equipment etc.)	
S11	Do you think the supplier should be more or less involved in I&C modification projects? (Please give exampels in *what* and *how)*	

Appendix 2. Interview questions.

Test Leader / Commissioning I&C

ID	Test Leader I&C	Comments
T1	Are tests conducted in-house or at the supplier? For SW tests in-house, does the NPP have enough competence, working processes and technical tools?	
T2	Who are developing test procedures (FAT/SAT)?	
T3	What is the scoop of tests that are being conducted in FAT VS SAT?	
T4	What technical tool is used for tests (FAT)?	
T5	How much of the I&C changes results in rework due to fail in FAT/SAT? Are the failures mostly due to errors in the change requirements, errors made during code development, or errors made during the development of tests?	
T6	Has the term *regression analysis* been defined by the NPP? Is the term used? If yes, how is regression analyses interoperated and managed in the project?	
T7	How are test cases managed over time? (Are new test cases developed for each change or are test cases reused)	
T8	How is the organization handling the requirement on independence between development and testing?	
T9	Are there available spare parts on the market?	
T10	Will the I&C platform need an extensive hardware refurbishment?	

Appendix 2. Interview questions.

Lead Engineer I&C

ID	Strategy	Comments
K2	Are SW development conducted in-house or by the supplier? (Describe the interface)	
K3	For SW development in-house, does the NPP have enough competence, working processes and technical tools?	
K4	Are technical specifications (that are being input to SW development) developed in-house or by the supplier?	
	Process	
K5	Are the technical processes/instructions for I&C modifications sufficient? If not, why?	
K6	Are the technical processes/instructions for I&C modification developed by the supplier or NPP?	
K7	Are technical risks managed sufficient in the I&C projects?	
K8	How much of the I&C changes results in rework due to fail in FAT/SAT? Are the failures mostly due to errors in the change requirements, errors made during code development, or errors made during the development of tests?	
K9	How is the organization handling the requirement on independence between development and testing?	
	Platform	
K10	What functions are the I&C system used for?	
K11	How is the basic architecture for the I&C system? (Number of subs, processors, communication etc.)	
K12	Is the platform, according to your assessment; structured in a way that makes it easy or difficult to perform modifications and to verify them in a quality safe and cost effective way?	

Appendix 2. Interview questions.

ID	Requirements and Documentation	Comments
K13	How are I&C structured in SAR and SD (System Description)?	
K14	Are the requirement management for the I&C system sufficient? Existing system requirements and change requirements?	
K15	How are requirements and verificates managed over time? Life cycle?	
K16	Are changes made in the original I&C documentation (from the supplier) or are new documentation generated for I&C changes?	
K17	Does all I&C documentation exist as Plant documentation or are some information (e.g. design specifications or test reports) saved as project documentation?	
K18	Who is updating I&C documentation? (Updated by supplier or in-house)	
K19	Has the term regression analysis been defined by the NPP? Is the term used? If yes, how is regression analyses interoperated and managed in the project?	

Appendix 2. Interview questions.

Quality and Validation Manager I&C

ID	Quality and Validation Manager I&C	Comments
KV1	Does the role ”Quality and/or Validation Manager” exist?	
KV2	Describe the overall validation strategy and process. Does the project write a validation plan?	
KV3	How are the requirements followed up? Is for example a requirement matrix used?	
KV4	How are the code verified before installation on the plant? What verification activities?	
KV5	How are test cases managed over time? (Are new test cases developed for each change or are test cases reused)	
KV6	How are verificates managed over time? Life cycle?	
KV7	How are system requirements managed over time? Does an updated requirement system specification exist?	
KV8	Has the term *regression analysis* been defined by the NPP? Is the term used? If yes, how is regression analyses interoperated and managed in the project?	
KV9	How is regression analyses interoperated and managed in the project?	
KV10	Are verification conducted by an independent organization? Who and to what extent?	
KV11	How is the organization handling the requirement on independence between development and testing?	

Appendix 2. Interview questions.

Line Manager I&C

ID	Strategies and Background	Comments
C1	What degree of I&C changes are supposed to be conducted in-house (without involvement from supplier)?	
C2	Do you think you have appropriate processes and instructions to perform I&C modifications in accordance with the strategy? (see above question)	
C3	Does the NPP have sufficient development and test tools for SW?	
C4	Do you think the rest of the organization supports I&C in a successful way? Does the rest of the organization have an understanding for I&C?	
C5	Is there a CM strategy? If yes, is the CM strategy well implemented and understood in the organization? If not, how do you work instead?	
	I&C projects	
C6	What I&C modification projects has been realized? During what years? What was the scoop of the projects? (Safety System, Safety Related System, functional changes, HW, bas SW, appl. SW)	
C7	Approximately, how many hours have each project conducting I&C changes required? (If possible, specify by Project Management, Quality Management, Lead Engineer, System Engineer, Programming and Testing)	
C8	Did the projects follow the original budget?	
C9	Did the projects follow the original time plan?	
C10	Did the projects encounter challenges regarding quality (eg error found late in the project)?	
C11	Has the supplier been involved in I&C modification projects? What role did the supplier have? How much did it cost?	

Appendix 2. Interview questions.

ID	Process	Kommentar
C12	Does complete processes/instructions exist for I&C modifications for all phases?	
C13	Has the I&C department or the modification project been responsible for developing and/or complement the I&C processes/instructions?	
C14	How are I&C structured in SAR and SD (System Description)?	
C15	How are changes ordered from operations/maintenance handled (that are not included in a project)? (Order and implementation)	
C16	Is there a process to handle temporary changes? (Safety System and Safety Related System)	
	Competence	
C17	Do you have the right I&C competence in your group? Are you dependent on suppliers or consultants?	
C18	How are you working to develop your group and the I&C competence?	
	Hardware	
C19	Are there available spare parts on the market?	
C20	Will the I&C platform need an extensive hardware refurbishment?	

Appendix 2. Interview questions.

Process Owner Configuration Management

ID	Process Owner Configuration Management (CM) or equivalent	Comment
CM1	Is there a CM strategy? If yes, is the CM strategy well implemented and understood in the organization? If not, how do you work instead?	
CM2	How is I&C structured in SAR and SD (System Description)?	
CM3	Are changes made in the original I&C documentation (from the supplier) or are new documentation generated for I&C changes?	
CM4	Does all I&C documentation exist as Plant documentation or are som information (e.g. design specifications or test reports) saved as project documentation?	
CM5	How is the impact on SAR handled by the I&C project?	

Appendix 2. Interview questions.

Process Owner Quality Management System / Process Owner Verification and Validation / QA

ID	Process Owner Quality Management System / Process Owner Verification and Validation / QA	Comments
Pr1	Describe the overall process used when conducting changes in the plant?	
Pr2	Are the I&C process complete through all phases? What phases/tollgates shall an I&C project go through?	
Pr3	How is the interface towards other projects/stakeholders?	
Pr4	Has the I&C process been inspired by agile working methods?	
Pr5	How are changes during the development process handled?	
Pr6	Which standards describing *processes* have been used when developing the I&C system? What process standards are identified in SAR (safety analysis report)? Process standards that are interpreted in addition to SAR?	
Pr7	How is the organization handling the requirement on independence between development and testing?	

Appendix 2. Interview questions.

Project Manager I&C

ID	I&C projects	Comments
P1	What is the scope of the changes that the I&C project is conducting?	
P2	What do you think are the largest contributors to the success in your I&C-project?	
P3	What have been the largest challenges in your I&C-project?	
P4	Has the project followed the original time plan, budget and delivered the right quality?	
P5	What would you have done differently in the project?	
P6	What would you recommend for future I&C-projects?	
P7	Did the project have enough resources (both seen to competence and amount)?	
	Interface	
P8	How are modifications in I&C conducted? Are all changes gathered and implemented by one specific I&C project, or are every change managed by each plant project? How are the interfaces between the projects?	
P9	Has the supplier been involved in I&C modification projects? What role did the supplier have? How much did it cost?	
P10	How much ”use” did you have of the supplier? Could parts have been done in-house?	
P11	Has the I&C department or the modification project been responsible for developing and/or complement the I&C processes?	
P12	Has the rest of the organization given enough support to the project and understood the challenges when conducting I&C changes? (Line managers, operation, maintenance, project sponsor etc.)	

Appendix 2. Interview questions.

PSG Executioners

ID	PSG	Comments
PSG1	How does PSG review an I&C project?	
PSG2	How has the I&C modifications been presented for PSG? At what technical level has it been presented?	
PSG3	Is the completeness of the plant changes presented for PSG (plant level to detailed design)?	
PSG4	What do you see as the largest risks when conduction changes in the I&C system?	
PSG5	Do you think the radiation authority has a good understanding and questioning of I&C modification projects?	

Appendix 2. Interview questions.

SSM

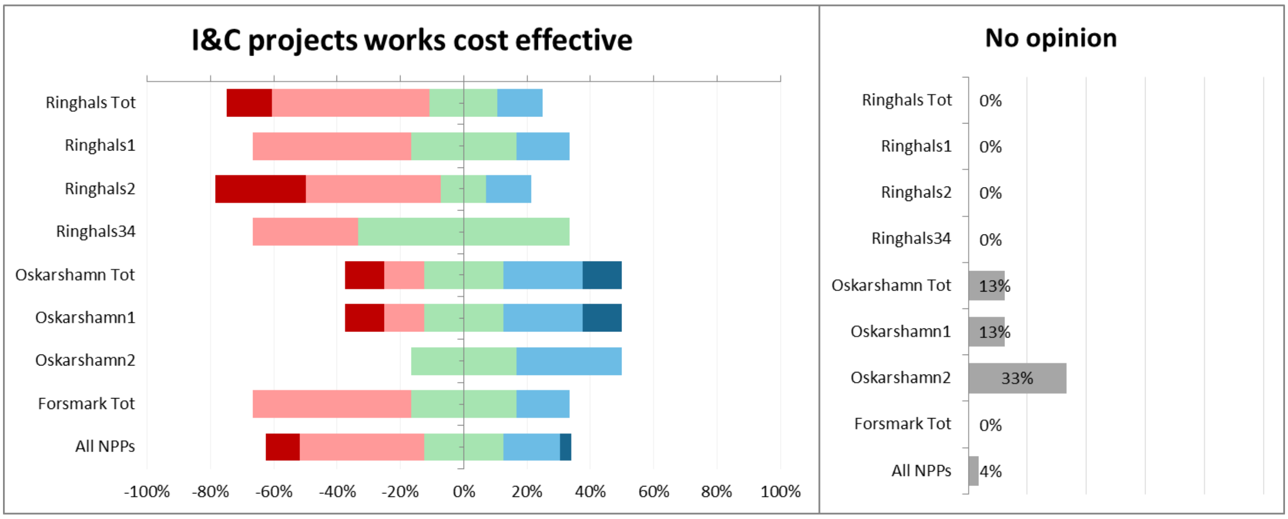
ID	Programmable I&C Strategy	Comments
SSM1	Do you think the programmable I&C or analog technology is preferred in nuclear power? Why?	
SSM2	Do you think that the supplier should be more or less involved in the I&C modification project? (Please give examples in which parts and how)	
SSM3	Do you think the Swedish nuclear power industry has a long term and sustainable management strategy for I&C systems?	
SSM4	Do you think that the nuclear industry has sufficient understanding of I&C modifications?	
SSM5	Compared to international standards, do you think the Swedish nuclear power industry has a good understanding of I&C?	
	Programmable I&C Platform	
SSM6	Are there models and/or configurations of I&C platforms where you think it is easier to see what changes have been made thus facilitating the V&V process. (Makes it easier for SSM to assess if the extent of the V&V have been reasonable)	
SSM7	What factors, regarding the configuration of the I&C platforms, do you consider to complicate the change operation? (For example, the number/type of functions implemented in the system, the operator's ability to influence, communication system, etc.).	
	Programmable I&C Process	
SMM8	Do you believe that there are complete processes/instructions for the I&C modifications of NPPs? If no, what are the weaknesses?	
SSM9	Do you think there is a well-developed and functional configuration approach (CM) for I&C systems? If no, what are the weaknesses?	
SSM10	Do you believe that the NPPs have the appropriate level in the verification of I&C modifications? If no, what are the weaknesses?	

Appendix 2. Interview questions.

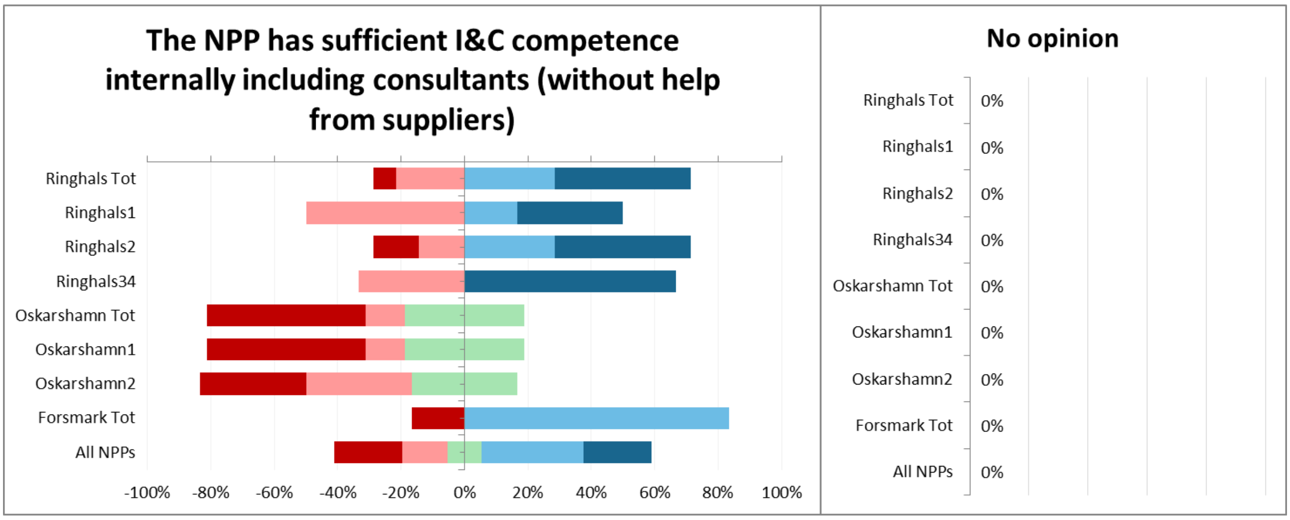
SSM11	What do you think is the purpose of the regression analysis? How should it be done? Is it correctly interpreted by the nuclear industry?	
SSM12	Do you think that the requirement of independence between development and testing is handled adequately?	
SSM13	Do you think that verification by an independent organization occurs sufficiently?	
SSM14	What factors do you think is the most important when testing I&C? (Eg strategy FAT, SAT, independent testing, simulation testing etc.)	
SSM15	What factors do you think is the most important when using existing tools (development and testing of I&C)?	
	SSM review I&C modifications	
SSM16	How does SSM review an I&C modification?	
SSM17	What are the difficulties during a SSM review of an I&C modification?	
SSM18	What type of reporting documentation would SSM wish upon review of I&C modifications? (Complement to SAR, eg overall score I&C, requirements / receipts setup etc.)	

Appendix 3. Graphs of multiple choice questions.

Strongly disagree	Tend to disagree	Neither agree or disagree	Tend to agree	Strongly agree	No opinion



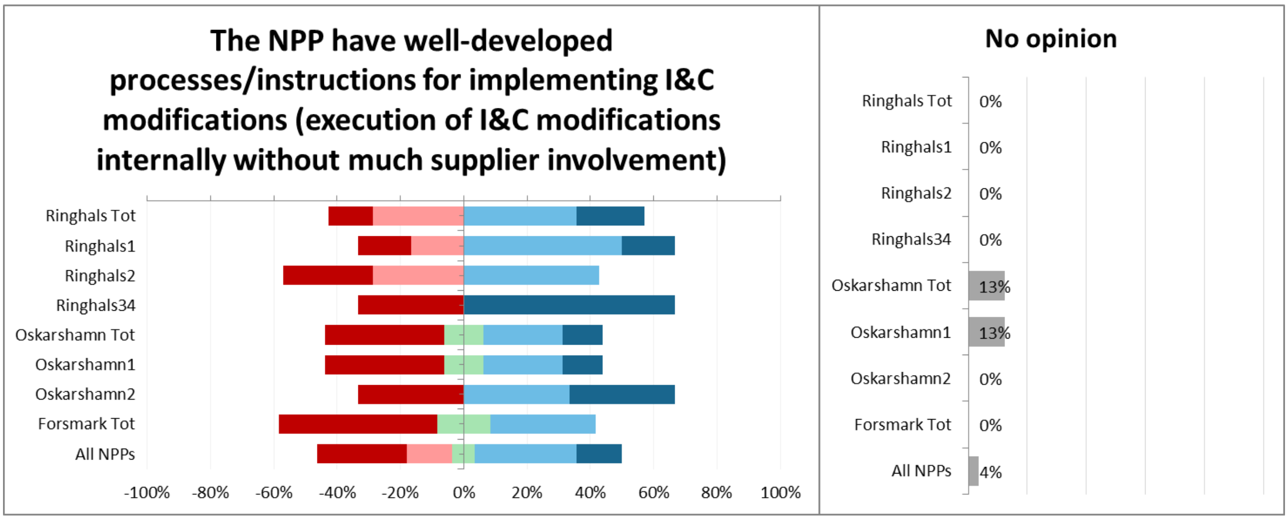
Graph 1. I&C projects works cost effective.



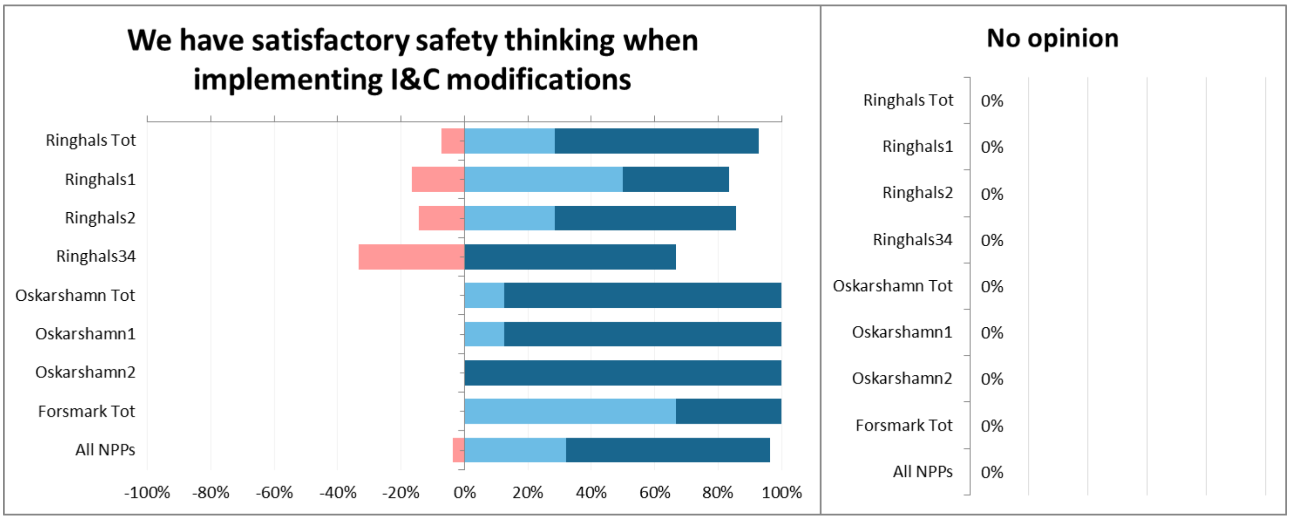
Graph 2. The NPP has sufficient I&C competence internally including consultants (without help from suppliers).

Appendix 3. Graphs of multiple choice questions.

Strongly disagree	Tend to disagree	Neither agree or disagree	Tend to agree	Strongly agree	No opinion



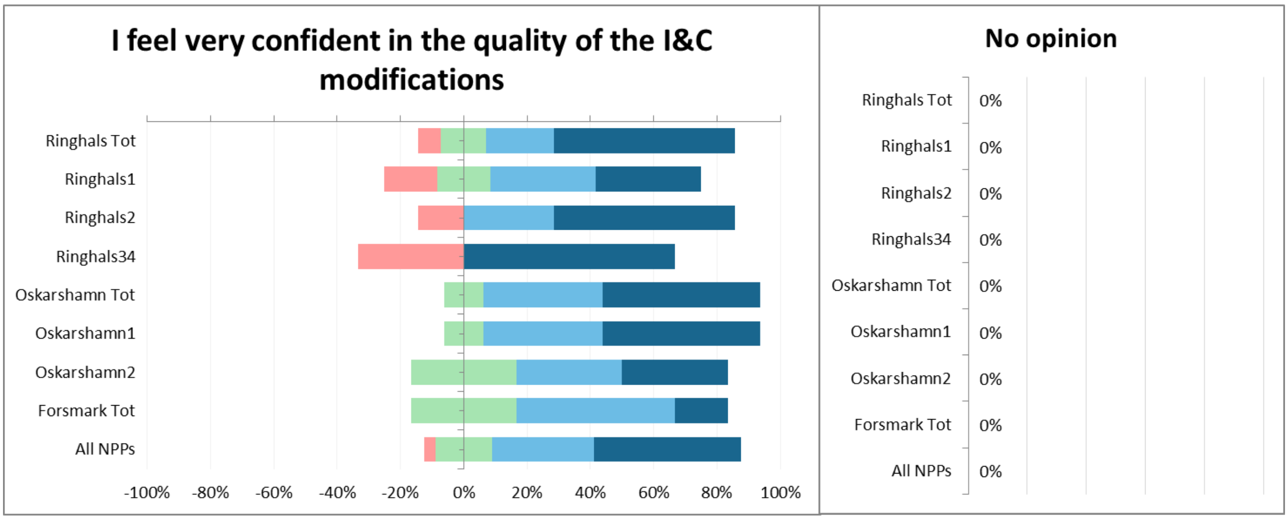
Graph 3. The NPP have well-developed processes/instructions for implementing I&C modifications (execution of I&C modifications internally without much supplier involvement).



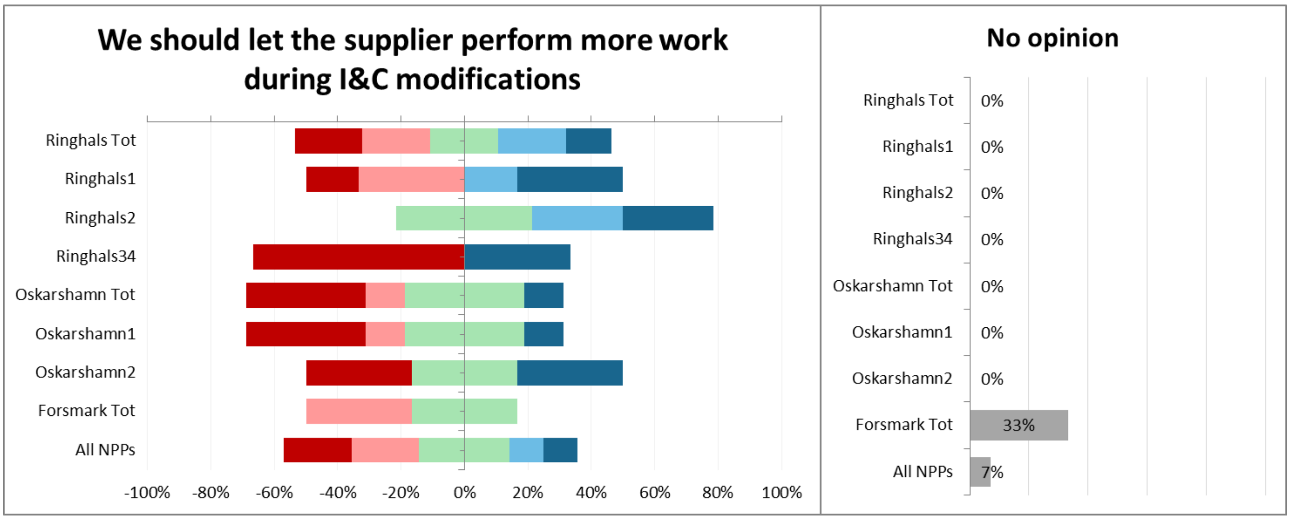
Graph 4. We have satisfactory safety thinking when implementing I&C modifications.

Appendix 3. Graphs of multiple choice questions.

Strongly disagree	Tend to disagree	Neither agree or disagree	Tend to agree	Strongly agree	No opinion



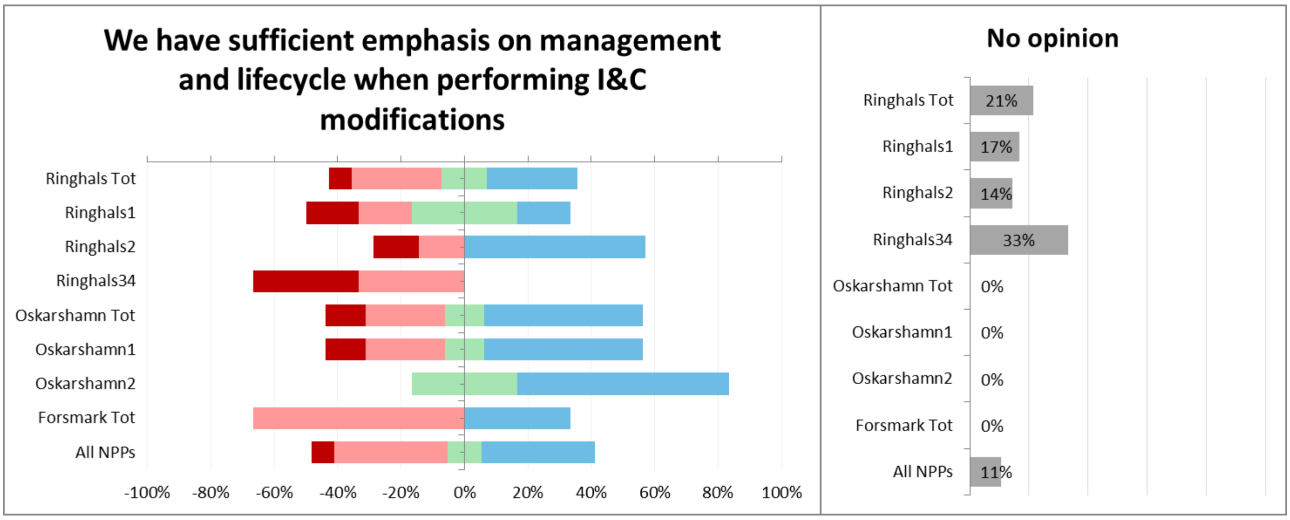
Graph 5. I feel very confident in the quality of the I&C modifications.



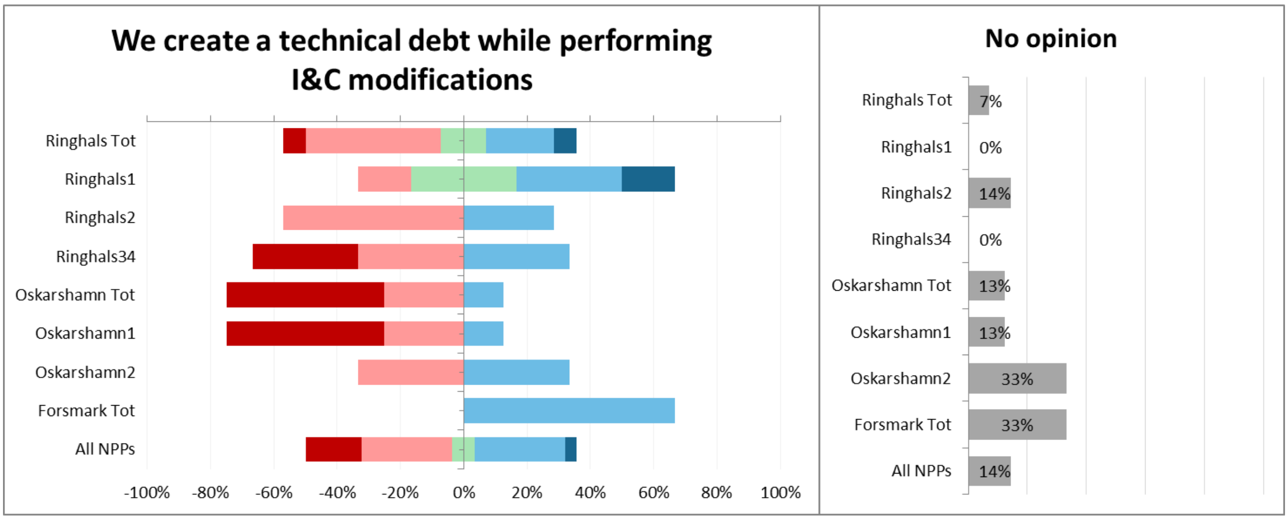
Graph 6. We should let the supplier perform more work during I&C modifications.

Appendix 3. Graphs of multiple choice questions.

Strongly disagree	Tend to disagree	Neither agree or disagree	Tend to agree	Strongly agree	No opinion



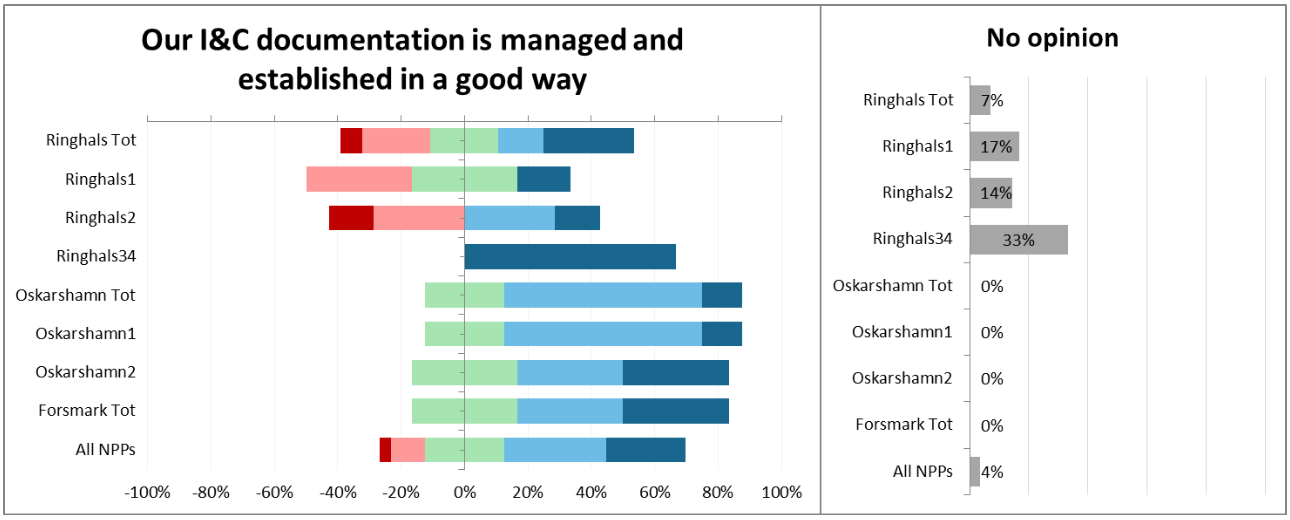
Graph 7. We have sufficient emphasis on management and lifecycle when performing I&C modifications.



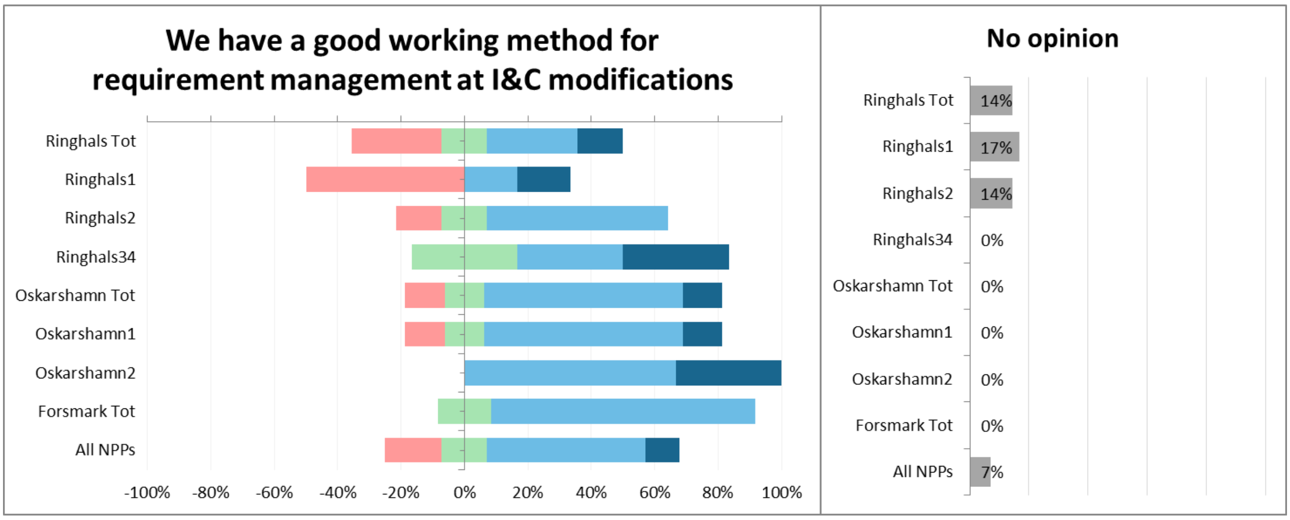
Graph 8. We create a technical debt while performing I&C modifications.

Appendix 3. Graphs of multiple choice questions.

Strongly disagree	Tend to disagree	Neither agree or disagree	Tend to agree	Strongly agree	No opinion



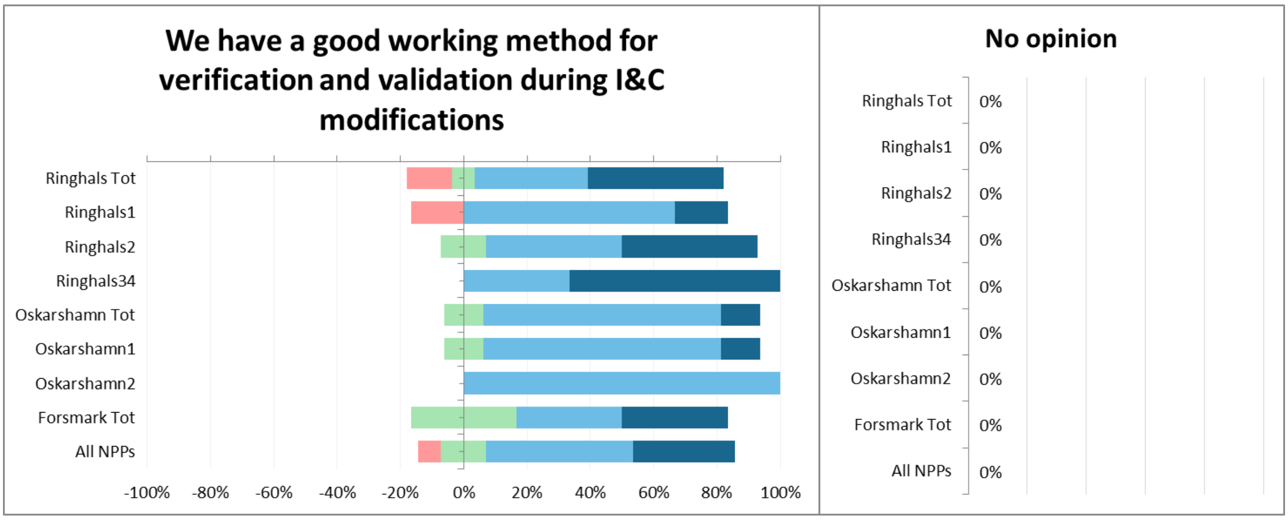
Graph 9. Our I&C documentation is managed and established in a good way.



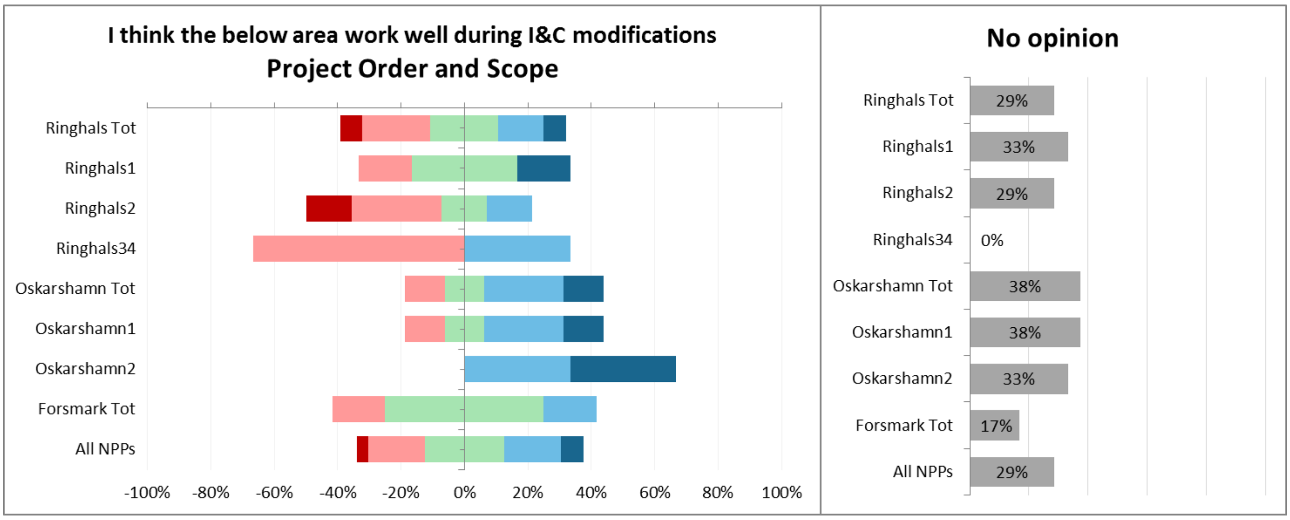
Graph 10. We have a good working method for requirement management at I&C modifications.

Appendix 3. Graphs of multiple choice questions.

Strongly disagree	Tend to disagree	Neither agree or disagree	Tend to agree	Strongly agree	No opinion



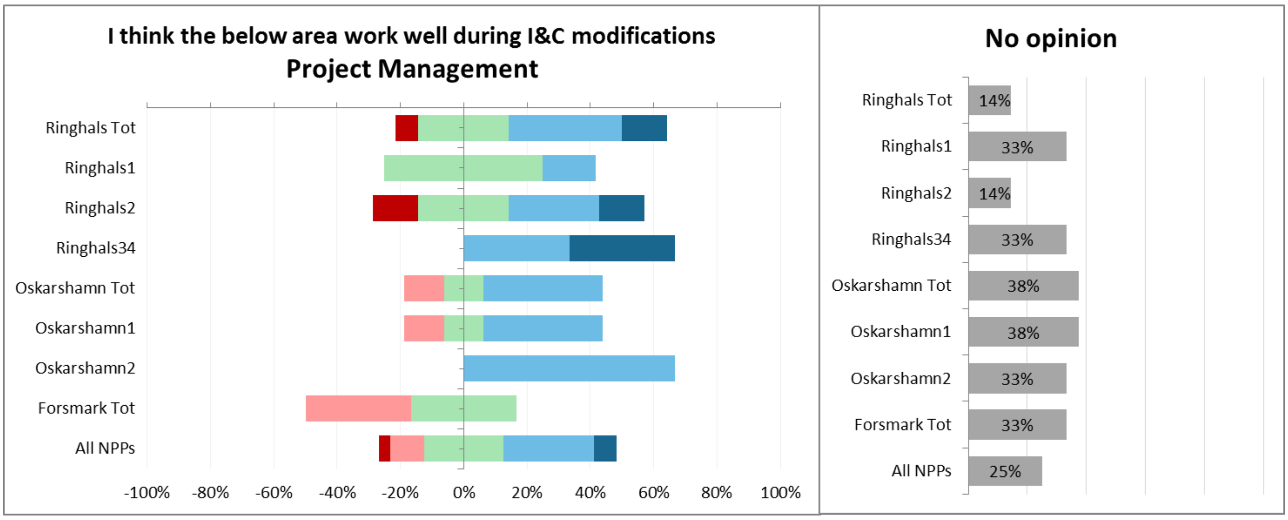
Graph 11. We have a good working method for verification and validation during I&C modifications.



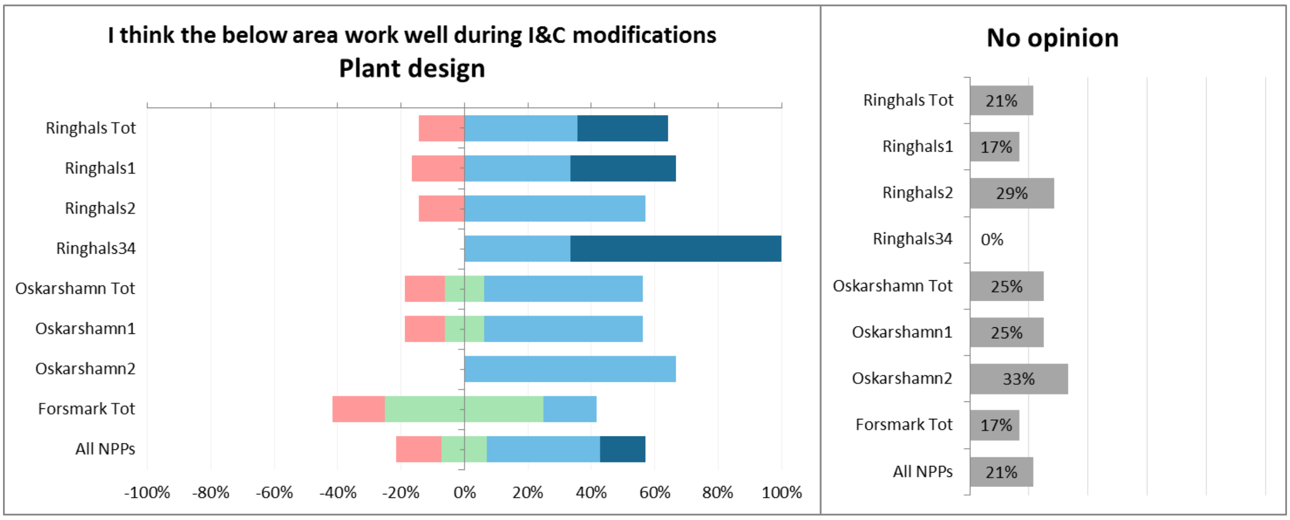
Graph 12. Project Order and Scope.

Appendix 3. Graphs of multiple choice questions.

Strongly disagree	Tend to disagree	Neither agree or disagree	Tend to agree	Strongly agree	No opinion



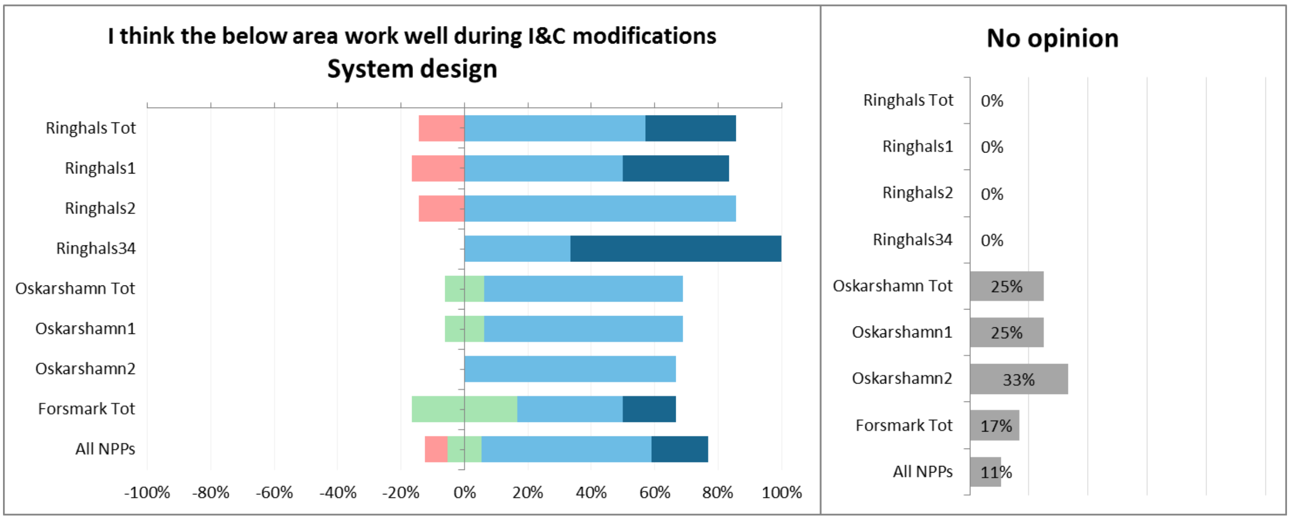
Graph 13. Project Management.



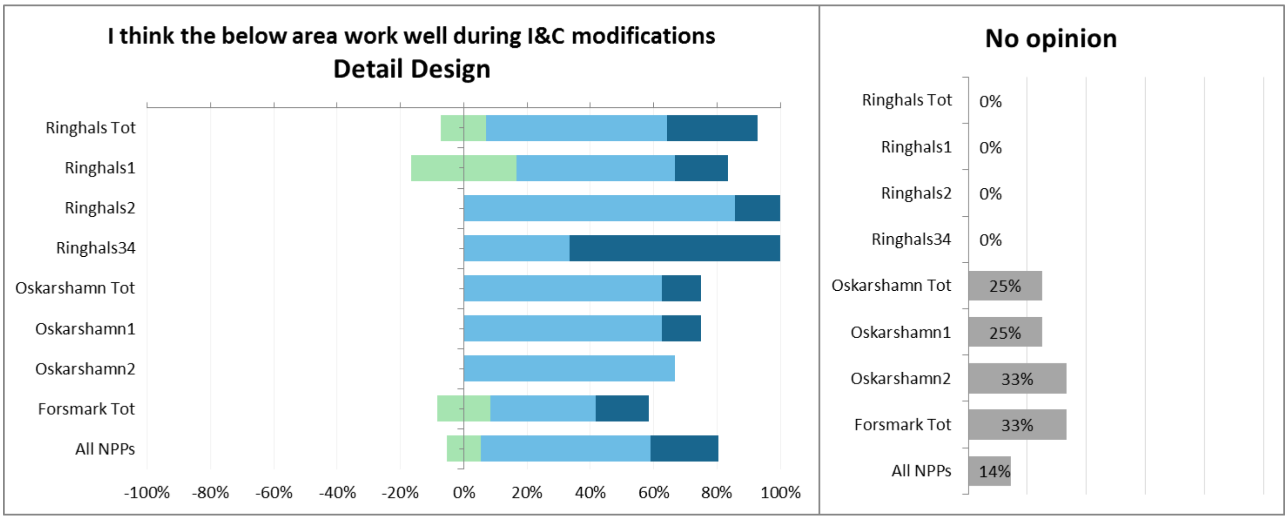
Graph 14. Plant design.

Appendix 3. Graphs of multiple choice questions.

Strongly disagree	Tend to disagree	Neither agree or disagree	Tend to agree	Strongly agree	No opinion



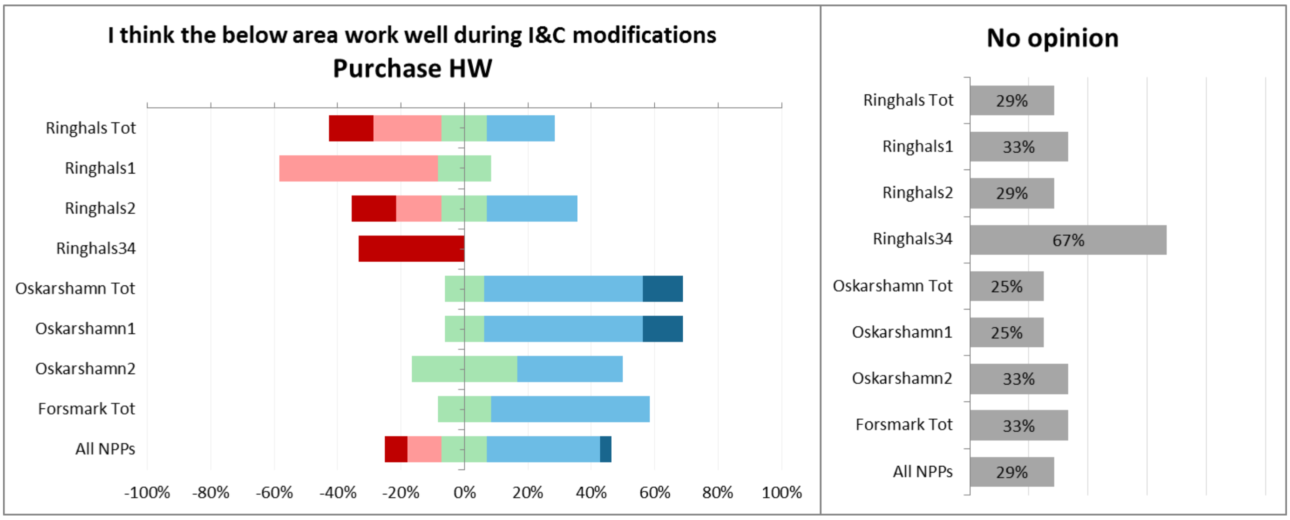
Graph 15. System design.



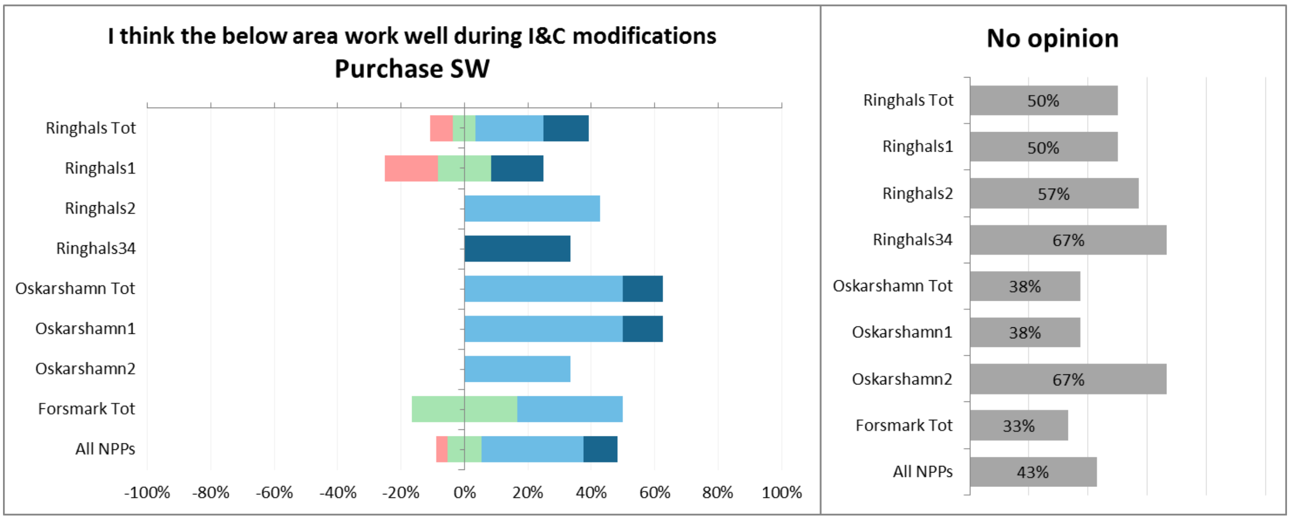
Graph 16. Detail Design.

Appendix 3. Graphs of multiple choice questions.

Strongly disagree	Tend to disagree	Neither agree or disagree	Tend to agree	Strongly agree	No opinion



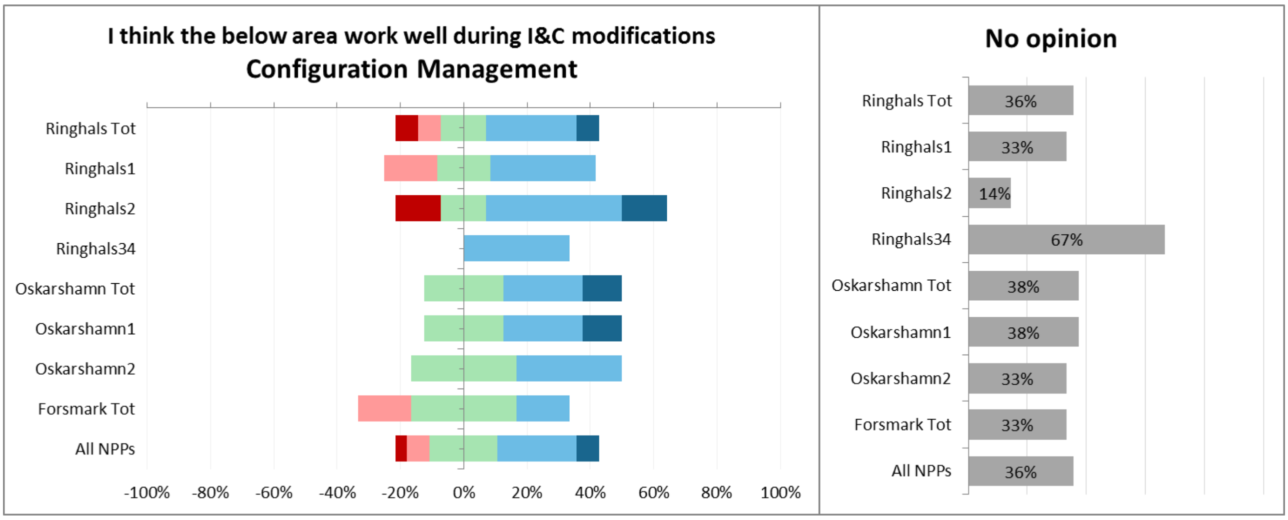
Graph 17. Purchase HW.



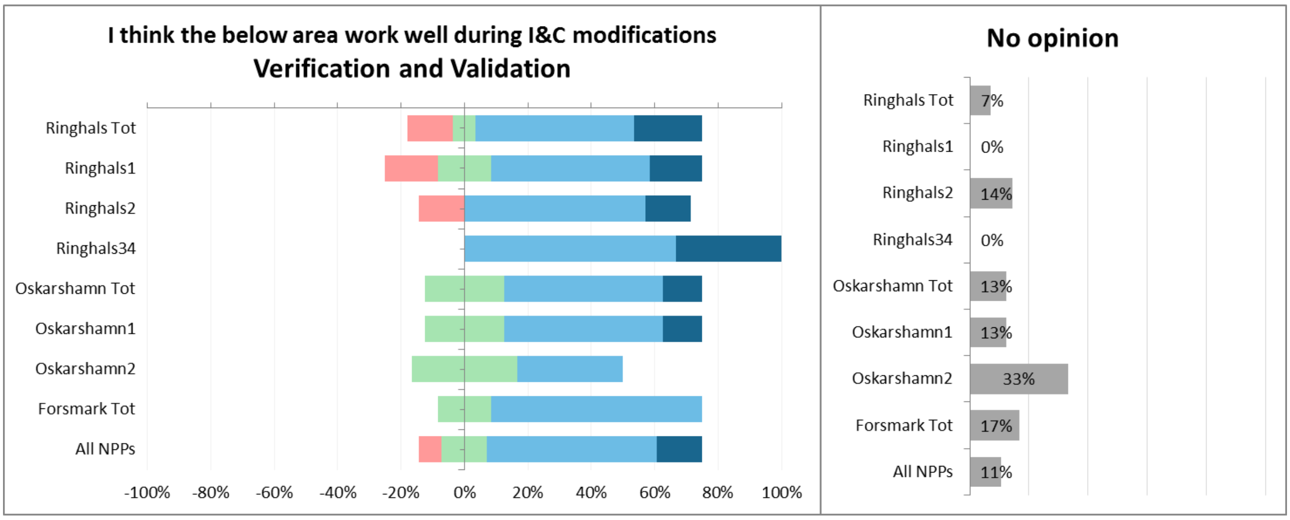
Graph 18. Purchase SW.

Appendix 3. Graphs of multiple choice questions.

Strongly disagree	Tend to disagree	Neither agree or disagree	Tend to agree	Strongly agree	No opinion



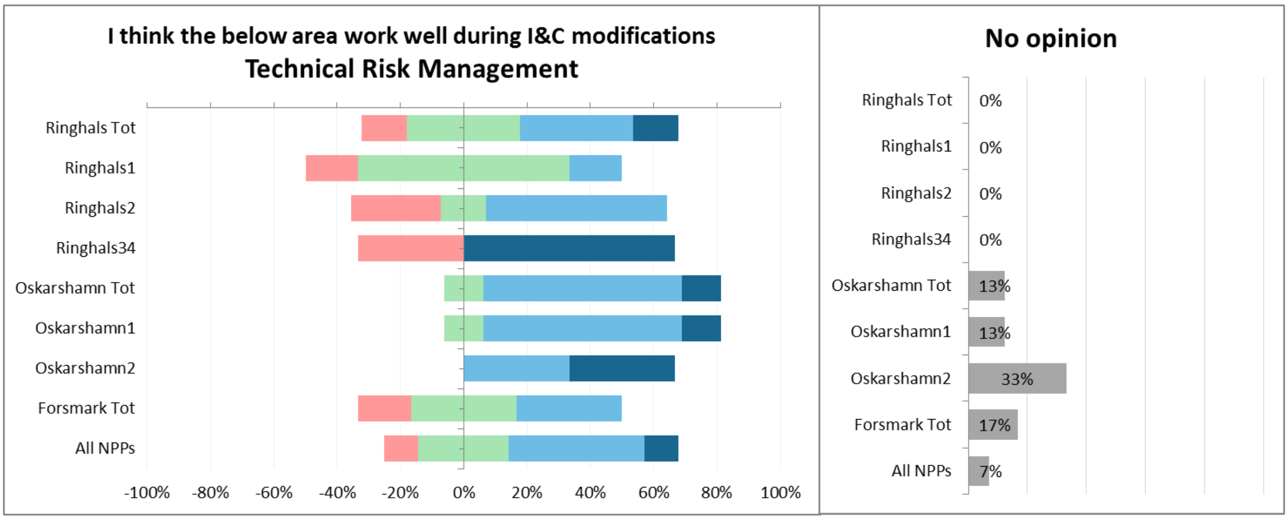
Graph 19. Configuration Management.



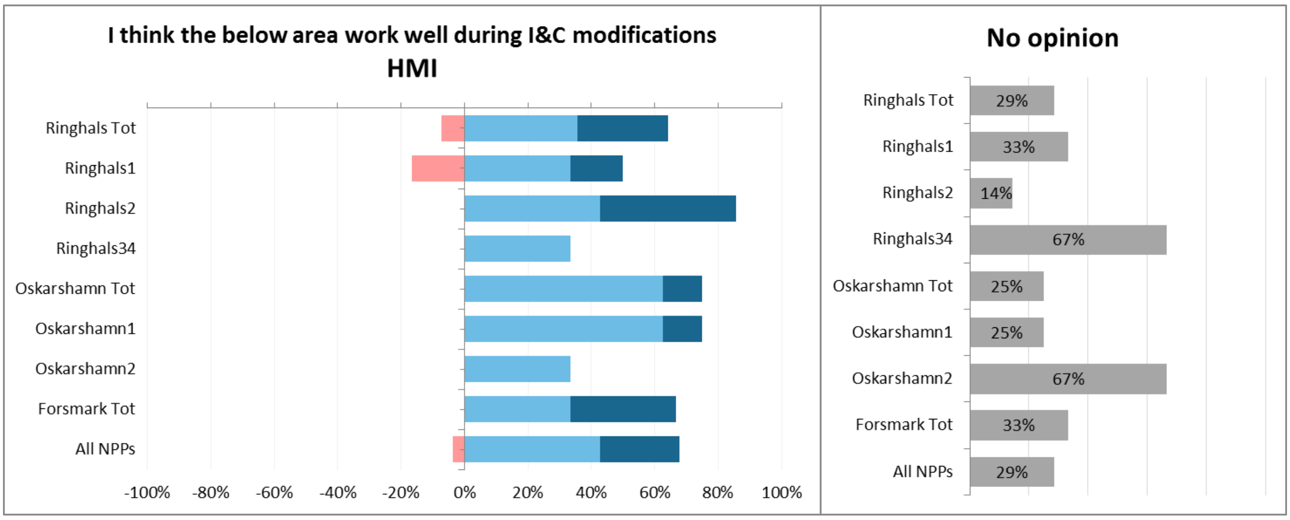
Graph 20. Verification and Validation.

Appendix 3. Graphs of multiple choice questions.

Strongly disagree	Tend to disagree	Neither agree or disagree	Tend to agree	Strongly agree	No opinion



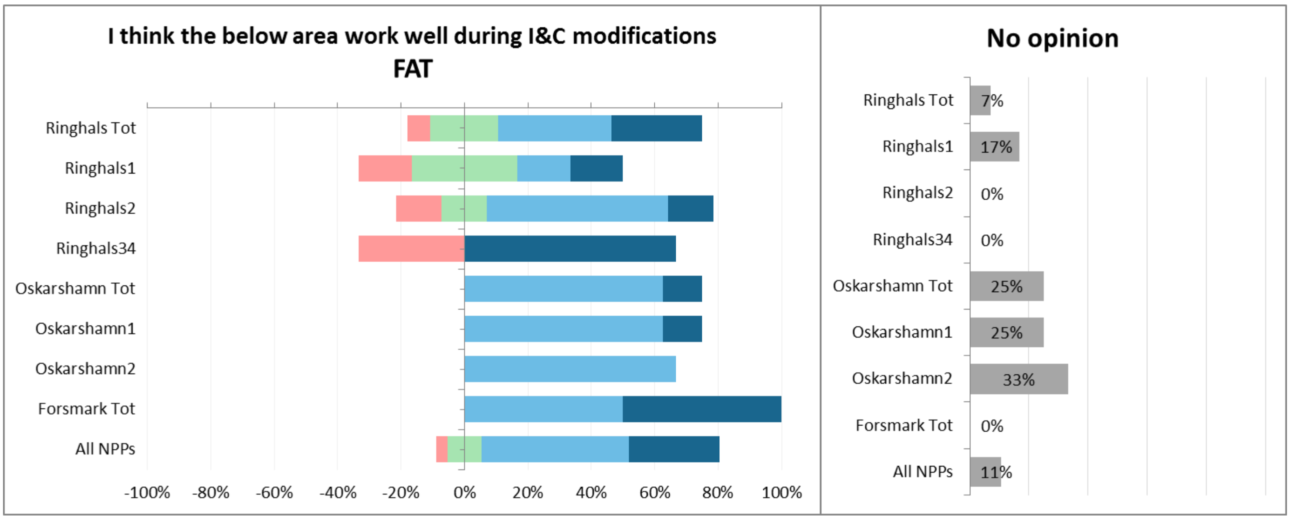
Graph 21. Technical Risk Management.



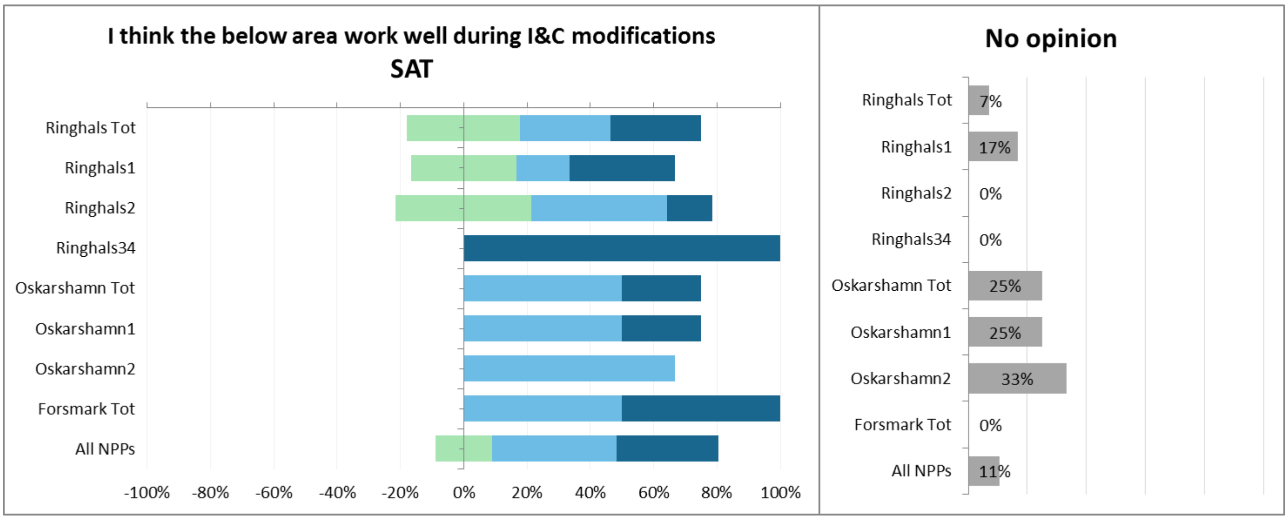
Graph 22. HMI.

Appendix 3. Graphs of multiple choice questions.

Strongly disagree	Tend to disagree	Neither agree or disagree	Tend to agree	Strongly agree	No opinion



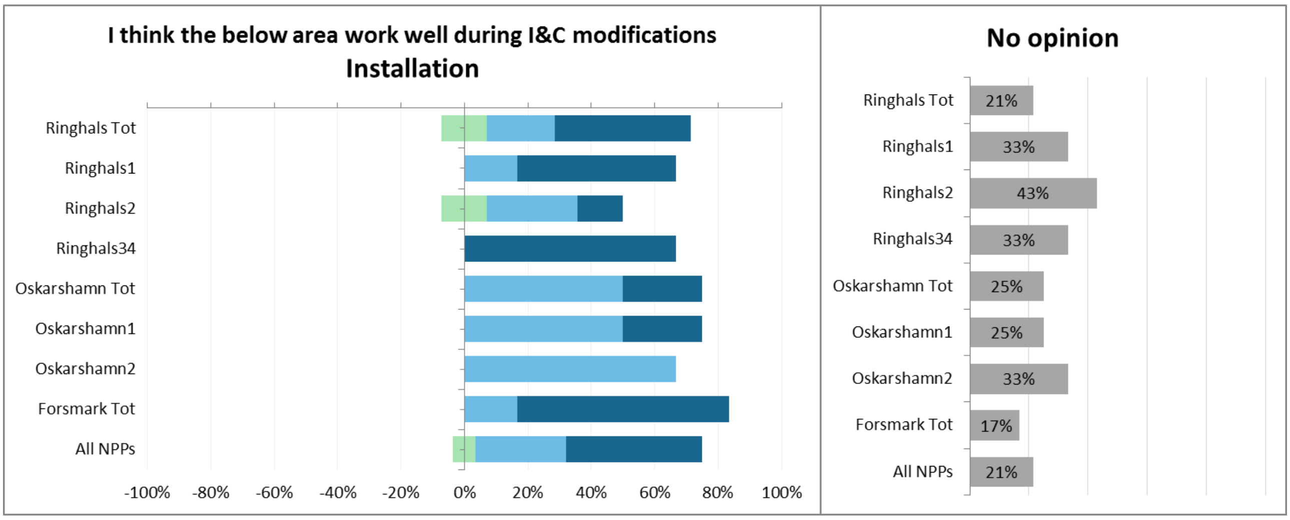
Graph 23. FAT.



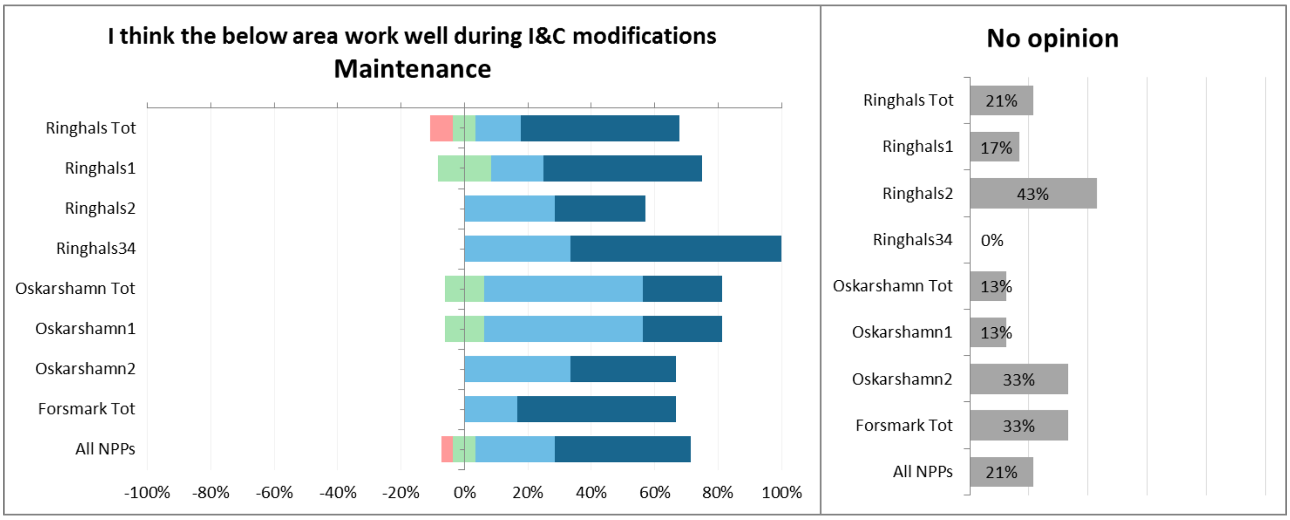
Graph 24. SAT.

Appendix 3. Graphs of multiple choice questions.

Strongly disagree	Tend to disagree	Neither agree or disagree	Tend to agree	Strongly agree	No opinion



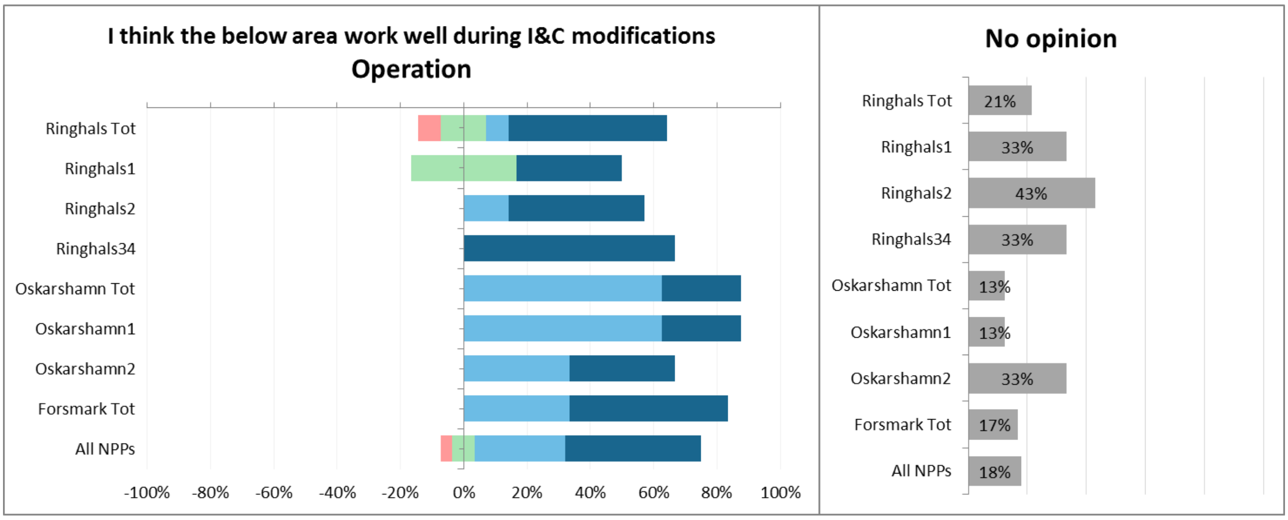
Graph 25. Installation.



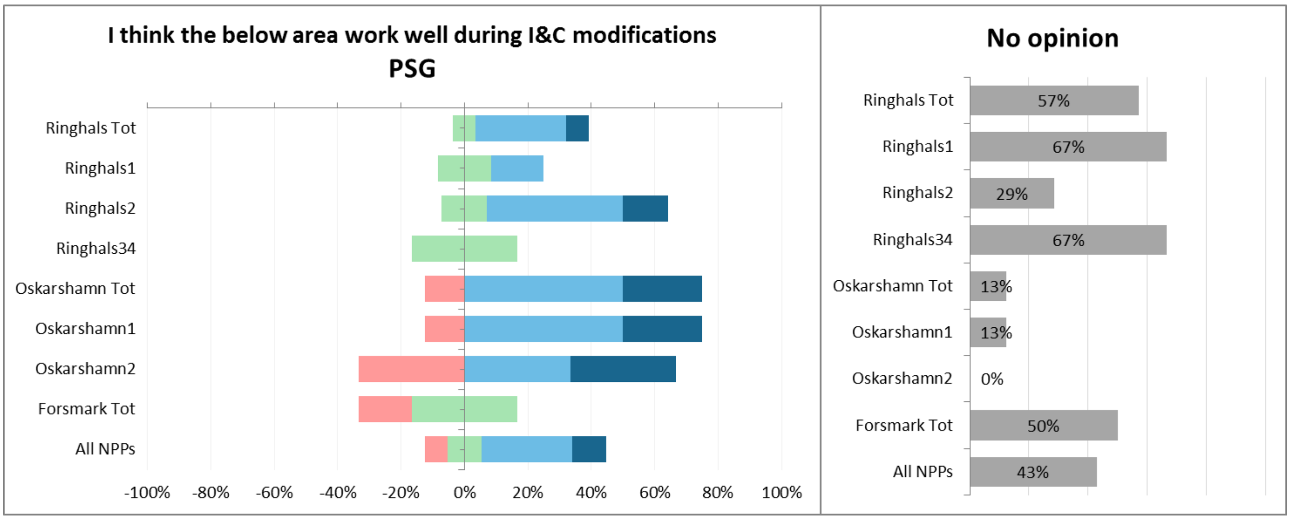
Graph 26. Maintenance.

Appendix 3. Graphs of multiple choice questions.

Strongly disagree	Tend to disagree	Neither agree or disagree	Tend to agree	Strongly agree	No opinion



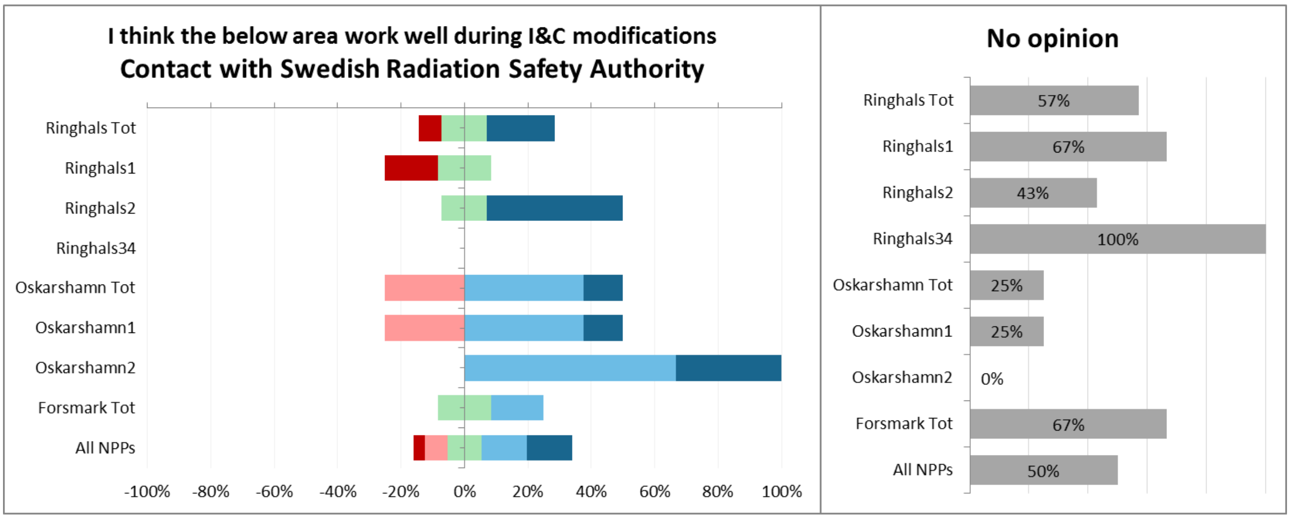
Graph 27. Operation.



Graph 28. PSG.

Appendix 3. Graphs of multiple choice questions.

Strongly disagree	Tend to disagree	Neither agree or disagree	Tend to agree	Strongly agree	No opinion



Graph 29. Contact with Swedish Radiation Safety Authority.

Appendix 4.
Comparison: AC160 - O1 VS R2. TXS – O2 VS R1.

Table 1. Comparison AC160 – Oskarshamn 1 VS Ringhals 2.

	O1	R2
	Safety System	**Safety System**
Platforms	AC160 from WEC TXS from Areva (for system 531)	AC160 from WEC
I&C platform application and functions	Reactor Protection (RPS) and all other Cat A functions in EKB (backup control building). A few Cat A functions is still placed in the old electric building and thereby in analogue systems. Neutron flow measurements PRM WRM, SRM, IRM, APRM, LPRM, SIRM system 531	Reactor Protection (RPS) + PRM (Reactor Trip, Engineering Safety Features, diesel sequence, Post-Accident Monitoring System)
I&C platform insertion year	Project MOD installed 2001-2002. Neutron flow measurement installed 1997.	1999-2010 Project TWICE
Projects that have been done on the platform. **Scope of project.**	The Autobor project has done the only function change (that was outside the qualification). Some smaller logic changes (alarms/measurement points) and parameter changes have been made. HW (CPU card changed), SW new version (high speed link).	PICUP 2011 was only remaining points from TWICE and DCRs. PICUP 2012 conducted smaller changes. PICUP 2013 changed basSW in AC160. PICUP 2014/2015 included changes (HW/applSW) in AC160 and Ovation.
Architecture basics (number of subs, processors, communication links etc.)	Number of subs: The logic is built in four subs where AC160 is used for CAT A, B and C functions. All that belongs to EKB is found in AC160. Number of electrical enclosures: 12 Cat A and 16 Cat B Number of Processors: AC160 has 174 processors Communication: Communication between the subs in Cat A is done via High Speed Link while all other communication is done via Advant Fieldbus 100 Other: O1 has no ODP or MTP screens (R2 has) There is a diversified RPS system (516-DPS) that is realised with electronic cards from Foxboro.	Number of subs: Four subs, A, B, C & D Number of electrical enclosures: Division A and B have 14 electrical enclosures and division C and D 12 electrical enclosures. Number of Processors: In total 96 processors, 4 MTP and 4 Operator Display Panels (ODP). Communication: Communication between subs in Cat A is done via High Speed Link.

Appendix 4.
Comparison: AC160 - O1 VS R2. TXS – O2 VS R1.

Table 1. Comparison AC160 – Oskarshamn 1 VS Ringhals 2

	O1	R2
	Safety System	**Safety System**
Spare parts	Available	Available
I&C changes conducted in-house / by supplier.	Supplier conducts parameter modifications Supplier conducts functional modifications Tests are made in TUSS by WEC.	R2 conducts parameter changes in-house. R2 conducts functional changes in-house (WEC is partly used for reviews and council). Tests are made in R2's test tool LES (1 of 4 subs).
Supplier strategy	Important to give WEC assignments so they do not lose interest in O1. O1 have signed a contract between OKG/WEC regarding minimum hours to be used for modifications at OKG each year. O1 believes it to be more cost effective to bring in WEC. The collaboration is currently very well-functioning. Important to have internal competence that knows the integration towards the plant. Supplier knows their product but it needs to be correctly implemented at OKG. O1 believes the supplier will be involved further on.	R2 have another supplier strategy compared to the other NPPs. It was a condition when starting TWICE that R2 should be able to perform changes in I&C without help from the supplier. R2 consider it to be risky when too much responsibility is put on the supplier since the NPP will lose competence and it will make the NPP more vulnerable. There could have been several benefits if WEC had been involved more in the 2014/2015 modifications in AC160 and Ovation. In that case it should have been important with internal competence which could have questioned the Supplier. R2 shall be able to evaluate errors in plant by them self. R2 has a lot of internal competence available. Therefore, the supplier contributes most if used for basic design criteria. WEC will have AC160 competence further on.
Resources in-house	O1 would like to conduct more modifications in-house, but do not have enough competence. O1 uses the supplier. O1's strategy has been to have sufficient I&C competence internally and to do changes without involvement from the supplier. It has been problematic to get enough resources. Now when O1 is starting to be old there is no longer any incentive to build up the internal competence. O1 will decommission in year 2032.	R2 have sufficient resources to conduct functional modifications in-house.

Appendix 4.
Comparison: AC160 - O1 VS R2. TXS – O2 VS R1.

Table 2. Comparison TXS – Oskarshamn 2 VS Ringhals 1.

	O2	R1
	Safety System	**Safety System**
Platforms	TXS from Siemens	TXS from Siemens/Areva
I&C platform application and functions	Reactor Protection (RPS) including all other 1E functions Neutron flow measurements PRM WRM, SRM, IRM, APRM, LPRM, SIRM system 531	RPS RPS - Diversified reactor protection system RHR - Diversified rest effect cooling RPM-Neutron flow measurement surveillance. R1 has divided RPS in to two parts, a new part DPS run by TXS and an old part OPS which still is analogue. HVAC - Safety ventilation for control electrical enclosures in V-building.
I&C platform insertion year	PLEX ongoing. Neutron flow measurement installed 2000 but will be updated during PLEX.	PRM installed 2006. RPS/RHR/HVAC installed 2009.
Projects that have been done on the platform. Scope of project.	No changes in neutron flow measurements besides corrections of errors. Otherwise PLEX.	The two coming outage after installation were clean-up project performed at R1, where remaining open items were closed, such as parameter changes, text changes etc. After that projects which have included functional changes have been performed: Autobor and the change of 314 valves. 2015 the last ÖGP project will be implemented which include functional changes.

Appendix 4.
Comparison: AC160 - O1 VS R2. TXS – O2 VS R1.

Table 2. Comparison TXS – Oskarshamn 2 VS Ringhals 1.

	O2	R1
	Safety System	**Safety System**
Architecture basics (number of subs, processors, communication links etc.)	There are approximately 60 TXS electrical enclosures and 60 TXP electrical enclosures in total. Processors: approximately 140 TXS (531 is in same platform)	Number of subs: Three subs, S1, S2 and S3. Two main subs (S1 and S2). Number of electrical enclosures: 55 Number of Processors: Approximately 70 processors in TXS. There are a few stand-alone processors. Communication: Processors communicates via fiber (five data bases).
Spare parts	Available	Available
I&C changes conducted in-house / by supplier.	Supplier conducts parameter modifications Supplier conducts functional modifications	Collaboration R1/Supplier when modifying parameters and functions.
Supplier strategy	Important to have internal competence that knows the integration towards the plant. Supplier knows their product but it needs to be correctly implemented at OKG. O2 believes the supplier will be involved further on.	R1 is positive in using the supplier for TXS changes.
Resources in-house	Could be more resources. O2 is vulnerable if staff disappears. O2 makes changes in the system now and then. Not enough to conduct a few modifications to retain competence.	Lack of in-house competence is an upcoming risk.

Experience from asset management of installed safety related programmable platforms/systems in Swedish NPPs

The examined NPPs have a large diversity in I&C products, configurations, complexity of changes and chosen strategies. It is important to plan ahead when programmable instrumentation and control equipment is chosen and configured for the first time in the Nuclear Power plant. The more functionality that are installed in the platform and the more communication, the more complex it will be to change and verify the system over time. From a strategic perspective, it is recommended to be selective when accepting changes in programmable systems. It should be evaluated if the requested plant functionality can be achieved by other technical solutions that do not lead to changes in programmable systems. If few changes are planned, this study indicates that NPPs are more satisfied using the supplier for changes.

Another step forward in Swedish energy research

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

Energiforsk