nks

Nordisk kernesikkerhedsforskning
Norrænar kjarnöryggisrannsóknir
Pohjoismainen ydinturvallisuustutkimus
Nordisk kjernesikkerhetsforskning
Nordisk kärnsäkerhetsforskning
Nordic nuclear safety research

NKS-163
ISBN 978-87-7893-228-0

MORE: Management of Requirements in NPP Modernisation Projects Project Report 2007

Rune Fredriksen, Vikash Katta and Christian Raspotnig
Institutt for energiteknikk (IFE), Norway

Janne Valkonen
Technical Research Centre of Finland (VTT)

March 2008

Abstract

This report documents the work and related activities of the MORE (Management of Requirements in NPP Modernisation Projects, NKS_R_2005_47) project in the period January 1 – December 31 in 2007. The focus of this report is on improvements of the former project results, to identify and apply a couple of case studies from NPP projects, and activities in order to initiate and implement the industrial take-up and utilisation of the research results in real modernisation projects. The report also provides a brief description of the extended industrial network and disseminations of the results in Nordic and NKS related events such as seminars and workshops.

Key words

change management, requirements engineering, software engineering, software requirements, traceability, verification and validation

NKS-163
ISBN 978-87-7893-228-0

Electronic report, March 2008

The report can be obtained from
NKS Secretariat
NKS-776
P.O. Box 49
DK - 4000 Roskilde, Denmark

Phone +45 4677 4045
Fax +45 4677 4046
www.nks.org
e-mail nks@nks.org

MORE
Management of Requirements in NPP Modernisation Projects
- Project Report 2007 -

Rune Fredriksen, Vikash Katta, Christian Raspotnig
Institutt for energiteknikk (IFE)

Janne Valkonen
Technical Research Centre of Finland (VTT)

MORE

Management of Requirements in NPP Modernisation Projects

NKS_R_2005_47

Title

Project report 2007

Author:

Rune Fredriksen, Vikash Katta, Christian Raspotnig, Janne Valkonen

Keywords:

change management, requirements engineering, software engineering, software requirements, traceability, verification and validation

Abstract:

This report documents the work and related activities of the MORE (Management of Requirements in NPP Modernisation Projects, NKS_R_2005_47) project in the period January 1 – December 31 in 2007. The focus of this report is on improvements of the former project results, to identify and apply a couple of case studies from NPP projects, and activities in order to initiate and implement the industrial take-up and utilisation of the research results in real modernisation projects. The report also provides a brief description of the extended industrial network and disseminations of the results in Nordic and NKS related events such as seminars and workshops.

Issue Date:		Name	Date
	Prepared by:	Rune Fredriksen	25.01.2008
	Reviewed by:	Bjørn Axel Gran	30.01.2008
	Approved by:	NKS	March 2008

Foreword

This document constitutes the 2007 report for the project MORE: Management of Requirements in NPP Modernisation Projects (NKS-R project number NKS_R_2005_47, started on July 1, 2005). The project aims at the industrial utilisation of the results from the project TACO: Traceability and Communication of Requirements in Digital I&C Systems Development (NKS-R project number NKS_R_2002_16, completed in June 30, 2005), and practical application of improved approaches and methods for requirements engineering and change management.

The purpose of this report is to document the work and related activities in the period January 1 – December 31 in 2007, including dissemination activities. The work in this period has been concentrated on improvements of the former project results, to identify and apply of a couple of case studies from NPP projects, and activities in order to initiate and implement the industrial take-up and utilisation of the research results in real modernisation projects. We have also extended the industrial network through disseminations and presentations of the results in Nordic and NKS related events such as seminars and workshops.

Halden, January 2008

Rune Fredriksen

Table of Contents

Applied Abbreviations

DRE	Dependable Requirements Engineering
EUP	Enterprise Unified Process
I&C	Instrumentation & Control
ICT	Information and Communication Technologies
IFE	Institute for energy technology
LPRM	Local Power Range Monitoring
MBRA	Model-based Risk Assessment
MORE	Management of Requirements in NPP Modernisation Projects
NKS	Nordic nuclear safety research
NPP	Nuclear power plant
RUP	Rational Unified Process
SKI	Swedish Nuclear Power Inspectorate
STUK	Radiation and Nuclear Safety Authority of Finland
TACO	Traceability and Communication of Requirements in Digital I&C Systems Development (NKS project number NKS_R_2002_16)
V&V	Verification & Validation
VTT	Technical Research Centre of Finland

Summary

This document constitutes the 2007 report for the project MORE: Management of Requirements in NPP Modernisation Projects (NKS-R project number NKS_R_2005_47, started on July 1, 2005). The project aims at the industrial utilisation of the results from the project TACO: Traceability and Communication of Requirements in Digital I&C Systems Development (NKS-R project number NKS_R_2002_16, completed in June 30, 2005), and practical application of improved approaches and methods for requirements engineering and change management.

The overall objective of the project MORE is to improve the means for managing the large amounts of evolving requirements in Nordic NPP modernisation projects. In accordance to this objective, the activity will facilitate the industrial utilisation of the research results from the project TACO, and practical application of improved approaches and methods for requirements engineering and change management.

On the basis of experiences in the Nordic countries, the overall aim of the TACO project was to identify the best practices and the most important criteria for ensuring effective communication in relation to requirements elicitation and analysis, understand ability of requirements to all parties, and traceability of requirements. The project resulted in the development of a traceability model for handling requirements from their origins and through their final shapes. The traceability model is in terms of a *requirement change history tree* built up by linking the different requirements together through the definition of a simplest syntactical form for a requirement being a *paragraph*, through a complementary set of basic requirement *change types*, and through generic mechanisms for requirement *categorisation*.

On the basis of compiled experiences on the problem of handling large amounts of information in relation to Nordic modernisation projects, the project MORE aims at investigating how to handle large amounts of evolving requirements in modernisation projects, where the original requirements and their patterns of development are subject to change. Developing pragmatic mechanisms for change management is therefore an important prerequisite for the success of the project MORE.

The work in this period has been concentrated on improvement of the former reported results from the project. The improvements are based on received feedback and gained knowledge. Our goal has been to identify and apply the results on case studies from NPP projects and activities in order to initiate and implement the industrial take-up and utilisation of the research results in real modernisation projects. We have continued to compile experiences on the problem of handling large amounts of information in relation to Nordic modernisation projects, amongst others, through organised visits to selected plants, and extended the industrial network through disseminations and presentations of the results in Nordic and NKS related events such as seminars and workshops.

The purpose of this report is to document the work and related activities in the period January 1 – December 31 in 2007, including dissemination activities.

1. Introduction

Experiences from modernisation projects at NPPs, particularly in Sweden and Finland, indicate the importance of adequate structure and modularisation of the requirements. It is important to handle the evolution of the requirements and the completeness with respect to the requirement sources, supported by some formalism for structuring the requirements. A particular issue is how to make an evolutionary, iterative systems engineering process that reflects the evolving nature of the requirements and their understanding, and at the same time meets the requirements set by the licensing authorities, e.g. with respect to quality assurance and documentation. An important part of such a process is traceability features making it possible to trace the requirements back to their origins and forward to their final (actual) specifications.

The overall objective of the project MORE is to improve the means for managing the large amounts of evolving requirements in Nordic NPP modernisation projects. In accordance to this objective, the activity facilitates the industrial utilisation of the research results from the project TACO, and practical application of improved approaches and methods for requirements engineering and change management. On the basis of experiences in the Nordic countries, the overall aim of the TACO project was to identify the best practices and most important criteria for ensuring effective communication in relation to requirements elicitation and analysis, understandability of requirements to all parties, and traceability of requirements. The project resulted in the development of a traceability model for handling requirements from their origins and through their final shapes. The traceability model is in terms of a *requirement change history tree* built up by linking the different requirements together through the definition of a simplest syntactical form for a requirement being a *paragraph*, through a complementary set of basic requirement *change types*, and through generic mechanisms for requirement *categorisation* [1][2].

The purpose of this present report is to document the work and related activities carried out in the period January 1 – December 31 in 2007 and the further research and related activities to the project MORE: Management of Requirements in NPP Modernisation Projects (NKS-R project number NKS_R_2005_47, started on July 1, 2005).

Chapter 2 describes the approach for dependable requirements engineering adopted in the project MORE. Chapter 3 discusses the improvement of the approach for dependable requirements engineering (DRE) and the application of the approach on the Local Power Range Monitoring (LPRM) case study. Chapter 4 describes some related activities within the Nordic area we are familiar with. Chapter 5 contains a brief summary of some of the topics of interest within the network. Chapter 6 acknowledges the contributors to MORE. Chapter 7 presents the references used to compose the report.

Appendix A features the project activity plan and organisation, and appendix B contains the MORE dissemination for 2007.

2. An Approach for DRE

This chapter describes a practical approach for dependable requirements engineering (DRE) of computerised systems. The approach is the joint result of research within requirements engineering, systems modelling (mainly based on object-oriented, semi-formal and agent-oriented modelling methodologies), dependability analysis and model-based failure and risk analysis and assessment [3][4][5]. The following provides some background and covers the main aspects of the approach.

2.1 The Background

Especially within information and communication technologies (ICT) and their applications in different branches, several approaches have been proposed towards a better system development process. Among the most applied approaches is the Rational Unified Process [6] (RUP) that provides a matrix-oriented lifecycle model highly supporting the time aspect of the lifecycle. Here, the road map is formed by two main activity categories: disciplines followed to develop the system and phases related to its life-path. The workload in each phase is decided by the actual discipline in focus: More elaboration phase is required during the design discipline, whereas more construction is needed during the implementation. Figure 1 illustrates another extended version of the RUP model, called the Enterprise Unified Process (EUP).

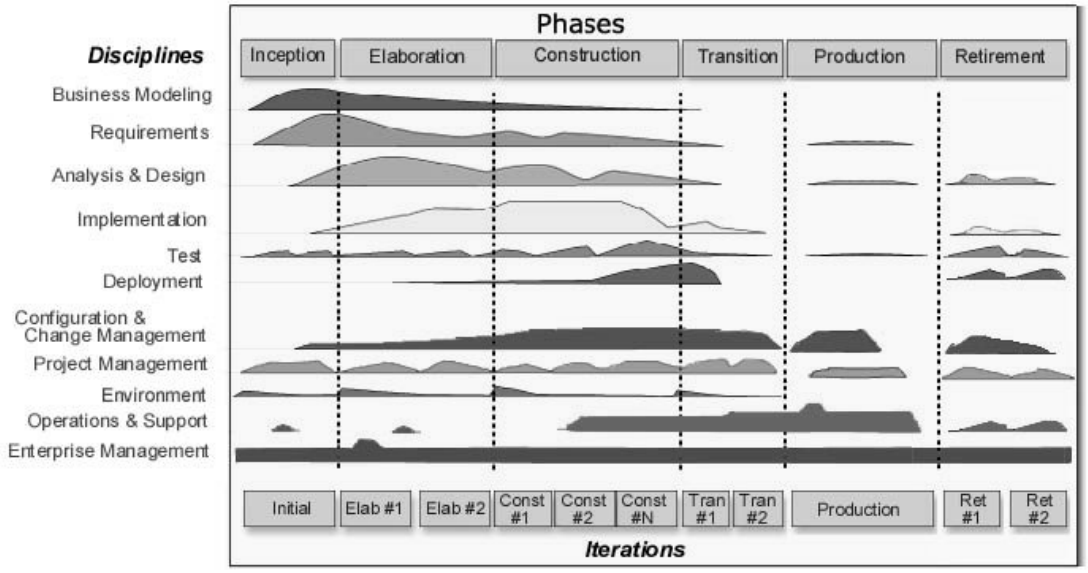

Figure 1. The Enterprise Unified Process (EUP).

Nevertheless, despite the availability of detailed guidelines for sub-activities in each discipline and for the number of iterations in each phase, neither RUP nor any other lifecycle model provides guidelines on how to achieve traceability among phases and disciplines. Also, if system properties are addressed at all, the implied concern is almost entirely on functional and operational factors, and not on other dependability factors such as safety, security, reliability, flexibility and maintainability. To exemplify, there exist no instructions on how the security issues associated with the

specific system architecture or application domain can influence the length of a certain phase, or the amount of certain sub-activities during the iterations [4]. The lack of addressing dependability factors in available life cycle models explains also why the concept of risk and risk analysis has not been an issue to take into account for these models.

Change management is closely related to the maintainability of the system development process and the result (product) of this process, the operational and applied system itself. In reality, clear and sound change management mechanisms are necessary to ensure the dependability of the task of requirements engineering. Typically, the requirements at each stage of the development process of a system undergo many changes before the development is completed. These changes may be due to changes in the prospected operation environment, but may also happen simply as a result of improved insight during the development or a desire to incorporate technological advances into the development stages (use of new methods, procedures, tools, etc.). Thus, it appears that change management mechanisms themselves depend highly on whether they utilise requirements traceability mechanisms.

2.2 The Four Pillars of the Approach

The approach for dependable requirements engineering is different from the traditional understanding of requirements engineering, as the approach advocates a perception of a requirement to be applicable for *all stages* of the system development process (or system lifecycle) and not only the high-level stages. Based on this perception, the requirements should be identified, specified, validated and verified, and finally implemented for all stages of the system development process. Referring to the disciplines in the RUP/EUP model shown in Figure 1, this means that requirements should be defined and specified in an inter-disciplinary fashion.

Furthermore, the approach aims at making a computerised system and its lifecycle analysable with regard to several *dependability factors* such as safety, security, reliability, flexibility and maintainability [3]. This means that dependability factors are integrated into the lifecycle, thus also integrated into the very definition of dependability-critical requirements. Additionally, the approach recognises the relationship between how a requirement can be met and how it can be opposed to, due to unexpected or unwanted events. Thus, the requirements expressed in this approach are also *risk-informed* [3][5]. Finally, the approach acknowledges the importance of well-defined *traceability mechanisms* to provide links between the requirements belonging to a particular stage or different stages of the lifecycle.

In order to validate and verify the requirements and their changes in a dependable manner, different analyses are needed as an integrated part of carrying out each stage of the development process. One of the most important analyses is that of thorough risk analysis and assessment with focus on one or several dependability factors, before introducing any progress or any change. There is a need for traceability of the requirements related to a specific risk analysis method or process, in accordance with the requirements of system development process and its product a risk analyst is supposed to analyse.

From the above, the four main aspects of the approach are:

1. Requirements engineering for all stages of the system development process.
2. Integrating dependability factors into the system development process, hence into very definition of the requirements.
3. Integrating risk analysis and assessment into the system development process and thus requirements engineering, so that risks are associated with the dependability-critical requirements.
4. Utilising traceability mechanisms for providing well-defined links amongst the requirements within a stage and across the stages.

The approach takes advantage of several well-known methods and techniques and ties them to the development life-cycle. The work done earlier in the TACO and MORE projects makes a solid background for further development of the approach. Integrating different types of analysis into the development process and life cycle in a structured and traceable manner is an important aspect.

2.3 The Prototype Tool Supporting the Approach

The prototype tool TRACE [15], which is being developed at IFE, is used to document the traceability information. The tool supports the approach for DRE and builds on the results from the TACO project. The results from MORE project are also fed back to further develop the TRACE tool so that it will support the traceability mechanisms identified. Figure 2 shows how system artefacts (e.g. requirements, design models) can be modelled in the TRACE tool using paragraphs.

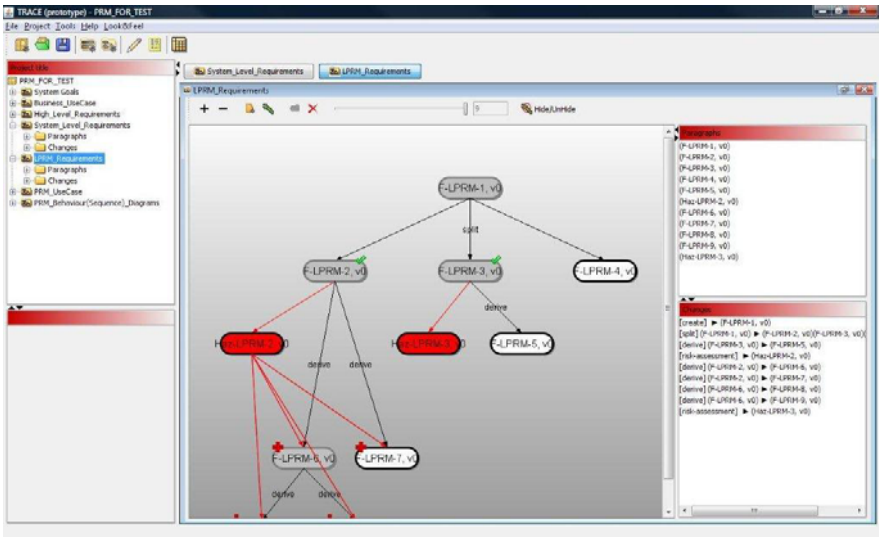

Figure 2. The TRACE tool

3. Improvement of the DRE Approach

One of the four pillars of the DRE approach is to integrate risk analysis and assessment into the requirements engineering. This aspect has been further investigated, first by studying the relationship that exists between requirements engineering and risk assessment, and then using the results from the study to further improving the DRE approach by integrating requirements engineering and risk assessment. For the study the model-based risk assessment (MBRA) approach for risk assessment has been considered.

In order to better understand and experience the role of requirements engineering during the risk assessment process, a case study was performed. Section 3.1 describes the relationships between the requirements engineering and the MBRA. Section 3.2 presents the case study and the results obtained. Section 3.3 presents the work being carried out to improve the DRE approach by integrating results from the risk assessment process into the requirements engineering process.

3.1 Relationship between Requirements Engineering and MBRA

Risk assessment can be defined as the overall process of identifying, analysing and evaluating the risks to a system. Model-based risk assessment (MBRA), which has been considered for the study, is a risk assessment process which builds on the concept of applying system modelling when specifying and describing the systems to be assessed as an integrated part of risk assessment [6][7][8][9][10][11][12]. In general, MBRA uses system models as input in order to identify and model the risks to the system.

Figure 3 presents the complementary relationships between requirements engineering, MBRA and systems modelling. Success-oriented system models (henceforth referred to as system models) are the output of the requirements engineering process and failure-oriented system models (henceforth referred to as failure models) are the output of the MBRA. The output models of one process serve as input models to the other.

During the MBRA process, the system models are analysed to identify and model the sources of vulnerabilities and threats that might lead to risks to the system. The failure models developed in this way are then used to assess risks and to suggest mitigation options. The proposed mitigation options might lead to changes in requirements and system models, thereby becoming direct input to the requirements engineering process. In this way requirements engineering and MBRA contribute to each other's inputs. We argue that for a system development process to be efficient, these two processes should be tightly integrated in a complementary manner into all the phases of the lifecycle.

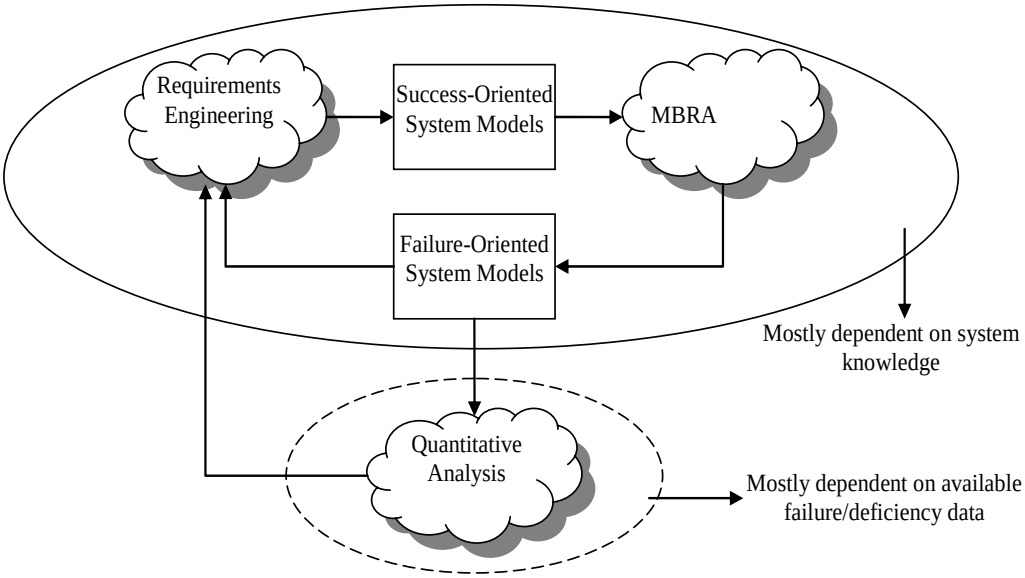

Figure 3. The relationships between requirements engineering, model-based risk assessment and systems modelling

3.1.1 The Need to Integrate

Having described the relationship between requirements engineering and MBRA, we will now look at the importance of integrating requirements engineering and MBRA. To understand clearly the role of requirements engineering during the MBRA process, the two aspects presented in sub-sections 3.1 and 3.2 are considered.

3.1.1.1 Using the "right" system models for risk assessment

For the MBRA methodology to be efficient, a basic condition is that the system models being used as input are appropriate i.e. the system models shall represent the actual needs or requirements of the system or part of the system being assessed. Requirements evolve during all the phases of the development process. Therefore they should be analysed, specified, validated and implemented in all the phases of the life cycle. As requirements evolve, so do their corresponding system models and other system artefacts. The development process of a system, especially large and complex system, generates very large volume of requirements that without transformed into system models will be very difficult to use for developing failure models of the same system. In the context of MBRA, when a system or part of the system is being assessed, it is important to know whether the system models being used for the assessment represent the actual needs or requirements of the system.

3.1.1.2 Handling the requirement changes properly

Requirements changes are inevitable during the system development process. It is likely that more than 50% of requirements change before the system is deployed [13]. As mentioned earlier, requirements changes occur during all the phases of the system life cycle. Changes to the requirements might lead to changes in other requirements, system models and system structure.

In the context of MBRA, if there is a change in requirements, it is important to make the necessary changes in their corresponding system models.

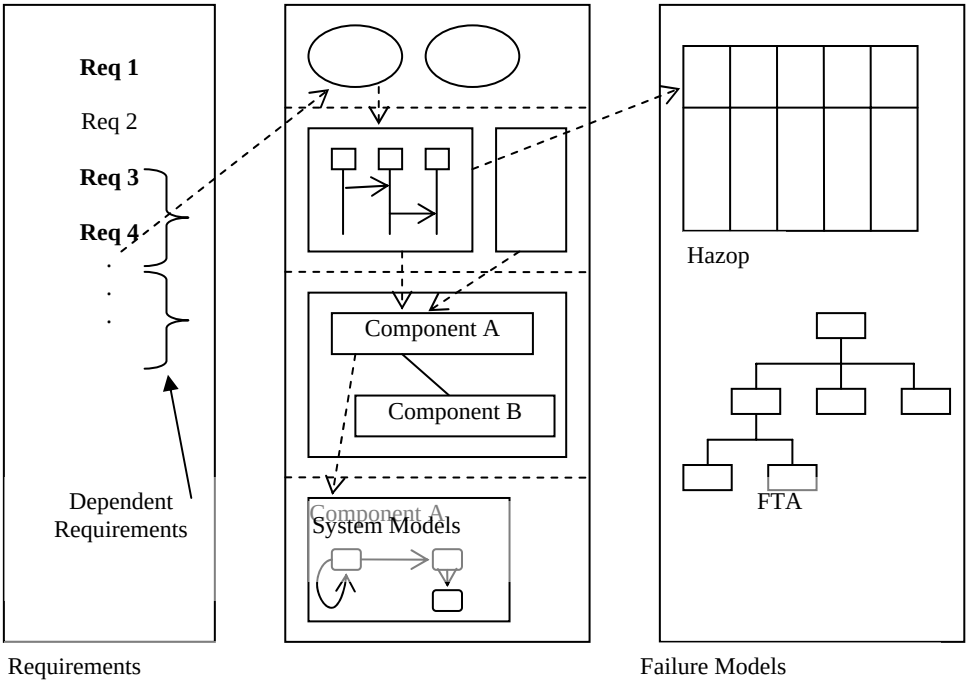

Figure 4. Requirements, system models and failure models during development process

Figure 3 presents a simple example showing different kinds of relations that exist between requirements, system models and failure models. For example, imagine that requirements 1, 3 and 4 represent the functionalities of the system that should be analysed for the risks. For a risk analyst, it is important to find the system models related to these three functionalities. Imagine also that even though requirement 2 is not a part of the system functions being analysed, it is related to requirement 3. If, during the development process, requirement 4 is modified, the analyst as well as the system development team need to consider whether requirements 2 and 3 and their respective system models are affected by this requirement change. To make the risk assessment and development processes easier and effective the requirements and the various relationships between them and the models need to be handled properly.

This is a very simple example to imply a complex problem. If the system is large and complex, then there will be lots of requirements and models that need to be handled. The above also illustrates that any MBRA approach without the support of requirements engineering might result in the usage of inadequate and incomplete system models during the risk assessment. The system models risk ignoring the system features that might, separately or in combination, become vulnerability and deficiency sources.

The following section presents the case study to demonstrate how requirements engineering can improve the MBRA approach.

3.2 Case Study: the LPRM System

One of the main activities for this reporting period is to perform case studies in order to initiate and implement the industrial take-up and utilization of the research results of this project. A case study has been performed both to:

- Illustrate the importance of requirements engineering during risk assessment process, and thereby integrating risk analysis and assessment results into the system development process and thus requirements engineering.
- Use the case study to further improve the DRE approach.
- Demonstrate and evaluate the usage of the TRACE tool [15] during a real case example.

The case study undertaken was to develop the Local Power Range Monitoring (LPRM) system, which is a part of the computer-based Power Range Monitoring (PRM) system of a nuclear reactor. The LPRM was thereafter analysed for failures using the CORAS approach [9], which is an approach based on MBRA methodology. The case study is used as a reference to identify the problems while performing risk assessment, and to observe how requirements engineering can address these problems. The idea here is to show the importance of synergy between requirements engineering and risk assessment processes.

Figure 5 presents the high level architecture of the PRM system. The PRM system is deployed in four different computer systems. The main functionalities of the LPRM are:

1. Receive 88 detector signal values from 22 probes about the state of the nuclear core.
2. Amplify each signal separately if needed.
3. Compare each amplified signal with a set of alarm levels.
4. Activate alarms when signals are not within the range of alarm levels.

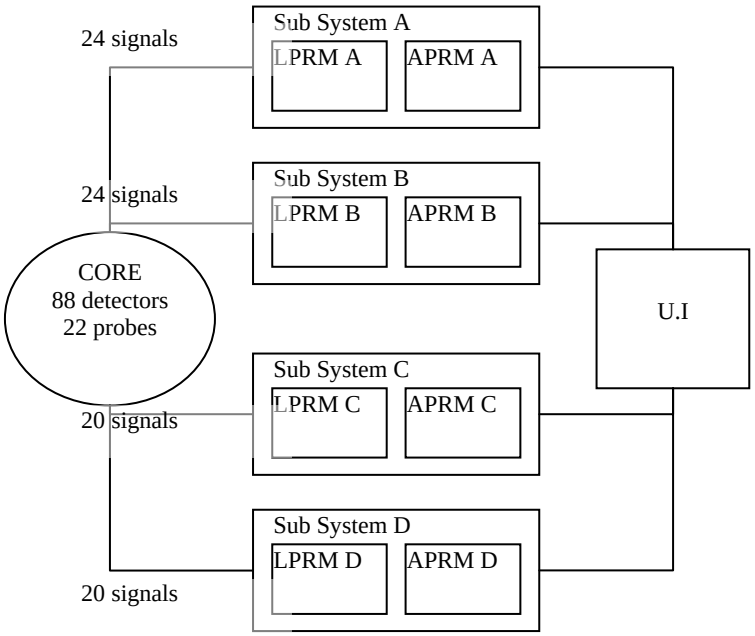

Figure 5. High level architecture of the PRM system

During the case study, the LPRM system was developed in two trials. In the first trial no specific requirements engineering process was followed while developing the LPRM system and assessing it for risks using the CORAS approach. Neither was any specific traceability mechanisms followed to specify traceability information (for example to relate depending requirements and to relate requirements with system models).

In the second trial, the LPRM system was once again modelled and assessed, but this time the DRE approach was followed to specify and maintain the traceability information. In this way the case study provides the pros and cons of performing and not performing requirements engineering while developing and more importantly while assessing the system for risks. The following sub-sections present the observations from the two trials.

3.2.1 MBRA without support of DRE

When we decided to perform a case study, we first used only a sub part of the LPRM system. Only the functionalities related to the alarm (functionalities 3 and 4 mentioned in the sub-section 3.2) were considered. The chosen system was small with very few requirements and system models. We observed that, even without following a requirements engineering process during the development process it was easy to perform the risk assessment. We did not have any problems to select the models or to manage requirements changes.

Then we chose the whole LPRM system for the case study. The number of requirements and system models that needed to be considered for risk assessment increased considerably. The system was large and complex enough to understand the role of requirements engineering. UML use case diagrams, class diagrams, sequence diagrams and state chart diagrams were mainly used to specify the system models. Hazard and operability (Hazop) and Fault tree analysis (FTA) failure modelling methods were applied on the developed system models in order to identify and model the risks. Some of the high level critical risks identified were:

- Improper synchronisation of signal and alarm level information transmitted between PRM system components (ex: LPRM, APRM, User Interface).
- Malfunction of the system clock.
- Wrong entry of signal and alarm level information by the operator.

As the system was being developed, we observed that not much effort was required to specify the system and failure models related to the requirements of the system. Then requirements changes were induced to the system. Due to the space constraints and simplicity, only a sub-set of the example is discussed in this and following sub-sections. The requirement change considered in the example is:

> *The requirement* “For each probe, the operator should set 1 high level and 1 low level alarm” *was changed to* “For each sub-system, the operator should set 1 high level and 1 low level alarm”.

We found the models related to the above requirement without much difficulty. However, we encountered problems to find the other requirements and system models

that might get affected by this particular requirement change. The selected requirements and the system models were changed accordingly. The failure models were updated by assessing the modified system models. One of the failures that were modified is:

> *The failure* "Operator assigns wrong alarms to probes" *was changed to* "operator assigns wrong alarms to Central Unit".

Figure 6 presents a failure model (FTA diagram) modified due to the requirement change. The changed failure is the event displayed in the FTA diagram.

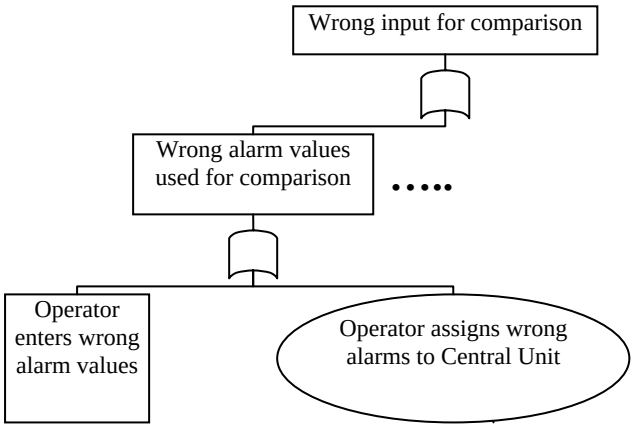

Figure 6. FTA diagram developed using CORAS approach.

3.2.2 Trial 2: MBRA with the support of DRE

In trial two the LPRM system was once again modelled, now using the DRE approach during the systems modelling activity. The traceability was documented using the mechanisms implemented by the TRACE tool. The guidelines provided by CORAS for analysing the system models were also followed.

As requirements and system models evolved during the systems modelling activity, the relationships between them were defined and maintained using the TRACE tool. Figure 7 presents a part of the requirement traceability tree of the LPRM system. A new paragraph (each paragraph represents a node in the tree) was created for each new requirement and the relationship between it and the previously specified requirements were specified using different "change type" relations (as supported by TRACE). In Figure 7, the text box below the tree represents the paragraph for the requirement "Fun-5". Each paragraph contains the requirement information such as how the requirement had originated (brainstorming meeting, from a system model, etc.), textual description of the requirement and system models related to the requirement. Each requirement was related to its respective use cases and each use case was related to its respective system models (sequence diagrams, state charts and class diagrams). In this way the relationships between requirements and system models were maintained.

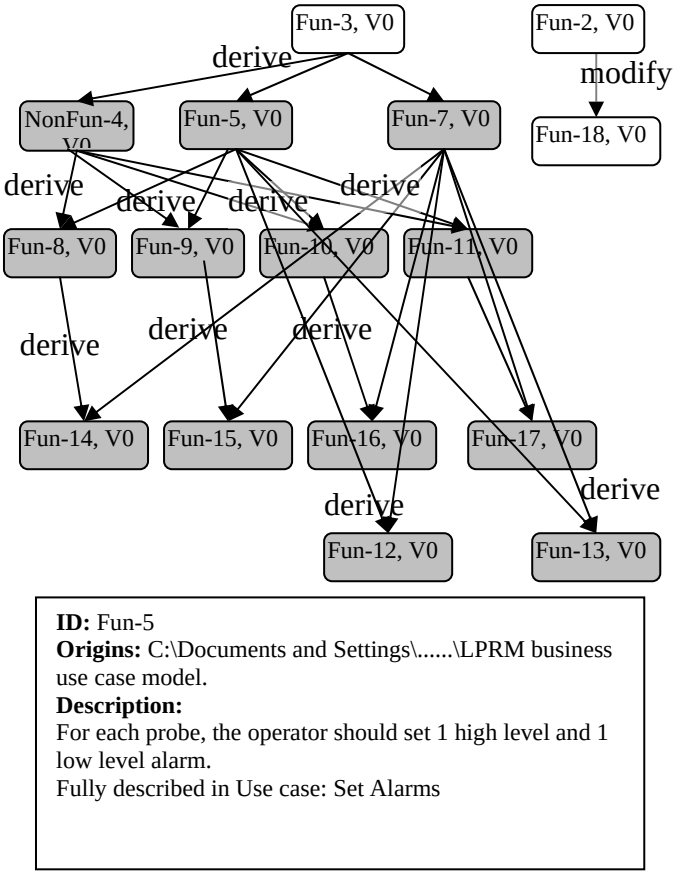

Figure 7. Traceability between requirements and models

The system models developed were very much similar to the ones developed using the MBRA approach without support of DRE. However, it was now much easier to develop the models from the requirements, also taking into account that we now already had a good knowledge of the system. The same failure modelling methods (Hazop and FTA) were applied on the system models. This time four more hidden failures were identified compared with the previous trial. The reason was that, in the previous trial we failed to consider all the system models related to a particular system model analysed (for example, how the same object or component is present in different system models). This time it was much easier to identify the related system models as the relationships between the systems artefacts were already defined during the modelling.

Finally, we induced the same requirements changes as before. By using the traceability trees we observed that it was very easy to select the requirements and models related to the changed requirements. The system models were modified accordingly and they were analysed for possible system failures. Again , more failures were identified than in the previous trial.

Let us consider the same requirement change discussed in the previous sub-section. This requirement is represented as “Fun-5” in Figure 7. The requirements related to “Fun-5” were identified using the traceability mechanisms. In Figure 7, the related requirements are highlighted. When the system models related to those requirements

were analysed, we found more sources of system deficiency than in the previous trial. Figure 8 presents one of the failure models that were modified because of the requirement change. The model presented in Figure 8 is similar to that of Figure 7 except that it has more events that will lead to a top event. We observed that the reason for the lack of identifying these was that we did not consider the requirements “Fun-12” and “Fun-13” in the previous trial. These two requirements were dependent on the requirement “Fun-5”. The new sources of failure presented in Figure 8 are the result of our analysis on the system models related to these two requirements.

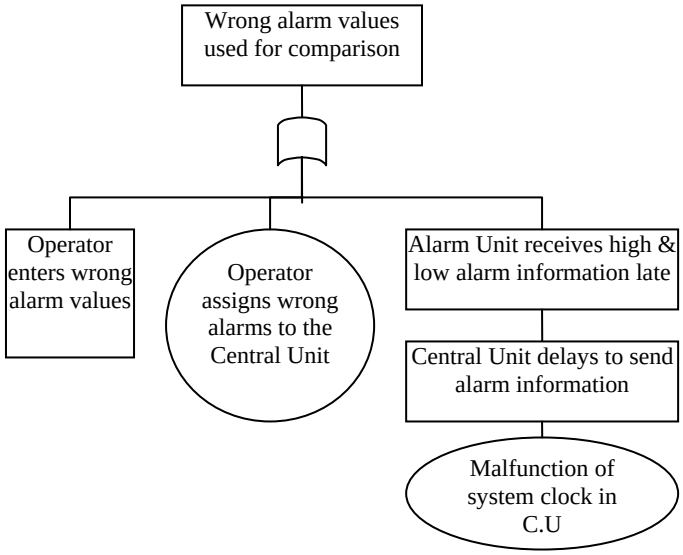

Figure 8. FTA diagram developed while using the DRE approach

3.2.3 Observations from the case study

From the results of the two trials presented we observed that dependable requirements engineering indeed plays a major role not only during the system development process, but also during an MBRA process. However, if the system is small and not particular complex, the need to follow systematic requirements engineering throughout the system development process is less.

During the case study we observed that using dependable requirements engineering explicitly will have the following advantages:

- Eases the development and maintenance of better and valid system requirements and models.
- Aids MBRA by providing appropriate input models for assessment.
- Improves MBRA by better identification and specification of the failures and thus eventually their associated risks.

From the two trials, we concluded that systematic requirements engineering through all the phases of system life cycle should be followed especially if the system being developed is complex.

3.3 Ongoing Work: Integrating Risk Assessment into DRE Approach

From the study described above, we concluded that maintaining traceability relationships between requirements and other system artefacts will improve the overall risk analysis process. We also observed the need to maintain more traceability relationships between various system artefacts and failure models, in order to efficiently handle the changes to the system.

We are presently doing research on the ways of identifying, documenting and maintaining the various traceability information needed for the efficient risk management of a system. In this regard, the main focus is on the relationship that exists between risk assessment and requirements engineering, and how traceability can have a positive effect on this relationship. Figure 9 presents some of the traceability information that will be considered during this work. Some of the traceability information includes:

- Traceability between various system artefacts (for example, between requirements and system design models).
- Traceability between system artefacts and risk assessment results.
- Traceability between informal documentation (for example email, meeting notes and phone conversations) and system artefacts. The informal documentation can be sources of artefact changes.

We also believe that improved traceability will enhance the change management process and the development of better safety cases.

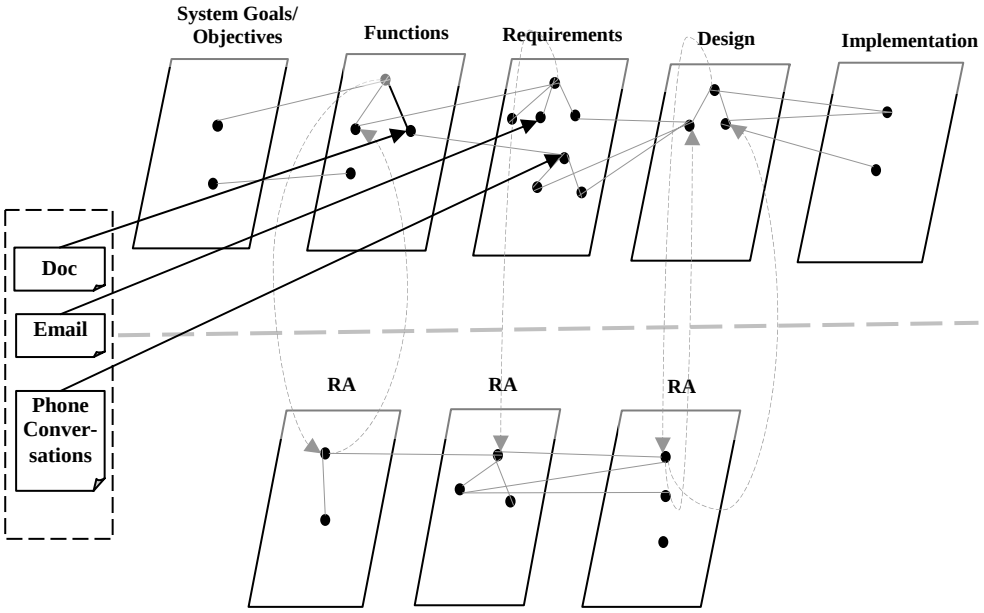

Figure 9. Different traceability information needed

Currently we are also performing another case study, where the entire PRM system is being developed. This provides better understanding, as the system being developed is much larger. The experiences from the previous and ongoing case studies will thereby help us to investigate the viability (scalability, usability, maintainability) of the concept. The system is being modelled using UML notation as well as function block diagrams. Risk assessment is performed at different phases. During the development and risk assessment of the system, we identify and document traceability information between the system artefacts and failure-oriented artefacts. While obtaining the traceability information, we try to determine the feasibility of the information, and how it can be applied in practice. The tool TRACE, is used to document the traceability information.

In the future, the plan is to use the results of our work in the areas of change management and safety case development, where we believe that traceability plays an important role.

4. Related Activities

4.1 SAFIR 2010 Programme

SAFIR2010 (SAfety of nuclear power plants – FInnish national Research programme) started in the beginning of 2007 with the main objective to develop and maintain the nuclear safety expertise and deterministic and probabilistic methods to assess safety so that new matters related to nuclear safety appearing their significance can be assessed without delay [16].

The programme is divided in eight research areas, which are:

1. Organisation and human factors
2. Automation and control room
3. Fuel and reactor physics
4. Thermal hydraulics
5. Severe accidents
6. Structural safety of reactor circuit
7. Construction safety
8. Probabilistic safety analysis (PSA)

For the MORE project the research area 2 “Automation and control room” is the most interesting. Some of the topics related to digital automation described in the SAFIR2010 framework plan are also within the scope of the MORE project. It is recognised that the end users need support in the different stages of an I&C modernisations. The support may be e.g. the ability to conduct different types of independent assessment on different life cycle phases, like review methods for evaluating requirements, and system and programme specifications.

One of the ongoing projects in the SAFIR2010 programme is about model-based safety evaluation of automation systems (MODSAFE). The assurance of automation systems and devices for use in critical applications requires the safety assessment of their software. In this project, methods based on formal model checking are developed and applied in the safety analysis of NPP safety automation. The general objectives of the project are development of methods and guidelines for model-based safety evaluation of NPP automation and evaluation of the suitability of formal model checking methods for NPP automation analysis. Also the operationalisation of model-based safety evaluation to be a part of a safety case of safety automation systems is considered in the project. The safety case development makes a connection to the ideas of the MORE project (see section 3.3).

4.2 Assessment of Smart Device Software

A project called “Assessment of smart device software” was in the SAFIR programme 2003-2006. The project proposed a safety case approach for the assessment of smart devices. Also a generic safety case compatible with the Finnish regulatory context

was outlined. The approach is a goal based method that defines claims, elaborates and apportions them to smart devices and components and then creatively identifies the arguments required to show these claims. Then, one has to assess whether the claims are satisfied in the light of available evidence. The approach was applied to an actual smart device in cases of selected safety related functions at Finnish nuclear power plants [17].

4.3 Swedish Experiences

Following [18] and [19], the Swedish experiences from Oskarshamn 1 and Ringhals 2 I&C system modernisation project, there is early in the projects a need for:

- A documented licensing strategy at the utility.
- A documented licensing strategy at the supplier.
- A documented common licensing strategy between supplier and utility (difference in culture, history and regulatory environment is needed to pay attention to).
- A real communication with the regulator.

Therefore there is a need for further development of:

- The safety demonstration plan.
- The safety case.
- Common understanding between the regulator and the utility (and its suppliers).

For the safe operation of the system after installation it is needed to develop strategies for configuration management and change control with corresponding safety assessment methods and support tools for operators and maintenance departments.

By tradition, the documentation is focused on presenting the result. For safety review of digital I&C, it is needed to document the path and processes to get to the result. It is important to have top-down and also bottom-up traceability.

Within requirements engineering, two types of V&V can be associated:

1. Requirements on the platform.
2. Requirements on the application software.

They both are coming from the application and different standards.

5. Issues of interest

There are several issues of interest within the network regarding the management of requirements in NPP modernisation projects. Based on meetings and seminars related to the MORE project, the following issues has had special interest:

- Reijo Savola has been working on requirement driven evaluation of information security [20]. Requirements are in the focus of the dependability evaluation process. Dependability can be based on iterative risk assessment analyses, and technical and architectural information. There is a need for more practical ways to carry out this iterative process.

- Dependable requirements on computerised systems at NPPs result from two different sources. On the one hand they result from project or customer needs. On the other hand they come from state of the art e.g. as represented by standards. This issue was addressed in the VeNuS project sponsored by the German ministry for economics and work (BMWA) as project 1501282, and undertaken in cooperation with the Halden Project. The VeNuS project also developed a tool prototype to support the capturing of requirements on computerised systems at NPPs from standards.

- The project - "Qualification of Integrated Tool Environments (QUITE) for the Development of Computer-Based Safety Systems in NPP" has been engaged in the topic of the qualification of computer-based I&C systems. Also this project has been sponsored by the German ministry for economics and work (BMWA) as project 1501280, and has been undertaken in cooperation with the Halden Project

- Guttorm Sindre et al has proposed and developed the concept of misuse cases [21]. Misuse cases have been proposed and developed as a technique for early elicitation and specification of security requirements. This approach could possibly be extended to other dependability issues.

- Tamàs Bartha has been working with the starting point that the need for the integration of automated formal verification in the development process in order to increase software reliability is constantly increasing [22]. One suggestion is to use a coloured petri net based approach to the formal verification of function block diagram based specifications. The approach suggested is non-model based; only the control logic of the safety function is modelled and verified.

- Glen Dobson has presented some interesting ideas about ontology-based requirements engineering in [23]. An ontology is generally based upon some logical formalism, and has the benefits for requirements of explicitly modelling domain knowledge in a machine interpretable way, e.g. allowing requirements to be traced and checked for consistency by an inference engine, and software specifications to be derived. One suggestion is to revisit the ontology-based requirements engineering in the light of the semantic web.

6. Acknowledgements

The authors of this report would like to thank the following for their valuable contributions to the MORE project and the contents of this report. However, the authors are solely to blame for the conclusions and possible misunderstandings.

Martin Kropik	Faculty of Nuclear Sciences and Physical Engineering CTU in Prague	Czech Republic
Jozef Molnar	Nuclear Research Institute Rez plc	Czech Republic
Morten Lind	Oersted - DTU Automation Technical University of Denmark	Denmark
Harri Heimbürger	STUK	Finland
Kaj Juslin	VTT Technical Research Centre of Finland	Finland
Reijo Savola	VTT Technical Research Centre of Finland	Finland
Olli Ventä	VTT Technical Research Centre of Finland	Finland
Günter Glöe	TÜV Nord SysTec GmbH & Co. KG	Germany
Tobias Hadler	TÜV Nord SysTec GmbH & Co. KG	Germany
Arndt Lindner	ISTec GmbH	Germany
Horst Miedl	ISTec GmbH	Germany
Tamás Bartha	MTA SZTAKI Computer and Automation Research Institute	Hungary
Torgrim Lauritsen	NTNU	Norway
Andreas L. Opdahl	Universitetet i Bergen	Norway
Guttorm Sindre	NTNU	Norway
Patrick Isaksson	Vattenfall Power Consultant AB	Sweden
Bo Liwång	SKI	Sweden
Glen Dobson	Lancaster University Computing Department	United Kingdom
Øivind Berg	Institutt for energiteknikk / OECD Halden Reactor Project	Norway
Rossella Bisio	Institutt for energiteknikk / OECD Halden Reactor Project	Norway
Bjørn Axel Gran	Institutt for energiteknikk / OECD Halden Reactor Project	Norway
Atoosa P-J. Thunem	Institutt for energiteknikk / OECD Halden Reactor Project	Norway
Harald P-J. Thunem	Institutt for energiteknikk / OECD Halden Reactor Project	Norway

7. References

[1] T. Sivertsen et al., “Traceability and communication of requirements in digital I&C systems development”, TACO final report, NKS-115, October 2005.

[2] A. P-J Thunem et al., “Management of Requirements in NPP Modernisation Projects”, MORE project report 2005 (NKS_R_2005_47, 2005-2008, NKS-133, ISBN 87-7893-195-9) in January 2006.

[3] A. P-J Thunem, “Modelling of Knowledge Intensive Computerised Systems Based on Capability-Oriented Agent Theory (COAT)”, International IEEE Conference on Integration of Knowledge Intensive Multi-Agent Systems, IEEE-KIMAS’03 (58-63), September 2003, Cambridge (MA), USA.

[4] A. P-J Thunem, “A Framework for Dependable Development Process of Complex Computerised Systems”, the joint European Safety and Reliability 2004 (ESREL04) and the 7th International Probabilistic Safety Assessment and Management (PSAM7) conference (902-907), June 2004, Berlin, Germany.

[5] A. P-J Thunem, “Dependable Requirements Engineering and Change Management of Security-Critical ICT-Driven Systems”, PSAM8 international conference, (ASME Press, Topic Area: Security, paper “PSAM-0101”), May 2006, New Orleans, USA.

[6] A. Jalashgar, 1998. “Identification of Hidden Failures in Process Control Systems Based on the HMG Method”. *International Journal of Intelligent Systems*, February-March 1998 13: 159-179

[7] A.Jalashgar, 1999. “Goal-Oriented Systems Modelling: Justification of the Approach and Overview of the Methods”. *Reliability Engineering and System Safety Journal*, May 1999 64 (2): 271-278.

[8] A. P-J. Thunem, 2001. “A Cognitive and Formal Terminology for Descriptive Parameters in Concurrent Real-Time Distributed Software Systems”. In D.Ruan, J.Kacprzyk, M. Fedrizzi (eds), *Soft Computing for Risk Evaluation and Management*, ISBN 3790814067: Chapter 2, Part 3, pages 229-248. Heidelberg: Physica-Verlag.

[9] B. A. Gran et al. 2003. *The CORAS methodology for model-based risk assessment*. IST-2000-25031 CORAS project public report D2.4.

[10] Garrett, C.J., Guarro, S.B., Apostolakis, G.E. (1995): “The dynamic flow graph methodology for assessing the dependability of embedded software systems”, IEEE Trans. on Systems, Man, and Cybernetics, vol. 25, no. 5, pp 824-840.

[11] Guarro, S. B., Okrent, D. (1984): “The logic flowgraph: A new approach to process failure modeling and diagnosis for disturbance analysis applications”, Nuclear Technology, p 67

[12] Kim, I. S., Modarres, M. (1987): “Application of Goal Tree-Success Tree Model as The Knowledge-Base of Operator Advisory System”, Nuclear Engineering & Design Journal, No 04, pp 67-81.

[13] G. Kotonya, I. Sommerville. “Requirements engineering: Processes and Techniques”, John Wiley & sons,1997.

[14] P. Kruchten. *The Rational Unified Process - An Introduction*. Addison-Wesley, 1999.

[15] A. P-J, Thunem, H. P-J Thunem, “TRACE: Traceability of Requirements for Analysable Computerised Environments”, IAEA Technical Meeting on Implementing

and Licensing Digital I&C Systems and Equipment in Nuclear Power Plants, November 2005, Espoo, Finland.

[16] SAFIR2010 Working Group, National Nuclear Power Plant Safety Research 2007-2010. Proposal for SAFIR2010 Framework Plan, September 2006.

[17] VTT RESEARCH NOTES 2363 SAFIR. The Finnish Research Programme on Nuclear Power Plant Safety 2003– 2006. Final Report. Edited by Hanna Räty & Eija Karita Puska

[18] B. Liwång, 2005. “Licensing of Software-based Safety Systems, Some comments from the Regulator”, IAEA Technical Meeting on Implementing and Licensing Digital I&C Systems and Equipment in Nuclear Power Plants, November 2005, Espoo, Finland.

[19] B. Liwång 2006. “Software-based Safety Systems, Some comments from a Regulator on Documentation and Traceability”, International Seminar on Dependable Requirements Engineering of Computerised Systems at NPPs, November 27-29, 2006, Halden, Norway.

[20] R. Savola. “Towards Requirements Driven Evaluation of Information Security”, International seminar on Dependable Requirements Engineering of Computerised Systems at Nuclear Power Plants, Halden, Norway, November 27-29, 2006

[21] Guttorm Sindre, Andreas L. Opdahl: "Misuse Cases - Use Cases that Capture Security Threats", International seminar on Dependable Requirements Engineering of Computerised Systems at Nuclear Power Plants, Halden, Norway, November 27-29, 2006

[22] T. Bartha. “Formal Modelling and Verification of Specifications for the I&C System Software in NPPs”. International seminar on Dependable Requirements Engineering of Computerised Systems at Nuclear Power Plants, Halden, Norway, November 27-29, 2006

[23] G. Dobson, P Sawyer. “Revisiting Ontology-Based Requirements Engineering in the age of the Semantic Web”. International seminar on Dependable Requirements Engineering of Computerised Systems at Nuclear Power Plants, Halden, Norway, November 27-29, 2006

8. Appendix A: Project Organisation and Activities

8.1 Project Organisation

The project is led by Rune Fredriksen (IFE), and comprises the following organisations and persons:

Organization	Address	Project participants
IFE	Institute for energy technology P.O. Box 173 NO-1751 Halden Norway	Rune Fredriksen +47 69 21 24 30 (rune.fredriksen@hrp.no) Vikash Katta +47 69 21 22 65 (vikash.katta@hrp.no) Christian Raspotnig +47 69 21 22 96 (christian.raspotnig@hrp.no)
VTT	Technical Research Centre of Finland P.O. Box 1000 FIN-02044 VTT Finland	Janne Valkonen +358 20 722 6469 (janne.valkonen@vtt.fi) Olli Ventä +358 20 722 6556 (olli.venta@vtt.fi)

The activity organisation is subject for extension by involvement of additional industrial partners. In addition, the network represented by the activity organisation is extended though the arrangement of the industrial seminars.

The project leader is responsible for organising the work within the project and for directing it towards its objectives. This includes:

- Project planning and tracking
- Establishment and maintenance of the project archive
- Establishment of good communication and cooperation within the project
- Reporting to NKS
- Coordination of activities, in particular the production of the project deliverables
- Follow up of meetings and decisions
- Securing of proper quality control, including review and approval of documents included in the project archive
- Reporting of deviations and implementation of agreed corrections

All the individual participants represent important parts of the technical competence within the project, and are responsible for contributing to the activities in such a way that the project can meet its objectives.

The funds received from NKS for the work in 2007 are estimated to cover 50% of the overall costs. The remaining 50% will be covered through the individual costs and efforts of each participating organisation. Each organisation will be responsible for ensuring that their contribution is sufficient to satisfy their fraction of the overall budget. In order to facilitate roughly the same amount of effort from IFE and VTT to the technical part of the project, an estimated 20% of the funds will be allocated for project coordination (IFE). The remaining 80% will be split equally between IFE and VTT. This gives the following split of funds:

IFE	60% (= 20% + 40%)
VTT	40%

Possible common costs related to the arrangement of project meetings and seminars will be split equally between IFE and VTT. The approximate division of costs between work, travel, and equipment is given in the Proposal Summary 2007.

8.2 Project Activities

The activity will be carried out through a three-year period, as a strategic follow-up activity to the TACO project. The activity started on July 1, 2005, and will terminate on June 30, 2008. The project will deliver two industrial seminars, closely related to the background, objectives and activities of the project, at least two organised visits to selected NPPs undertaking modernisation activities, three annual project reports, and one final report.

The activities in 2007 have been with focus on the following:

- Continuous improvement of the results from the project, on the basis of the received feedback and gained knowledge.
- Identification and application of a couple of case studies from NPP projects and activities in order to initiate and implement the industrial take-up and utilisation of the research results in real modernisation projects.
- Continuing to compile experiences on the problem of handling large amounts of information in relation to Nordic modernisation projects, amongst others, through organised visits to selected plants.

Extending the industrial network, also through disseminations and presentation of the results in Nordic and NKS related events such as seminars and workshops, and through the results from the international seminar on Dependable Requirements Engineering by IFE and with NKS co-sponsorship, in Halden, November 27-29, 2006.

The activities in 2008 will carry out the implementation plan in cooperation with an extended network of industrial partners. The network established through the activity

organisation and the TACO industrial seminars will be further extended and consolidated through the arrangement of industrial and international seminars.

The experiences and lessons learned from the research will be reported in the annual project reports, and summarised in a final report to be produced in the first half of 2008.

The remaining overall documentation schedule is as follows:

- January 2008: Activity report for 2007 (this report)
- June 30, 2008: Final report

The discussions from the project meetings and industrial and international seminars, and the progress of the project will be reported by means of detailed minutes.

9. Appendix B: MORE dissemination 2007

The following is a list of dissemination activities in the MORE project in 2007. The activities have also been funded from other sources than MORE.

V. Katta, and A. P-J. Thunem, “Improving Model-Based Risk Assessment methods by Integrating the Results of Requirements Engineering into the System Models”, presented at ESREL 2007, in Risk, Reliability and Societal Safety, Aven & Vinnem (eds), Taylor & Francis Group, pp 2357-2363, 2007.

J. Valkonen, “Requirements Dependability and Traceability in Automation Systems”, presented at the Enlarged Halden Programme Group Meeting (EHPG) 2007, in Halden Report HWR-853, 2007.

A. P-J Thunem, H. P-J Thunem, “Dependable Requirements Engineering: The Approach behind TRACE”, Halden Report HWR-846, 2007.

V. Katta, C. Raspotnig, “Towards Efficient Traceability of Safety Relevant Systems”, IEEE International Symposium on Software Reliability Engineering, 18 (ISSRE 2007), Trollhättan, Sweden.

Bibliographic Data Sheet **NKS-163**

Title	MORE: Management of Requirements in NPP Modernisation Projects, Project Report 2007
Author(s)	Rune Fredriksen[1)], Vikash Katta[1)] and Christian Raspotnig[1)] Janne Valkonen[2)]
Affiliation(s)	[1)]Institutt for energiteknikk (IFE), Norway [2)]Technical Research Centre of Finland (VTT)
ISBN	978-87-7893-228-0
Date	March 2008
Project	NKS-R / MORE
No. of pages	29
No. of tables	0
No. of illustrations	9
No. of references	23
Abstract	This report documents the work and related activities of the MORE (Management of Requirements in NPP Modernisation Projects, NKS_R_2005_47) project in the period January 1 – December 31 in 2007. The focus of this report is on improvements of the former project results, to identify and apply a couple of case studies from NPP projects, and activities in order to initiate and implement the industrial take-up and utilisation of the research results in real modernisation projects. The report also provides a brief description of the extended industrial network and disseminations of the results in Nordic and NKS related events such as seminars and workshops.
Key words	change management, requirements engineering, software engineering, software requirements, traceability, verification and validation

Available on request from the NKS Secretariat, P.O.Box 49, DK-4000 Roskilde, Denmark.
Phone (+45) 4677 4045, fax (+45) 4677 4046, e-mail nks@nks.org, www.nks.org