WHY ARE I&C MODERNISATIONS SO DIFFICULT?

EXPERIENCES WITH REQUIREMENTS ENGINEERINGS AND SAFETY DEMONSTRATION IN SWEDISH NPPS

Sofia Guerra and Catherine Menon·
Adelard LLP
3-11 Pine Street, London EC1R 0JH, UK
aslg@adelard.com; cm@adelard.com

ABSTRACT

Control and protection functions are long lived in comparison with the lifetimes of the equipment technologies that implement them. This implies that changes will need to be made to the I&C systems and the associated safety demonstrations over the lifetime of the plant. Indeed, there is often no choice but to change; the renovation is unavoidably dictated by a variety of circumstances including declining reliability of old installed equipment, reduced availability of spare parts, inability to maintain existing equipment, or amended requirements from the licensing authority. It is therefore important to ensure that the required safety level can be maintained over the plant lifetime in the face of these changes.

Several I&C modernisation projects have encountered issues and difficulties resulting in delays and overspend. This paper describes the work we have done with the aim of identifying the main issues that have been experienced in I&C modernization projects, and any lessons learnt during these projects. For this, we conducted a number of interviews in Swedish nuclear plants, focusing on the demonstration of safety and requirements engineering. The paper discusses the findings from our interviews, emphasising the problems associated with I&C projects in general, and with upgrades and modifications in particular. We present a brief discussion of these major problems, and suggest approaches to avoid them or ameliorate their effects. The lessons identified are applicable not just to I&C modernisation projects, but more generally to any I&C development projects. The consultation was followed by a series of workshops to discuss possible ways to address the difficulties that are often experienced by the industry.

Key Words: I&C modernization, Safety demonstration, Requirements engineering

1 INTRODUCTION

Several Information and Control (I&C) development projects have encountered difficulties, which have resulted in delays and overspend. As a result, Swedish Radiation Safety Authority (SSM) commissioned a consultation to determine whether these difficulties were caused by any fundamental underlying issues and if so, what lessons could be learnt from these projects. The long-term objective of this work was to identify ways to support licensees and, via the development of appropriate guidance, to reduce the difficulties of current or future projects.

During the autumn of 2012, Adelard conducted a number of interviews at Swedish nuclear plants focusing on modifications and upgrades of the I&C systems. We interviewed personnel from both new and existing builds across a wide range of roles, including both technical and technical management. The

focus of the consultation was on requirements engineering and safety justification approaches. This was followed up by two workshops that took place in 2013. These workshops allowed time for discussion of the most important issues raised in the consultation, and discussed possible ways forward.

This paper discusses the difficulties identified during the consultation and identifies with possible ways to reduce or mitigate these. The primary issues identified are those encountered by the existing plants in Sweden, as the new builds are yet to perform significant I&C development. However, in our experience, these issues identified are often encountered in I&C projects in general, independently of the specific regulations that are applicable. We believe that the lessons learnt and identified mitigations discussed are relevant to any I&C project, both modernisation or new build.

In Section 2 we discuss the main reasons for modernisation of I&C systems, as identified during the consultation. Section 3 describes the risks and issues recognised by the interviewees, while Section 4 discusses possible mitigations. Section 5 considers possible next steps. We conclude in Section 6.

2 REASONS FOR MODERNISATION

Control and protection functions are long lived in comparison with the lifetimes of the equipment technologies that implement them. This implies that changes will need to be made to the I&C systems, infrastructure and the associated safety justifications over the lifetime of the plant. It is therefore important to ensure that the required safety level can be maintained over the plant lifetime.

Indeed, there is often no choice but to change; the renovation is unavoidably dictated by a variety of circumstances. Obsolescence is one of the primary reasons for modifying or upgrading I&C systems. It may be difficult to obtain replacement components that are exactly the same as the originals, or the original vendors may not support the continued use of their product or service. In this case, a larger modification may need to be made than simply replacing the original component with a substitute.

A related reason for modifying systems is that of with plant life extension. Where a plant was originally planned to be shut down, a change in this plan can lead to a number of upgrades that must be made across the plant.

Problems with functionality or plant operation can also be a motivator for upgrading or modifying systems. In these cases, the upgrade may be performed as soon as the problem develops, or may be scheduled to be performed along with other planned modifications. In some cases these problems manifest when a particular event takes place (e.g., a power outage in the grid); a modification may be made to ensure that the plant can handle a similar event in future.

Modifications may be planned in order to introduce a change in functionality (e.g., a power upgrade), or to conform with new regulations (e.g., new regulations about diversity and defence in depth). They may also be introduced to reduce failure rates of the plant or of a particular subsystem

3 RISKS/ISSUES

3.1 Poor documentation of existing systems

When undertaking refurbishment projects, the system being developed has to be integrated into an existing working environment. Consequently, a full understanding of the existing functionality and of the plant design basis is essential, even in the case where the refurbished system is intended to provide identical functionality to that which already exists. This in-depth understanding of the existing system is essential to ensure that the system will satisfy the user's needs and achieve exactly the desired behaviour.

However, the existing documentation is often deficient, incomplete or out-of-date. As one of the interviewees pointed out, in Sweden, the existing plants were scheduled to be shut down in 2010 and therefore were not designed to be maintained. While the existing system requirements may be stated in plant documentation, the plants do not always have a process for documenting and managing requirements that has been consistently maintained since the plant's inception.

Instead, many requirements have not been formally documented, and those which have are to be found across a large number of paper documents, some of which may be missing or poorly maintained. These documents themselves are not necessarily consistent with each other, either because they were never cross-checked, or because they have been inappropriately updated (see Section 3.3). A comment from one of our interviewees illustrates this situation well: "There are three sets of requirements: what the requirements really are, what the documentation captures, and what is actually there in the plant".

This is a significant issue for refurbishment projects. "Everything is there for a reason, and it is needed to understand why", was one of the comments we heard. However, achieving this understanding is a problem that may not be easy to address.

3.2 Weak requirements elicitation process

The issues described in the section above could be addressed by a strong, well-structured approach to requirements elicitation. In some cases no such adequate process for requirements elicitation exists. There is uncertainty around requirements (both on functionality and licensing) and inconsistencies are only addressed late in the development process.

For larger projects, the requirements elicitation is performed by both the utility and the supplier: the utility will start by producing a specification that is then passed to the supplier (or suppliers, if more than one is under consideration). The suppliers will then develop their own solution, and negotiation between supplier and utility will take place to agree the final solution (and corresponding set of requirements).

Several weaknesses in the process have been pointed out, which include:

- Lack of detailed understanding, both on the utility and supply side, of the plant constraints and plant behaviour.
- Lack of detailed understanding of the requirements on the component being replaced. It may not always be possible to deduce the requirements from the component characteristics, as the actual requirements may be more or less stringent than the characteristics of the component being replaced.
- Lack of understanding of the impact of new functionality and failure modes.
- Lack of understanding of HMI and interface requirements.
- Lack of familiarity of suppliers with the relevant nuclear requirements.
- Lack of agreed interpretation of regulatory requirements.
- Requirements vague and unclear at the time of setting the contract.

The interviewees identified examples of projects where the utility relied on the supplier to understand the plant behaviour and to define the requirements for the new system. In the 1970s, when most of the plants operating today were constructed, suppliers were large, experienced organisations that had comprehensive in-house capabilities for design and manufacturing. Since then, suppliers have lost much of their knowledge and skills because experience experts have retired, and until recently, there has been no need to keep such knowledge and skills in-house. Even in the cases where the supplier developing the replacement solution is the same that originally developed the system, there is no guarantee that they will

still understand the plant and the national regulations in any level of detail. This was identified as a problem by several of the interviewees.

3.3 Lack of requirements traceability

To manage requirements there is a need to keep *requirements traceability*. Requirements traceability assists the understanding of the relationships between requirements, their sources, the design and the implementation of a system. Without appropriate requirements traceability, it is difficult to show that requirements have been met, and consequently it can be difficult to justify the licensing of the system.

Lack of traceability between high-level plant requirements and component-level requirements means that it is difficult to assess the impact of a change made at the component level. Specifically, the extent to which this change impacts the high-level behaviour of the plant may be unknown. This is especially important during the development and negotiation of the requirements specification. As described in Section 3.2, suppliers develop their own requirements specification that may or may not meet all the initial plant requirements provided by the utility. In order to agree on a final specification, it is necessary that the effect of any change in requirements can be fully predicted. Furthermore, being able to identify the sources of the requirements is crucial for achieving a successful specification.

3.4 Scope creep

A major problem in modernisation projects of I&C system is *scope creep*: unintentional introduction of extensive or uncontrolled change as a result of implementing a smaller change. In several of the interviews, participants identified situations where introducing a (small) change to an I&C system resulted in a much larger modification. This was due to the fact that the systems in question were very integrated. That is, there was limited separation by design of these systems.

The modernisation project, therefore, became a much larger project than originally anticipated, with the resulting difficulties of implementing, managing and licensing a complex I&C system. This is likely to be exacerbated when using new designs and solutions, resulting in potential difficulties with modifications and maintenance.

3.5 Impact of new technologies

New digital technology does not always allow the new systems to work exactly the same way the old relay based systems used to work. Without understanding the plant behaviour in detail, and the difference in behaviour between the existing and new system (which may be unavoidable consequence of the new technology and the choice of Commercial-Off-The-Shelf (Cots) products available in the market), there may be unforeseen interactions that may have undesirable results. The incident in Forsmark in 2006 was given as an example of such problem [1].

Competency is a problem with introduction of new technologies, as referenced in Section 2. This problem was explained to us as a generation gap caused by the plans for shutting down all plants by 2010: there was no need to train a new generation of engineers, as the plants would not be in operation. The generation that used to understand the plant has retired, and the new generation may understand the new technology, but not the plant behaviour and the impact of subtle failure modes that may have an undesired impact.

More subtly, there are problems associated with being the first to use a particular new technology. Lack of historical evidence means that it is harder to adequately support the safety claims; this can then result in problems licensing the plant. Similarly, even if new or innovative technologies meet the functional requirements of the plant, they may not meet the regulatory requirements. Similar issues arise with being “one of a kind”, i.e. the only plant to use a particular solution or technique.

3.6 Software is difficult

In spite of the clear advantages of software-based systems, including flexibility, greater accuracy and stability, diagnostics, etc., the inherent difficulty with the justification of software-based systems means that well-founded and accepted strategies for justifying software in the Swedish nuclear industry are still at their infancy.

One of the most notable differences between conventional or electrical systems, and software-based systems, is related to the discrete nature of software. For example, when a software-based system is tested on a particular input, there is no way to guarantee what its behaviour will be on other inputs, even if the inputs are "near" to the one tested.

In addition, given the inherent complexity of software-based systems and the magnitude of its state space, it is difficult to completely understand the behaviour of software-based system. Consequently, there is the potential for adding functionality without being fully aware of this (or without understanding the consequences, as discussed in Section 3.4). This, together with the fact that no procedures exist for designing completely error-free software, means that software is more prone to design faults.

Although there is some guidance and regulations on justifying software-based safety systems, considerable interpretation is still needed. In some cases, the approach taken was to avoid software in safety systems until more widely accepted strategies have been developed.

3.7 Dealing with Cots products

Several of the difficulties with dealing with Cots products have been discussed above: understanding the requirements for the component, the plant constraints and determining to what extent these are met by the product. In particular, requirements elicitation may be particularly difficult when a Cots product is involved in a change, as the component may be insufficiently characterised. That is, when introducing a Cots product, the complete extent of its functionality may not be known. There may be uncharacterised properties or unknown functionality, which means that the impact of the change is different to that which would have been expected.

In addition, Cots products often do not meet the high requirements of the nuclear industry. For example, they are often not developed to IEC 60880 and might not meet the nuclear regulations. However, this was not considered a significant problem by the interviewees, one of whom expressed that "standards are based on 10-year-old experience on aspects they could agree on. If the non-compliances are justified by good arguments, they are not a problem." It should be noted, however, that this is likely to become a problem if the competence does not exist to provide this justification, as discussed in Section 3.12.

3.8 Suppliers not familiar with licensing requirements

A common problem is the suppliers' lack of understanding of the licensing requirements. This may be because they are not accustomed to working with the nuclear industry, or because they do not understand the specific Swedish regulatory environment.

Regulatory requirements are different in different countries, and there is often an assumption that the requirements can be read across. This assumption may lead to underestimating the effort required for licensing, for example, where a platform has been previously licensed elsewhere. The lack of understanding of regulatory requirements can also lead to uncertainties in licensing, as seen in Olkiluoto 3 in Finland [2].

3.9 Safety justification considered too late

Often, the safety justification of the system is linked to the update of the Safety Assessment Report and to the Independent Safety Review (ISR), both of which are performed towards the end of the project. Consequently, there has been limited consideration of a justification strategy until relatively late in the process. As one of the interviewees pointed out, "if the ISR is done at the end, it is too late to influence the design, and there is a bias towards accepting the system."

This approach can lead to design changes late in the project, the need for additional verification activities, and multiple iterations of particular development activities. From a project risk viewpoint, all of these consequences increase the likelihood of project overrun and overspend. A number of interviewees cited recent projects that have acknowledged the importance of defining a justification strategy early, e.g., the definition of safety subject areas used for Twice [3]. The Twice approach has been transformed to a generic strategy "Safety Demonstration Plan Guide [4]. However, this "early-justification" approach is not yet widely accepted in the industry in Sweden.

3.10 Approach to justification unclear

There is no established approach to safety justification. For most projects, the justification is presented across several documents that interact and refer to each other. However, there is no single presentation of the safety justification that can be easily reviewed and it is not clear how these documents together present a coherent, compelling argument to justify the safety of the system.

The lack of an established approach to safety justification was identified as an issue by several interviewees, particularly for projects with a reasonable degree of complexity. "Each project is one of its kind," as a new strategy needs to be developed for each project. In general, there is no common agreed approach to safety justification.

3.11 Contractual arrangements do not support safety

Although contractual arrangements are somewhat outside the scope of the consultation, there was some indication that the arrangements used for a number of projects do not support safety demonstration. There are two major problems: the timing of the contractual negotiations and the division of responsibilities defined within these contracts.

Firstly, the licensing requirements are relatively weak or undefined at the start of negotiations with the supplier. This is partly due to a lack of clarity of the regulatory requirements, and partly due to a tendency on the part of the utility to delay engaging with the regulatory requirements sufficiently early in the project. As a result, the terms of the contract are in some cases set before the safety requirements have been fully clarified, meaning the contractual requirements as set may not match the plant needs, or may not be sufficiently clear. The result of this may be requirements creep later in the project (with the attendant increase in project spend on both cost and time), contractual difficulties, the de-prioritization of safety or the production of a solution that cannot be justified.

Secondly, interviewees identified a previous project that demonstrated a contractually problematic division of responsibilities. The contract placed all responsibility for the identification and satisfaction of safety and regulatory requirements on the supplier. This is contractually unsound because the utility, not the supplier, needs to own the safety requirements. That is, it is the utility who is ultimately responsible for the safety of the plant, and this cannot be delegated via contractual arrangements to the supplier. During the project, it became apparent that the effort required for the safety justification was considerably more onerous than anticipated. This resulted in project stress, delays and a temporary de-prioritization of licensing needs.

3.12 Lack of appropriate competence and skills

Lack of the appropriate competencies and skills was also identified as a major risk to plant upgrades and modification. There are a number of related factors that combine to make this a particularly pervasive issue.

Firstly, as discussed in Section 3.5, there is a competence split due to the "generation gap". Newer engineers are competent with emerging digital technology but do not necessarily understand the underlying plant behaviour, while older engineers are competent to understand the characteristics of the existing plant, but not necessarily those of new or emerging technologies and solutions. This means that the full impact of a change can be difficult to characterise as no single point has all the information regarding the change. Unforeseen interactions between the replacement and the existing systems may then occur.

Secondly, the plant operators are also part of the system and must be competent to operate both the existing and any replacement systems. The overall safety of the plant depends equally on the competence of the operators and the competence of the engineers. A lack of operator training was identified by one interviewee as potentially compromising this overall plant safety.

Finally, adequate competency is needed in order to justify the safety of the system. In particular, it may be possible to justify particular non-compliances with standards by use of a compelling and well-supported argument. This is particularly important for Cots products, where the development may not match the compliance route specified by the regulations. As one of the interviewees stated, "one cannot influence how Cots products are developed." As such, arguments to justify that the Cots product is suitable despite the non-compliance will be needed.

However, justifying the safety of complex digital systems requires particular skills and competencies. The digital technology must be well-understood, the underlying safety principles must be identified, the argument must be well-supported and compelling, and the safety requirements must be verified, validated and traceable. Without sufficient competency in safety analysis, and sufficient understanding of the plant, it may not be possible to construct an adequate argument to justify a non-compliance. This may result in licensing issues if the regulator considers that non-compliances have not been adequately justified.

4 MITIGATIONS

4.1 Adequate requirements engineering

One of the major recommendations to address most – if not all – of the issues identified above is to spend more time on requirements engineering. This includes all aspects of defining, refining, understanding, eliciting and validating requirements. In particular, the safety requirements need to be owned by the utility. They are not the responsibility of the supplier to define, and the utility should identify and manage these throughout their lifetime.

Furthermore, the requirements elicitation process should be begun well before contractual processes begin. This includes negotiation with suppliers to define a working set of requirements: this should precede, not follow, binding contractual arrangements.

The requirements engineering process should address:

- all explicitly documented requirements
- updates due to the proposed change
- requirements embedded in implementation decisions

To produce a complete survey of existing functions and interfaces, all available relevant information should be reviewed. If necessary, additional work may then be required to identify and record missing requirements. The resulting set of requirements, applicable to the original I&C system, must then be revised to reflect the new requirements and the reasons for change, so that they are relevant to the new I&C system.

4.2 Systematic approach to requirements management

This is related to the mitigation discussed in Section 4.1, and we note that requirements management is necessary throughout the plant life, not just during the stage of requirements elicitation. Requirements management includes adequate documentation and maintenance of requirements, such as the maintenance of traceability between a requirement and its source, as well as between a requirement and evidence showing this has been satisfied.

The requirements management process should include:

- identification of all requirements on a particular component or subsystem, and association of these with their sources
- the capability to track requirements and note their evolution throughout the project

More generally, adequate configuration management is essential to maintain consistency of requirements documentation throughout lifetime, and across multiple projects. All requirements and associated information should be subject to the configuration management process. This will aid in promoting a common understanding of the requirements across projects, as well as a common interpretation of licensing requirements.

4.3 Understanding existing systems

While requirements engineering and requirements management are essential, it is also important to understand that the documented requirements only represent part of the behaviour of the system. The actual behaviour of the original system is made up of the behaviour due to the requirements and the behaviour due to the implementation.

Characteristics and behaviour which may not be documented in the requirements include the way in which requirements were interpreted by the original developer – particularly where these requirements are non-specific or vague – the limitations of the system, the particular behavioural variations which may occur within the limits of the requirements, and any system dependencies which result from the choice of implementation.

More time needs to be spent on understanding the principles and functions of the plant, and understanding the rationale for why it has been built in any given way. This is perhaps most effectively performed by making use of relevant expertise including engineers familiar with the plant and its implementation. When performing modifications, it is essential that the underlying principles on which the plant was built should not be changed without a thorough assessment and adequate justification. Failing to perform this assessment and supply the justification can result in uncontrolled change.

4.4 Holistic approach to requirements

It is important to take a holistic approach to requirements engineering. This process should not be limited to technical requirements but should also include regulations, human factors requirements and general project requirements necessary for the safety justification. The requirements specification should include not only all aspects relating to the plant (e.g., scope, functional requirements) but also those aspects that relate to the project and its processes (e.g., quality assurance, organisation and competence, configuration management). The SQAD (Safety/Quality Assurance Demonstration) methodology used in

Ringhals is an example of how to effectively integrate product management aspects and safety and quality management aspects [3].

4.5 Architectural choices to support safety

There are certain architectural choices that can be made when performing modifications that are more likely to support safety or reduce the complexity of a safety justification. Choosing a simple, modular architecture with clearly designed interfaces can reduce the likelihood of an uncontrolled change in this or later modifications. In particular, this will promote explicit separation between I&C systems, which will correspondingly reduce scope creep and simplify impact analyses.

The requirements on the interfaces between I&C systems and the rest of the plant need to be clearly understood, as described in IEC 61513.

4.6 Timely consideration of safety and licensing needs

Early consideration of safety, licensing requirements and the safety justification strategy is essential in order to minimise project risk and costs. This can aid in the choice of a design that minimises the scope of safety assessment, and hence the project costs associated with this. In addition, a timely consideration of safety leads to a timely production of safety assessment evidence and a consequent reduction in project costs. By contrast, the retrospective production of safety evidence can add significantly to these costs.

The safety justification strategy should address the following questions:

- Is there a rationale for the I&C requirements, and are they feasible?
- Is there an associated safety justification and is it feasible?
- Is it feasible to acquire the evidence as the project proceeds?
- Is it credible that the supply chain can deliver the systems envisaged?

An appropriate safety justification strategy will ensure an adequate level of safety, minimise licensing risk and minimise commercial risk. The use of a Safety/Quality Assurance Demonstration Plan (as used in Ringhals) [3] is an example of early consideration of a safety justification strategy.

4.7 Improved communication with regulator

Improving communication with the regulator is likely to lead to an improvement in many of the issues identified earlier. Early communication with the regulator will aid in finding a common interpretation of the requirements, and will also help to clarify any vague or undefined requirements. Furthermore, this timely communication will provide the regulator with an opportunity to influence the design at a stage when the project costs associated with this are relatively slight. It should be noted that this communication should not be delayed until all details on the design and safety approach are available; general comments may be sourced at a high level from the regulator without all details being needed.

5 FOLLOWING UP RESULTS

The consultation results were presented and discussed in two subsequent workshops. The participants identified the following major motives for change:

- reduce overall lifecycle costs
- reduce licensing risks
- ensure that required functionality and safety requirements are met, achieved and demonstrated

- enable modifications to the I&C system
- enable effective communication
- writing contracts that support safety, including clear requirements on the system and suppliers.

The workshop participants developed a list of possible actions at utility, industry and regulator level. The major actions identified were:

- Development of guidance, education and training on requirement engineering and safety justification approaches. This should include a set of common principles, which could build on a number of sources, e.g., guide on New Build and Finnish documents on how to couple requirements, attributes and contexts.
- Knowledge transfer on plant design and design basis for I&C systems within each plant.
- Raise awareness at management level of the importance of Requirements Engineering and Safety Justification approaches to increase engagement and control, and change in safety behaviour.
- Organise and participate in workshops and seminars. This could include:
  - an industry wide workshop for sharing experiences on different projects, and include success stories as well as difficulties.
  - a workshop for managers to communicate the outcomes from this group

In fact, several initiatives are in place in Sweden to address some of these issues. For example, Elforsk has funded a project on Safety Demonstration Plan Guide [4].

6 CONCLUSIONS

In this report we have identified a number of issues around the upgrades and modifications of I&C systems in Swedish nuclear plants. We have presented multiple recommendations, most of which address several of these issues. It is clear that any attempt to improve the licensing process and safety assessment of I&C modifications will require commitment from all stakeholders – regulators, utility and suppliers – as well as involvement from both technical and managerial staff.

Although individual recommendations have been provided above, there are five major keystones to any successful future project. These are:

- spend more time establishing requirements
- understand the existing plant and the impact of any change
- start early on safety justification and licensing
- communicate early and often with the regulator
- adequate requirements management is crucial to safety justification

We believe that the issues and mitigations identified here are applicable to the nuclear industry in general, and can be considered within any general regulatory framework.

7 ACKNOWLEDGMENTS

This work was funded by Swedish Radiation Safety Authority (SSM). We thank all the people who participated at the consultation, by making time to talk to us about their experiences.

8 REFERENCES

1. E Ilina and Hakan Sundquist. “Incident in the Forsmark 1 nuclear power plant in 2006 and knowledge breakdowns” *Int J. Nuclear Knowledge Management,* **Volume 3, No.3**, 2010.
2. J Laaksonen.”Lessons Learned from Olkiluoto 3 Plant”. *Nuclear Power Europe*, 2010.
3. H Edvinsson and P Ryd. “Modernization of I&C in Ringhals Unit 2 – Licensing and Safety Demonstration Experience”. *Nuclear Power Europe*. 2011.
4. “Safety Demonstration Plan Guide. A general guide to Safety Demonstration with focus on digital I&C in Nuclear Power Plant modernisation and new build projects”. Elforsk Rapport 13:86.