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

NKS-178
ISBN 978-87-7893-244-0

MORE: Management of Requirements in NPP Modernisation Projects, Final Report

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

Janne Valkonen
Technical Research Centre of Finland (VTT), Finland

September 2008

Abstract

This report documents the work and related activities of the MORE (Management of Requirements in NPP Modernisation Projects) (NKS-R project number NKS_R_2005_47) project. This report also provides a summary of the project activities and deliverables, and discusses possible application areas. The project has aimed at the industrial utilisation of the results from the TACO: (Traceability and Communication of Requirements in Digital I&C Systems Development) (NKS-R project number NKS_R_2002_16, completed June, 2005) project, and practical application of improved approaches and methods for requirements engineering and change management. Finally, the report 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-178
ISBN 978-87-7893-244-0

Electronic report, September 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
- Final Report -

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

Final report

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 project number NKS_R_2005_47) project. This report also provides a summary of the project activities and deliverables, and discusses possible application areas. The project has aimed at the industrial utilisation of the results from the TACO: (Traceability and Communication of Requirements in Digital I&C Systems Development) (NKS-R project number NKS_R_2002_16, completed June, 2005) project, and practical application of improved approaches and methods for requirements engineering and change management. Finally, the report 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	23.06.2008
	Reviewed by:	Bjørn Axel Gran	30.06.2008
	Approved by:	NKS	

Foreword

This document constitutes the final report for the MORE project: Management of Requirements in NPP Modernisation Projects (NKS-R project number NKS_R_2005_47). The report provides a summary of the project activities and deliverables, and discusses possible application areas. The project has aimed at the industrial utilisation of the results from the TACO project: Traceability and Communication of Requirements in Digital I&C Systems Development (NKS-R project number NKS_R_2002_16, completed June, 2005), and practical application of improved approaches and methods for requirements engineering and change management.

We would like to express our gratitude to all the people involved in discussing issues related to the project and participating in the industrial network established during the projects.

Halden, June 2008

Rune Fredriksen

Table of Contents

Applied Abbreviations

DRE	Dependable Requirements Engineering
EHPG	Enlarged Halden Programme Group
EUP	Enterprise Unified Process
I&C	Instrumentation & Control
ICT	Information and Communication Technologies
IFE	Institutt for energiteknikk (Institute for energy technology)
KAERI	Korea Atomic Energy Research Institute
LPRM	Local Power Range Monitoring
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)
TRACE	Traceability of Requirements for Analysable Computerised Environments (tool)
V&V	Verification & Validation
VTT	Technical Research Centre of Finland

Summary

The title of the reported project is “Management of Requirements in NPP Modernisation Projects”, abbreviated MORE. The NKS project number is NKS_R_2005_47). The project has aimed 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, 2005), and practical application of improved approaches and methods for requirements engineering and change management. This document is the final report from the MORE project.

The overall objective of the project MORE has been to improve the means for managing the large amounts of evolving requirements in Nordic NPP modernisation projects. According to this objective, the activity has facilitated the industrial utilisation of the research results from the TACO project, 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, 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*, a complementary set of basic requirement *change types*, and generic mechanisms for requirement *categorisation*.

Compiled experiences has pointed to that there has been a problem of handling large amounts of information in relation to Nordic modernisation projects. On this basis, the MORE project was started. The MORE project has aimed 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 has therefore been an important prerequisite for the success of the MORE project.

In 2005, particular emphasis was put on utilising a prototype of the tool TRACE (*Traceability of Requirements for Analysable Computerised Environments* [22]) intended to support an adopted approach to dependable requirements engineering, suitable for modelling and handling large amounts of requirements related to all stages of the systems development process and not only those traditionally including requirements at high-level stages.

In 2006, the work concentrated on further research for adopting an approach for dependable requirements engineering and its supporting tool. The majority of the efforts in 2006 was spent on making the researchers, developers, utilities and licensees more aware of the importance of the area of requirements engineering, and

in that respect organising an international seminar on dependable requirements engineering.

In 2007, the work was concentrated on improvement of the former reported results from the project. The improvements were based on received feedback and gained knowledge. Our goal was 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 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.

In 2008, we have focused on summarising our experiences gathered through the MORE project on the problem of handling large amounts of information in relation to Nordic modernisation projects. The results and conclusions are presented in the final MORE report and disseminated at e.g. the EHPG 2008.

The main results from the MORE project are:

- Increased knowledge on handling of requirements during modernisation projects.
- Input and recommendations to the implementation of the TACO traceability model in a prototype tool (TRACE) on issues regarding the handling of requirements.
- Continuation of a Nordic network of experts within the area of dependable requirements engineering issues.
- Expansion of this network to also include researchers from Europe – and contacts with Korea and Japan.

One additional result was an application for a workshop: The 1st Workshop on Dependable Software Engineering (WDSE) for ISSRE 2008 in Seattle, USA. This workshop was accepted at the end of June 2008.

1. Introduction

Experiences from modernisation projects in the nineties at NPPs, particularly in Sweden and Finland, indicated the importance of adequate structure and modularisation of requirements. The experiences also showed that 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. Another particular issue identified was 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. From the experiences it was formed the hypothesis that 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.

From this background, the MORE project was started with the overall objective to improve the means for managing the large amounts of evolving requirements in Nordic NPP modernisation projects. In accordance to this objective, the activity should facilitate the industrial utilisation of the research results from the TACO project, and practical application of improved approaches and methods for requirements engineering and change management. 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*, a complementary set of basic requirement *change types*, and generic mechanisms for requirement *categorisation* [17][18].

The purpose of this present report is to document the work and related activities carried out in the whole lifespan of the MORE project and the further research and related activities to the project MORE.

Chapter 2 provides a summary of the activities and results provided in the MORE project. Chapter 3 describes the approach for dependable requirements engineering adopted in the MORE project. Chapter 4 provides a basic introduction to the prototype implementation in the tool TRACE. In Chapter 5 we provide a short discussion on some issues regarding the integration of requirements engineering and risk assessment. Chapter 6 describes some related activities within the Nordic area which we are familiar with. Chapter 7 contains a summary of the conclusions from the MORE project. Chapter 8 acknowledges the contributors to MORE. Chapter 7 presents the references used to compose this report.

Appendix A features the project activity plan and organisation. Appendix B includes the minutes from the International Seminar on Dependable Requirements Engineering of Computerised Systems at NPPs.

2. Activities and Results

The MORE project has been carried out through a combination work by each partner, project meetings, coordinated preparation of annual reports, seminars, and other dissemination activities. Each project meeting has focused on a limited set of issues, where the participating organisations have been asked to prepare presentations on their experiences and viewpoints. Particular emphasis has been given on utilising concrete experiences from safety-critical applications. The discussions from the project meetings and seminars, as well as the progress of the project, have been carefully reported by means of detailed minutes.

The overall documentation schedule for the MORE project has been as follows:

- April 2006: Documentation of the work for 2005 collected and sent in a suitable form to NKS (completed).
- February 2007: Documentation of the work for 2006 collected and sent in a suitable form to NKS – including minutes from the seminar on dependable requirements engineering (completed).
- January 2008: Documentation of the work for 2007 collected and sent in a suitable form to NKS (completed).
- June 2008: Final MORE project report (the present report – completed).

The next subchapters are organised such that we first present the annual work in the MORE project, and then summarise the dissemination activities of the project.

2.1 Utilising a Prototype (2005)

Particular emphasis for the MORE project in 2005 was put on utilising a prototype of a tool named TRACE (Traceability of Requirements for Analysable Computerised Environments) intended to support an adopted approach to dependable requirements engineering, suitable for modelling and handling large amounts of requirements related to all stages of the systems development process and not only those traditionally including requirements at high-level stages.

As the aim was to improve and maturate the results from the project TACO, the efforts during the period July 1 – December 31 in 2005 was put on the following:

- Adopting an approach for dependable requirements engineering and its supporting tool. The tool made use of the main concepts of the traceability model proposed in the project TACO, but also responded to other aspects and includes other features.
- Disseminating the background and objectives of the project MORE, in order to establish collaboration with NPP utilities involved in modernisation activities. Such collaboration was a prerequisite for the success of the project.

The activities related to the project MORE included a presentation in an NKS initiated seminar on decommissioning projects in Nordic countries (Roskilde, Denmark, September 13-15, 2005), a paper presentation [18] and demonstration of the prototype during SAFECOMP 2005 conference (Fredrikstad, Norway, September 28-30, 2005), a paper presentation [19] and demonstration during the EHPG 2005 (Lillehammer, Norway, October 17-21, 2005), a project meeting (October 18, 2005), and a paper presentation [22] and demonstration during an IAEA special meeting (Espoo, Finland, November 22-24, 2005).

2.2 Adopting an Approach (2006)

The work in this period concentrated on further research for adopting an approach for dependable requirements engineering and its supporting tool. The very focus of the approach was assessed to be valid and it was concluded that the approach provides efficient change management related to modernisation activities. The majority of the efforts in 2006 was spent on making researchers, developers, utilities and licensees more aware of the importance of the area of requirements engineering, and in that respect organising an international seminar on dependable requirements engineering. This seminar was defined as a deliverable in the activity plan for 2006 and became also the most important deliverable for 2006. The seminar was a success by that it was a door opener for more initiatives within the topic, proposed by several participants. The seminar was held in Halden, Norway, November 27-29 and it was hosted by the Institute for Energy Technology (IFE) and chaired by the NKS-R Programme Management. The work continued to have focus and using efforts on dissemination of the background and objectives of the MORE project within the nuclear community and towards NPP utilities that do carry out modernisation projects.

2.3 Further Improvement (2007)

In 2007 the work concentrated on improving the former reported results from the project. The improvements were based on received feedback and gained knowledge. Our goal was 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. This was also the conclusion from the MORE project meeting with Fortum/Loviisa NPP in 2005. However, identifying a real case and undertaking a case study requires also resources, e.g. in terms of availability to experts, from the case owners. This proved to be a major problem, and is also a lesson learned from dealing with modernisation projects.

We continued to compile experiences on the problem of handling large amounts of information in relation to Nordic modernisation projects, amongst others, reviewing the experiences from previous visits to selected plants. We also extended the industrial network through disseminations and presentations of the results in Nordic NKS related events, and at the EHPG 2007, as well as the ESREL and ISSRE conferences.

2.4 Evaluation and Conclusions (2008)

In 2008 our focus was to summarise our experiences on the problem of handling large amounts of information in relation to Nordic modernisation projects and trying to establish some conclusions from the MORE project. We arranged a meeting on TRACE, and a MORE project meeting was arranged at Loen at the same time as the EHPG 2008. In addition we had some discussions about how to maintain the industrial network established through the TACO and MORE projects, and continued the dissemination of the results at the EHPG 2008. The summary of results and conclusion is presented in the final MORE report (this report).

2.5 Dissemination

The MORE project has been presented at a number of meetings in the Nordic countries. The purpose of the different dissemination activities was twofold. One purpose was to present the MORE project and its deliverables to the industry and representatives from utilities, licensing and the academia. The other purpose was, and to identify opportunities for industrial utilization. The different activities are briefly discussed below.

2.5.1 NKS Initiated Seminar on Decommissioning (2005)

The seminar was arranged by NKS and in collaboration with Dansk Dekommissionering in Roskilde, Denmark, September 13-15, 2005. The focus was on decommissioning activities in Nordic countries, and the aim was to allow as many as possible presentations of 5-10 minutes duration. The last day of the seminar was reserved for group-work based on a pre-prepared set of questions and issues to discuss. Our focus was on traceability and communication of life cycle requirements for systems at nuclear facilities [2].

2.5.2 SAFECOMP (2005)

SAFECOMP (The International Conference on Computer Safety, Reliability and Security) was established in 1979 by the European Workshop on Industrial Computer Systems, Technical Committee 7 on Reliability, Safety and Security, EWICS TC7. SAFECOMP has contributed to the progress of the state-of-the-art in dependable applications of computer systems. It is an annual event covering the state-of-the-art, experience and new trends in the areas of computer safety, reliability and security regarding dependable applications of computer systems. SAFECOMP 2005 took place in Fredrikstad, Norway, September 28-30, 2005, and focused on dependability of critical computer applications. Due to the increasing awareness and importance of security issues of critical computer-based systems, SAFECOMP 2005 emphasised work in this area. Nowadays practical experience points out the need for multidisciplinary approaches to deal with the nature of critical complex settings. SAFECOMP 2005, therefore, was open to multidisciplinary work enhancing understanding across disciplines. From the MORE project the paper [18] was presented and a demonstration of TRACE was provided.

2.5.3 EHPG 2005

The Enlarged Halden Programme Group meeting (EHPG) in 2005, at Lillehammer, was the 32nd in the series of EHPG meetings. It was arranged in order to promote dissemination of the results of the Halden Project's research activities, and further to identify and discuss the research priorities of the member organisations of the Halden Project.

The meeting reviewed activities in all the main areas of the Halden Project's work. Reports on the Halden Project's joint programme results and on results from participant sponsored programmes were presented, as well as papers on related work performed at the participants' own establishments. Invited papers reviewing topics of interest within the scope of the Halden Project's activities were equally presented. From the MORE project the paper [19] was presented and a demonstration of TRACE was provided.

2.5.4 MORE Project Meeting (2005)

The meeting, October 18, 2005, was a combined project meeting and a meeting with Fortum. The participants were: Samuli Savolainen (Fortum/Loviisa NPP), Olli Ventä (VTT), Janne Valkonen (VTT), Jan Porsmyr (IFE), Atoosa P-J Thunem (IFE), Harald P-J Thunem (IFE), and Rune Fredriksen (IFE). Atoosa P-J Thunem presented an introduction to the TACO and MORE projects and the traceability model developed in the TACO project. She explained that this model would be further improved in the MORE project, along with the development of the tool TRACE supporting an approach for dependable requirements engineering. She stressed the need for one or several test cases in order for the MORE project and its results to become more applicable towards modernisation projects and other activities (e.g., maintenance improvement activities) at NPPs. Samuli Savolainen suggested that he could ask people at Loviisa to become involved. The best person might be someone from the QA department or archive. The plan was therefore as follows:

1. A group visit to Loviisa to see a small case study
2. Obtain access to some documentation of the case study (An issue might be that the documentation is in Finnish)

It was decided that Atoosa P-J Thunem should send an email to Samuli Savolainen about the intention behind a contact with Loviisa, including a brief introduction to the project (and remembering to point out that the work will be performed by the members of the project MORE, and will not cost anything for Loviisa beyond providing the test case). It should be mentioned that the project members would like to come to Loviisa for a visit in December 2005. It was decided that Samuli Savolainen should forward the email directly to Markku Tiitinen, Mikko Pihlatie and Arvo Vuorenmaa. Another conclusion from the meeting was that the MORE team would also like to get input on how people at Loviisa work with traceability issues and how these challenges should be dealt with in the future.

However, as already stated in the summary of 2006 identifying a real case and undertaking a case study requires resources, e.g. in terms of availability to experts, from the case owners. This has proven to be a major problem, and is a lessoned learned from dealing with modernisation projects.

2.5.5 IAEA Technical Meeting: Implementing and Licensing Digital I&C Systems and Equipment in NPPs (2005)

The purpose of the IAEA meeting in Espoo, Finland, November 22-24, 2005, was to provide an international forum for presentation and discussion of experience in implementing and licensing digital I&C systems and equipment in nuclear power plants. The meeting was intended for I&C experts from power utilities, vendor companies, licensing bodies, research organisations and academic institutions. The meeting provided both experience from earlier projects and descriptions of new and planned I&C projects. The meeting was hosted by VTT and was attended by 85 participants from 24 countries presenting 27 papers. During the meeting, new innovative methods and tools for test and validation of implementation and operation of digital systems were also presented. In addition, a technical document (TECDOC) initiated in August 2005 was further discussed during the meeting. The focus of the TECDOC was on implementing and licensing digital I&C systems and equipment in nuclear power plants. This TECDOC is to be issued in 2008, and experts from both VTT and IFE have taken part in the work of developing and finalising this report.

2.5.6 International Seminar on Dependable Requirements Engineering of Computerised Systems at NPPs (2006)

The seminar was hosted by IFE and was held in Halden, Norway, November 27-29. The seminar was chaired by the NKS-R Programme Management. IFE covered all direct costs associated with the seminar, and the majority of indirect costs, being mainly the technical work done prior to the seminar. The seminar had 25 participants, representing both Nordic and International organisations. A complete record of the meeting was presented in the 2006 project report of the MORE project. The program and participation list is in addition provided in this report as Appendix B.

There are several issues of interest within the network regarding the management of requirements in NPP modernisation projects. The following issues were identified to have a special interest:

- Reijo Savola has been working on requirement driven evaluation of information security [15]. Requirements are in the focus in the dependability evaluation process. Dependability can be based on iterative risk assessment analysis, 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 and 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 Vorgehen zum effizienten Nachweis der Benutzbarkeit und Sicherheit rechner-gestützter Leittechniksysteme (Procedure for the Efficient Demonstration of Usability and Safety of Computerised Control Systems) (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 included also development of 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 [16]. 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 from 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 [1]. 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 [3]. Ontology can be defined as a formal representation of a set of concepts within a domain and the relationships between those concepts. Ontology has therefore 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.

2.5.7 MORE Project Meeting and EHPG (2007)

The Enlarged Halden Programme Group meeting (EHPG) in 2007, at Storefjell, was the 33rd in the series of EHPG meetings. It was arranged in order to promote dissemination of the results of the Halden Project's research activities, and further to identify and discuss the research priorities of the member organisations of the Halden Project.

The meeting reviewed activities in all the main areas of the Halden Project's work. Reports on the Halden Project's joint programme results and on results from participant sponsored programmes were presented, as well as papers on related work performed at the participants' own establishments. Invited papers reviewing topics of interest within the scope of the Halden Project's activities were equally presented. From the MORE project the paper [26] and [25] was presented and a demonstration of TRACE was provided. In addition a MORE project meeting was held during the conference.

2.5.8 ESREL and ISSRE (2007)

The ESREL conference stems from a European initiative merging the European Safety and Reliability Association (ESRA) and Society for Risk Analysis Europe (SRA-E) annual conferences into the major risk analysis, safety and reliability conference in Europe during 2008. The conference provided a forum for presentation and discussion of scientific papers covering theory, methods and applications in the fields of risk, safety and reliability to a wide range of sectors and problem areas.

Results related to the MORE project were presented at the European Safety and Reliability (ESREL) 2007 conference in Stavanger, Norway [7].
ISSRE focuses on the theory and practice of Software Reliability Engineering. The conference scope includes techniques and practices to (1) verify and validate software, (2) estimate and predict its dependability, and (3) make it more tolerant/robust to faults. Over the years, the conference has grown steadily, attracting about 200 participants on a regular basis. The conference is big enough to represent major topics in software reliability engineering, but small enough to provide an in-

depth representation of theory or practice in these areas. Industry participation has also increased over time, leading to a healthy mixture of theory and practice.

Results related to the MORE project were presented at the IEEE International Symposium on Software Reliability Engineering, (ISSRE 2007) in Trollhättan, Sweden [6]

2.5.9 Traceability Work Meeting (2008)

Industrial experience has shown that traceability mechanisms play an important role in the development of software-based systems, especially regarding complex safety relevant systems. Traditionally, the concept of traceability has been used to specify the relationships between requirements and system models, and often only at the early stages of the system development process. However, both the research and industrial communities have started to recognise the need to capture more traceability for a better and safer system development.

This was the background for the work meeting on traceability issues related to safety systems January 30-31 2008, held at ISTec in Garching, Germany, with participation from KAERI, ISTec and Japan Manned Space Systems Corporation. The aim of the meeting was to work towards possible research collaborations to address some of the challenges related to safety system’s development. The scope of the meeting was on requirements engineering concepts, especially traceability issues related to how to include results from risk assessment. Special interest was on the TRACE tool originated from the TACO and MORE projects and the work done in the Halden Reactor Project at IFE. The ideas and results of the work meeting were presented at the EHPG meeting at Loen [4].

One additional result from this work meeting was an application for a workshop: The 1st Workshop on Dependable Software Engineering (WDSE)" for ISSRE 2008 in Seattle, USA. This workshop was accepted at the end of June 2008.

2.5.10 MORE Project Meeting and EHPG (2008)

In relation to the EHPG Meeting 2008 in Loen, Norway, the MORE project group had a meeting for planning further activities for continuation of the TACO and MORE projects. The growing interest towards traceability issues [4] [12] gives possibilities to establishing a follow-up project in the area of requirements engineering and traceability. The main topic of the informal researcher meeting was to discuss the future plans and possible financing sources for a new project.

The concluding remarks of the meeting were that:

- The tool TRACE should be further developed.
- Requirements engineering is still an important topic and nuclear regulators have shown continuous interest to it.
- The Nordic co-operation especially between IFE and VTT has been working well.
- For the next project, also a Swedish partner would be desirable.
- The industrial contact network established in TACO and MORE projects should be utilised in the future as well.

- The Nordic nuclear utilities and regulators should be brought into the contact network with even bigger volume and greater emphasis.
- In case of a new common project, IFE and VTT will consider deepening their co-operation by sending visiting researchers to each other for short periods.
- A follow-up project will be further planned before the next NKS call for proposals.

In addition to NKS, also other funding sources should be investigated to establish a larger project.

3. The Approach for Dependable Requirements Engineering

This chapter describes a practical approach for dependable requirements engineering (DRE) of computerised systems. The approach has been developed by the Halden Project on the basis of the collected experiences in the TACO and MORE projects. The approach is also characterised by joint 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 [20][21][24]. The following provides some background and the main aspects of this approach.

3.1 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 is the Rational Unified Process (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: The more the elaboration phase is requiring during the design discipline, the more construction is needed during the implementation. Figure 1 illustrates an extended version of the RUP model, called the Enterprise Unified Process (EUP).

Despite the availability of detailed guidelines for sub-activities in each discipline and for the number of iterations in each phase, neither EUP nor any other lifecycle models provide 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 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 size of a certain phase, or the amount of certain sub-activities during the iterations [21]. 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.

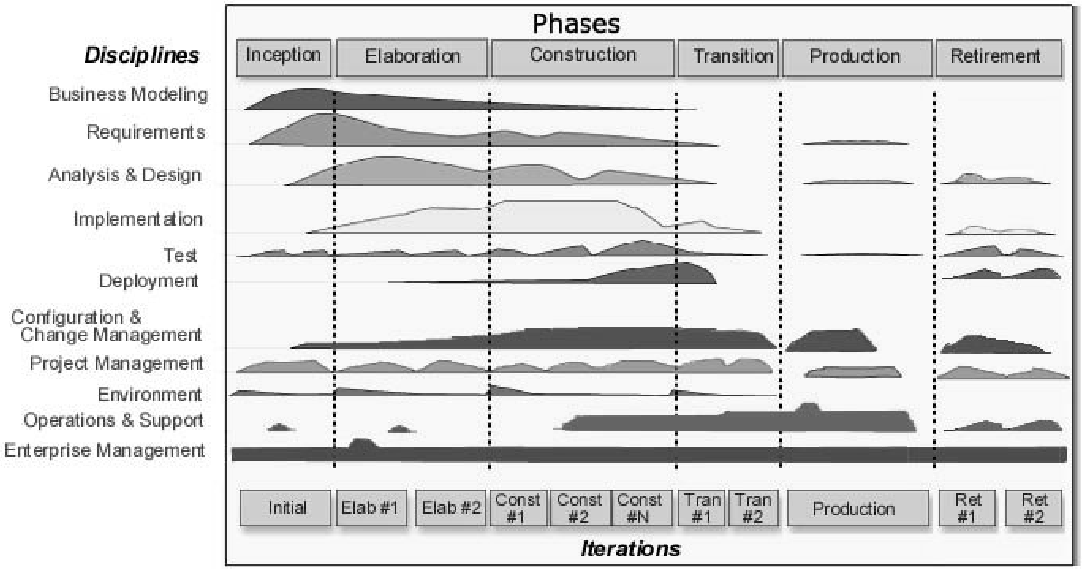


Figure 1. The Enterprise Unified Process (EUP).

As already mentioned, change management is closely related to the maintainability of the system development process and the result (the operational and applied system itself) of this process. 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.

3.2 The Four Pillars of the Approach for DRE

The approach for DRE is different from the traditional manner of understanding 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 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 [20]. 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* [20] [24]. 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. The most important analysis is that of thorough risk analysis with focus on one or several dependability factors that need to be analysed and assessed, 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, which a risk analyst is supposed to analyse.

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

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

The following chapter explains the main elements of the tool TRACE that aims to support the above approach. As far as traceability is concerned TRACE utilises the traceability model developed in the project TACO.

4. TRACE: A Tool for Traceability of Requirements for Analysable Computerised Environments

Providing tool support for the main elements of the traceability model suggested in the TACO project was among the important issues raised by the advisory group behind the TACO project. The group was formed through the industrial seminars arranged by the project. The prototype tool TRACE, an abbreviation for Traceability of Requirements for Analysable Computerised Environments, was developed to provide tool support for the approach for dependable requirements engineering (DRE); by utilizing and implementing the main elements of the TACO traceability model.

The ideas behind the features of TRACE were all concentrated on the four main pillars of the approach for dependable requirements engineering. Furthermore, it has been considered as a very important feature that the tool can be expanded as well as tailor-made (specialised), as response to different needs and applications.

This chapter describes the basic elements of TRACE that in combination can be used to achieve the objectives behind the approach for DRE in an efficient and practical manner. The following summarises therefore the main facilities of TRACE:

- Traceability between system artefacts defined at a particular stage of the system life cycle, hence traceability of system artefacts within the stages.
- Traceability between system artefacts defined at different stages of the system life cycle, hence traceability of system artefacts across the stages.
- Traceability of changing or changed system artefacts throughout the system lifecycle for better change management.
- Traceability of risk-oriented artefacts (representing failures, risks etc) with respect to a certain dependability factor, and thus associating risks with system artefacts. This supports better dependability analysis of the system.
- Traceability of dependability requirements throughout the system lifecycle, and thus associating risks with dependability requirements.
- Integration of or into additional tools, particularly systems modelling and risk analysis tools.

The basic elements of TRACE are *Paragraphs, Changes, Change Types, Links, History Trees,* and *Sets*. The following focuses on their description and their applications.

4.1 The Main Elements of TRACE

4.1.1 Paragraphs

The traceability approach and associated tool TRACE focuses on the concept of *Paragraphs*, which are objects containing the text describing a specific requirement. *Paragraphs* are associated with the following list of attributes:

id	Unique identifier.
label	Textual short label.
version	Version number. A *Paragraph* can be subject to a number of different *Changes*, where some *Changes* will cause creation of *Paragraphs* with a different label. In other cases *Changes* will cause creation of *Paragraphs* with the same label but with incremented version number (see description of *Change Types* below).
time	Time of creation.
Status	Status attribute (see Table 2 for valid values).
requirement	The text describing the actual requirement. The text should include a keyword such as “shall”, “should”. The purpose of the traceability approach is to keep a track of all changes to this attribute across different *Paragraph* versions and across development phases.
description	Additional textual description of the requirement.
changeIn	The change that caused the creation of the *Paragraph*.

changesOut	List of changes performed on the *Paragraph* causing the creation of other *Paragraphs*.
horizontalIn	List of *Paragraphs* belonging to other *History Trees*, which form the origin for the creation of the *Paragraph*. This attribute separates origin of type paragraph from the other origin types (see *origins* attribute below). See description of *Link* (which is implementing the concept of origin) below.
Origins	List of *Paragraph* origins. See description of *Link* (which is implementing the concept of origin) in sub-chapter below.
horizontalOut	List of *Paragraphs* for which this *Paragraph* is the origin.
ownerTree	The *History Tree* to which the *Paragraph* belongs. A *Paragraph* must belong to one and only one *History Tre*e.

Table 1: TRACE Paragraphs

The *status* attribute of a *Paragraph* or a *Change* can take the following values:

None	Default *Paragraph*/*Change* status.
Created	Indicates that the *Paragraph* is the first in a list of *Paragraphs* with the same label but with different version numbers. The *Paragraph* is the result of either a *create Change* or a *Change* performed on another *Paragraph* which creates one or more new *Paragraph*(s) (*derive*, *split*, *combine*...).
Trace	The *Paragraph/Change* is part of a trace result, e.g. a backward trace. The *Paragraph/Change* will be highlighted in the *History Tree* display.
Highlight	The *Paragraph/Change* is highlighted in the *History Tree* display.
Deleted	The *Paragraph* has been explicitly deleted (having been subject to the *delete Change*).

Table 2: TRACE status attribute of a Paragraph or a Change

4.1.2 Changes

A *Change* contains the properties of a single *Change* from one or more *Paragraphs* into one or more *Paragraphs*. *Changes* are associated with the following list of attributes:

Id	Unique identifier.
Type	Type of *Change* (see description of *Change Type* in sub-chapter below).
Sources	List of input *Paragraphs* to this *Change*.
Targets	List of output *Paragraphs* from this *Change*.
Status	Status attribute (see table above).
userId	Identifier of the user responsible for introducing the *Change*.
Time	Time of introduction of the *Change*.

Reason	Textual description of the reason for introducing the *Change*.
Basis	The basis for introducing the *Change* (see Table 5).
Validated	A Boolean value indicating whether the *Change* has been validated by a user.
validatedUserID	The ID of the user that validated the *Change*.

Table 3: TRACE Changes

The *basis* parameter is used to provide some description of the basis for applying the *Change* to one or more *Paragraphs*. The valid values for the *basis* parameter are defined as follows:

Method	The *Change* has been introduced due to the outcome of some analysis method, e.g. a HazOp analysis, which has suggested that the *Paragraph*(s) must be updated due to some shortcoming.
Expert	The *Change* has been introduced due expert judgement.
None	No special basis is given for the *Change*.

Table 4: TRACE basis parameter

4.1.3 Change Types

ChangeTypes are used to define different types of *Changes*. A *Change Type* is associated with the following list of attributes:

label	Unique label.
paraIn	The number of input *Paragraphs* (valid values are “0”, “1”, “1 or more” and “2 or more”).
paraOut	The number of output *Paragraphs* (valid values are “0”, “1”, “1 or more” and “2 or more”).
description	Textual description of the change type.
resultStatus	Status of output *Paragraph*(s) (see Table 1).
update	How to update the output *Paragraphs* label and version (see Table 6)
locked	A Boolean value indicating if the *Change Type* is “locked”, i.e. that no other attributes may be altered.

Table 5: TRACE Change Types

The *update* value defines how the *Paragraph* label and version number are determined for a *Paragraph* resulting from a *Change*. The valid values for the *update* value are defined as follows:

No update	The output *Paragraph* has the same label and version number as the input *Paragraph*.
New label	The output *Paragraph* is given a different label than the input *Paragraph*.
Increment version number	The version number of the output *Paragraph* is incremented relative to the input *Paragraph*.

Table 6: TRACE update value

The *Change Types* include:

- create
- modify
- combine
- replace
- split
- derive
- delete
- un-delete

An example of a *Change Type* is “modify”. The attribute values for “modify” are given in the following table:

label	“modify”
paraIn	1
paraOut	1
description	“This change denotes a modification of the paragraph”
resultStatus	None
update	Increment version number
locked	“true”

Table 7: TRACE attribute values for modify

Only one *Paragraph* at a time can be subject to a *Change* of the type *modify*, and the result is a single *Paragraph* where the label is kept, while the version number is incremented.

4.1.4 Links

In many cases it can be useful to include information regarding the reason for introducing a *Paragraph*. Examples of this information can be:

- A textual reference to a brainstorming meeting.
- A textual reference to a standard, suggesting an introduction of a specific safety function.

- A textual reference to statistical data showing the potential system reliability improvements.
- A link between a *Paragraph* of the *implementation* phase and a *Paragraph* of the *design* phase, indicating that the former fulfils the requirements of the latter.

The *origin* attribute of a *Paragraph* is used to provide information regarding the origination of the *idea* of the *Paragraph*. This information can be a combination of textual descriptions, files, hypertext links, and other *Paragraphs*. The *Link Type* implements the concept of the origin attribute. The attributes associated with the *Link* type are as follows:

type	Type of link
string	Textual information regarding the Link

Table 8: TRACE Link type attributes

Examples of *Links* are given in Table 9:

A textual link

```
object Link
      type: TEXT
      string: “This Paragraph was included due to a discussion at project meeting
      in Halden on 2005-04-08”
end
```

A file link

```
object Link
      type: FILE
      string: “c:\projects\more\p08-basis.doc”
end
```

A hypertext link

```
object Link
      type: HYPERTEXT
      string: “http://standards.ieee.org/catalog/olis/index.html”
end
```

A Paragraph link

```
object Link
      type: PARAGRAPH
      string: “PA_002389” (the ID of a particular Paragraph)
end
```

Table 9: Examples of Links

4.1.5 History Trees

A *History Tree* holds all required information about a history tree, including all of it’s *Paragraphs* and *Changes*. An example of a history tree is shown in Figure 2. *History Trees* will show the development of a number of *Paragraphs* as they are subject to *Changes*, and for software development projects a typical use is to create one *History Tree* for each development phase.

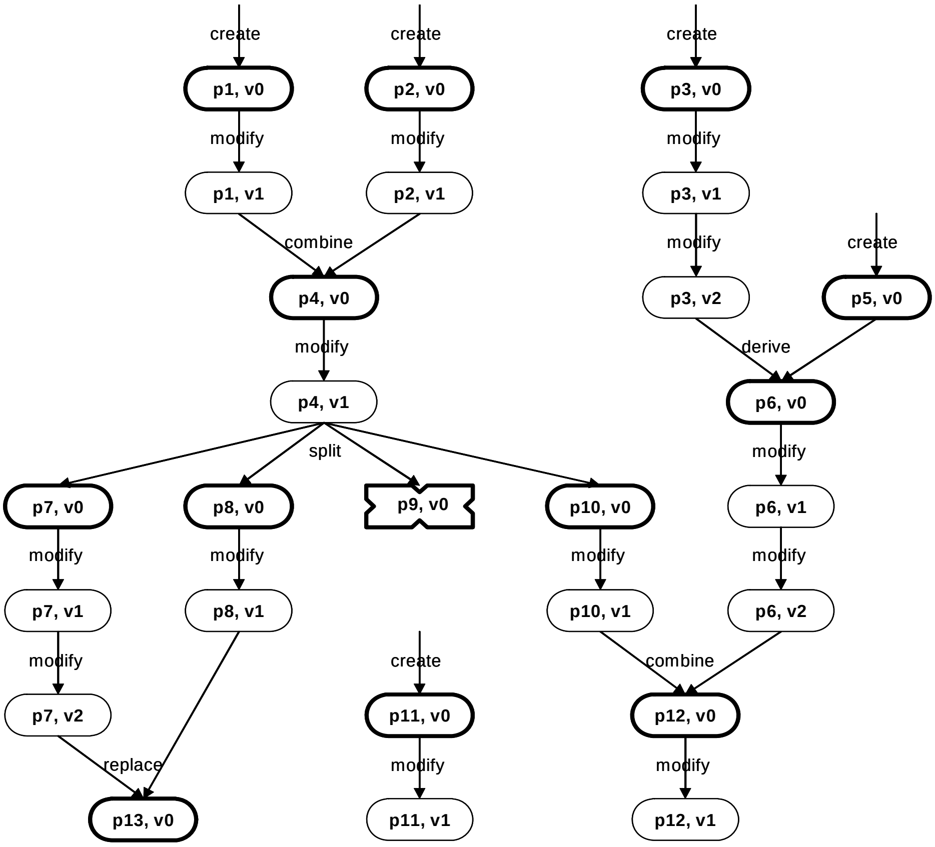


Figure 2. Example: History Tree

The list of attributes associated with a *History Tree* is:

id	Unique identifier.
label	Textual label provided by user.
paragraphs	List of *Paragraphs*.
changes	List of *Changes*.
createTime	Creation time.
lastChangeTime	Last time history tree was changed.
description	Textual description of the *History Tree*.

Table 10: TRACE History Tree attributes

4.1.6 Sets

A *Set* extends the *History Tree* to include a list of subsets, links to parent and child sets, and information about opening and closing times and status. This allows a *Set* to contain any number of *Paragraph* objects, as well as any number of *Set* objects, and to maintain a derivative relationship between *Set*s.

The list of attributes associated with a *Set* (in addition to those inherited from *History Tree*) is:

trees	List of *History Trees*.
sets	List of subsets.
parent	Parent set.
child	Child set.
open	Indicates whether *Set* is open or closed. If the *Set* is “open”, objects may be added to or deleted from the *Set*.
closeTime	Time the *Set* was closed.

Table 11: TRACE Set attributes

One typical use of the *Set* could e.g. be to group all *security-related* requirements into a separate *Set*, facilitating a subsequent *security analysis* and its associated *risk analysis*.

A *Set* will be able to compare its content (specifically its list of *Paragraphs*) to the content of another *Set*, i.e. which *Paragraphs* are common to both *Sets*, and which *Paragraphs* are unique for each *Set*. This ability is particularly relevant in *change management*, where the difference between two versions of the same software with regard to which *Paragraph* versions they implement is readily apparent.

An open *Set* can have its content (i.e. list of *Paragraphs*, *History Trees* and subsets) edited, while a closed set is not editable. In software development this will typically correspond to a version of the software where the feature *Set* has been frozen.

4.2 Basic Analysis

Using the features of the classes described in Section 3.1, TRACE can perform a number of analysis relevant to software development and change management:

Created Paragraphs	Whenever a new *Paragraph* is created from scratch or by certain *Changes* to other *Paragraphs* (e.g. derive, split, combine...), the Paragraph is marked as “Created”.
Current Paragraphs	The current or most recently updated version of a *Paragraph* is found by iterating through the list of *Paragraphs* and for each *Paragraph* label find the *Paragraph* with the highest version number. (Paragraphs that have been explicitly deleted are not included in this search)
Deleted Paragraphs	Whenever a *Paragraph* is deleted, it is marked as “Deleted”.
Paragraph History *(upward/downward)*	The *Paragraph* history for any *Paragraph* can be determined by finding all versions of the selected *Paragraph*, all *Changes* affecting these versions, as well as the relevant version of all *Paragraphs* included in these *Changes*. This is straightforward, as all *Paragraph objects* contain lists of “incoming” and “outgoing” *Changes*, and all *Change objects* contain lists of “input” and “output” *Paragraphs*.

Paragraph vertical Trace *(upward/downward)*	**Upward:** Upward traceability relates to the development of *Paragraphs* starting with a selected *Paragraph* in a single *History Tree*. The result will include all *Paragraphs* affected by the selected *Paragraph* (see Figure 3). The trace is performed by a recursive search through all output *Changes* starting with the selected *Paragraph*. The search through a sub-tree is halted once a Paragraph without any output *Changes* is reached. **Downward:** Given a *Paragraph*, we want to find the development of *Paragraphs* that leads to this Paragraph, i.e. the minimum fragment of the *Change* history that has influenced the development of the given *Paragraph* (see Figure 4). The trace is performed by a recursive search through all input *Changes* starting with the selected *Paragraph*. The search through a sub-tree is halted once a *Paragraph* whose input is a “create” *Change* is reached.
Paragraph Horizontal Trace *(forward/backward)*	**Forward:** Given a *Paragraph*, we want to find how the *Paragraph* belonging to a *History Tree* has been further developed (has lead to the creation of *Paragraphs*) in other *History Trees*. The *horizontalOut* parameter in the *Paragraph* class provides links to *Paragraphs*, which were created based on the selected *Paragraph*. The trace is performed by a recursive search through all *horizontalOut* with the selected *Paragraph*. The search through *History Trees* is halted once a *Paragraph* whose *horizontalOu*t is empty is reached. **Backward:** Given a *Paragraph*, we want to find the *Paragraphs* in other *History Trees* that lead to the development of the selected *Paragraph*. The *horizontalIn* parameter in the *Paragraph* class provides links to *Paragraphs* used when creating a *Paragraph*. The trace is performed by a recursive search through all *horizontalIn* with the selected *Paragraph*. The search through *History Trees* is halted once a *Paragraph* whose *horizontalIn* is empty is reached. A typical use of the horizontal trace could be during a software development project, where a separate history tree is created for each development phase (requirement, design, implementation, test...). Here, each *Paragraph* would represent a specific version of a specification, and often a specification in the design phase would be based on a specification in the requirement phase, and will further lead to a specification in the implementation phase (see Figure 5).
Origin Trace	The *origin* parameter in the *Paragraph* class provides links to information used when creating a *Paragraph*. This information could e.g. be a textual description of why the *Paragraph* should be included, a shortcut to a file, or a hypertext link to an IEEE standard used as basis for the *Paragraph*.

Table 12: TRACE Basic analysis

Figure 3-5 illustrates the different options for traceability: downward, upward, horizontal between the different requirements (e.g. F-PRM-1, v0 and F-PRM-2, v0) from the PRM case.

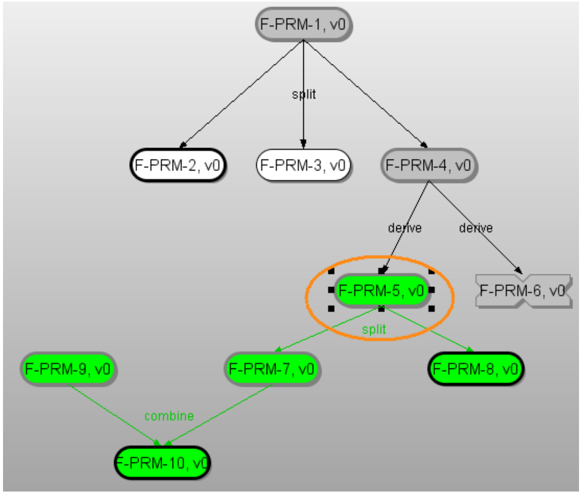


Figure 3. Downward trace from (FPRM-5, v0)

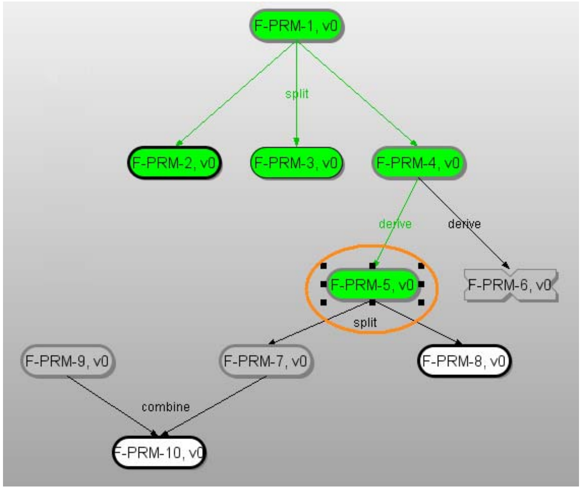
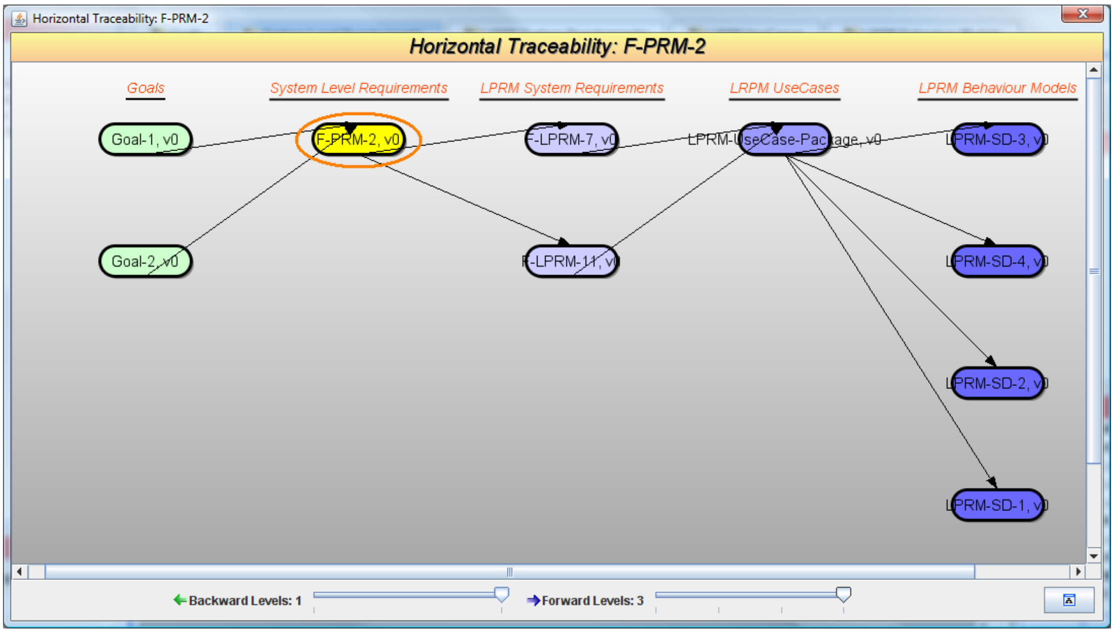


Figure 4. Upward trace from (FPRM-5, v0)



Backward Levels: 1

Forward Levels: 3

Figure 5. Horizontal trace - The lines from (F-PRM-2, v0) are links to other Paragraphs *in other phases*

5. Further Integration of Requirements Engineering and Risk Assessment

The work on integrating requirements engineering and risk assessment is also going on in the Halden Project The research being carried out to better integrate the risk assessment and dependability factors into the system life cycle, and thus making both the system and life cycle analysable with regard to the dependability, has a close relation to the work that has been done in the MORE project. The TACO traceability model and the tool TRACE will in the future also be improved accordingly.

The ongoing work focus on the following steps:

- Further develop a case study, and based on the results and experiences from the case study and the DRE approach, improve the TACO traceability model and extend the work on management of requirements.
- Apply and further develop the tool TRACE during the case study.
- Evaluate the above, using the case study results and regular expert reviews.
- Use the approach and tool TRACE during a real-case study.

The case study chosen was to develop a whole Power Range Monitoring (PRM) system. For the case study we choose a part of the computerised power range monitoring (PRM) system of a nuclear reactor. The PRM system has been applied in several studies in the Halden Project, and was introduced in HWR-397 [5].

The case study is undertaken as two trials, the first developing the PRM system using a semi-formal approach. The second trial using a formal approach (using the tool NuSEE developed by KAERI [9]) will be carried out as a part of the future work in the Halden Project. This will provide a much larger system, and the opportunity to look into the challenges encountered while developing and assessing such a system using different methods and techniques.

6. Related Activities

This chapter lists some activities from Finland and Sweden that are somehow related to MORE and have been interesting for the project group.

6.1 SAFIR Programme 2003 – 2006

SAFIR 2003 – 2006 (SAfety of nuclear power plants – FInnish national Research programme) [13] was the continuation of the former research programmes on nuclear power plant safety (FINNUS, RATU2, RETU, RATU, YKÄ). The programme was divided into six research areas out of which the areas “Automation, control room and information technology” and “Risk-informed safety management" had projects closest to the interests of the MORE project.

A project called “Assessment of smart device software” (ASDES) raised interest among the researchers of MORE. The ASDES 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 was a goal-based method that defined claims, elaborated and apportioned them to smart devices and components and then creatively identified the arguments required to show these claims. Then, one had to assess whether the claims were 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 [30].

6.2 SAFIR Programme 2007-2010

SAFIR2010 (SAfety of nuclear power plants – FInnish national Research programme 2007-2010) 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 [14].

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 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) [27][29]. 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 being 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 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.

6.3 Swedish Experiences

Following [10] and [11], the Swedish experiences from Oskarshamn 1 and Ringhals 2 I&C system modernisation project, there is early in the projects 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).

It has been recognised that 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 concerning the developed systems is focused on presenting the result. For the safety review of digital I&C, the documentation concerning the path and the processes for achieving the results are needed as well. Having top-down and bottom-up traceability in systems and documentation is also important to enable effective validation.

7. Conclusions of the MORE Project

In general, it can be said that the MORE project was successful in the sense of making contacts and establishing, not only Nordic but also European, contact network. Also contacts to Korea and Japan were made around the topics of MORE.

During the past years of research in the MORE project (and also the predecessor project TACO) the focus has been on requirements engineering and requirements traceability. The project group has familiarized itself with the research field through several contacts and discussions with the members of the expert network created during the project. Several topics of interest and worth researching have been raised and brought up by the researchers of the MORE project and the expert network. In the following, there is list of insight gained on issues that need more thorough research to be fully tackled.

- Licensing of safety critical systems has been too much focused on technical issues and too little on higher level strategies and planning. A single requirement has not very significant role compared to a high quality overall system design that is unambiguous, traceable, and testable.
- There are several existing tools for requirements engineering. They have some differences and similarities but the most important thing is not the tool itself. The way the tool is used and what kinds of principles and working processes there are behind it counts the most. High-quality tools will not help if the process is bad. Healthy processes compensate lack of tools.
- In the system development process, there are several actors with different responsibilities and viewpoints:
    - Utilities / Licensees (investor customers).
    - Vendors / Product developers.
    - Regulators (Laws and safety requirements).
    - Consultants (Independent assessors).
    - Marketing / Financial actors.
    - Certifiers.

  The complexity increases with the number of interest groups with different priorities.
- Validation and verification (V&V) are difficult topics that typically invoke strong opinions. In order to avoid conflicts it is necessary that the stakeholders agree upon and thoroughly define their role, responsibilities and duties in the V&V process. In system validation, as well as in system development, incremental approach was tried and found useful. Whenever there are changes in the

- Utilising formal methods in V&V is difficult if the system complexity is high and if the system has not been formally specified during development i.e. the system properties have been modelled in an unambiguous manner beforehand. However, formal methods can be used for supporting V&V activities as shown in [28] where model checking has been used for formal verification of safety I&C system designs although the target system was not formally developed.
- Not all requirements can be presented in formal way. E.g. compliance with standards and user friendliness are difficult to formalise. That is why the systems must be divided according to their aspects, functions, modules, components, in order to identify which ones are suitable for formal analysis. After this identification the most appropriate methods can be selected for each particular part of the system.

Thus, the MORE project can be concluded by stating that it has been very important forum for deepening the Nordic co-operation and improving the contact network within the researchers in the area of nuclear safety. The funding received from NKS has enabled exchange of information and several happenings that would have left undone without the MORE project.

8. 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 responsible for the contents of the report.

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

9. References

[1] 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

[2] K. Brodén (ed.): Seminarium om avveckling. Risø, 13-15 september 2005, NKS-116, NKS_R_2004_27, December 2005.

[3] 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

[4] B. A. Gran, V. Katta, C. Raspotnig, J-S Lee, H. Miedl, J. Märtz, J. Valkonen, H. Nakao, Recommendations and Proposals to the Research on Requirement Engineering and Risk Assessment, Enlarged Halden Programme Group Meeting, 18th – 23rd May 2008, Proceedings of the Man-Technology-Organisation (MTO) Sessions, Loen, Norway

[5] A.K. Groven, T. Sivertsen: “Formal Software Development – A Case Study on the Development of a Reactor Safety System”, HWR-397, OECD Halden Reactor Project, October 1994.

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

[7] V. Katta, 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.

[8] V. Katta, C. Raspotnig. Integrating Requirements Engineering and Risk Assessment: Solving the Missing Links, HWR-891, OECD Halden Reactor Project, May 2008.

[9] S. R. Koo et al.: “NuSEE: An Integrated Environment of Software Specification and V&V for PLC based Safety-Critical Systems”, Nuclear Engineering and Technology, Vol 38, pp. 259–276, 2006.

[10] B. Liwång. “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.

[11] B. Liwång. “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.

[12] C. Raspotnig, V. Katta, J. E. Simensen, TRACE - from Research to Application, Enlarged Halden Programme Group Meeting, 18th – 23rd May 2008, Proceedings of the Man-Technology-Organisation (MTO) Sessions, Loen, Norway

[13] SAFIR 2003 – 2006 web pages. http://www.vtt.fi/safir

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

[15] 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

[16] G. Sindre, A. 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

[17] T. Sivertsen, R. Fredriksen, A. P-J Thunem, J-E Holmberg, J. Valkonen, O. Ventä, J-O Andersson, “Traceability and communication of requirements in digital I&C systems development”, TACO final report, NKS-115, October 2005.

[18] T. Sivertsen, R. Fredriksen, A. P-J. Thunem, J. Holmberg, J. Valkonen, O. Ventä and J-O. Andersson: “The TACO Approach for Traceability and Communication of Requirements”. In Proc. Safecomp 2005, Computer Safety, Reliability and Security, LNCS 3688, Rune Winther, Bjørn Axel Gran, Gustav Dahll (Eds.), Springer, Fredrikstad, Norway, 2005.

[19] T. Sivertsen, R. Fredriksen, A. P-J. Thunem, J. Valkonen, J.E. Holmberg, O. Ventä, J-O. Andersson: “TACO – a Framework for Traceability and Communication of Requirements”, HWR-774, OECD Halden Reactor Project, June 2005.

[20] 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), Cambridge (MA), USA, September 2003.

[21] 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), Berlin, Germany, June 2004.

[22] 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.

[23] A. P-J Thunem, R. Fredriksen, H. P-J Thunem, O. Ventä, J. Valkonen, J-E Holmberg, “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.

[24] 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”), New Orleans, USA, May 2006,

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

[26] 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.

[27] J. Valkonen, V. Pettersson, K. Björkman, J-E Holmberg, M. Koskimies, K. Heljanko, and I. Niemelä. Model-Based Analysis of an Arc Protection and an Emergency Cooling System – MODSAFE 2007 Work Report. VTT Working Papers 93, 2008.

[28] J. Valkonen, M. Koskimies, V. Pettersson, K. Heljanko, J-E Holmberg, I. Niemelä, J. J. Hämäläinen, Formal Verification of Safety I&C System Designs: Two Nuclear Power Plant Related Applications, Enlarged Halden Programme Group Meeting, 18th – 23rd May 2008, Proceedings of the Man-Technology-Organisation (MTO) Sessions, Loen, Norway

[29] J. Valkonen, I. Karanta, M. Koskimies, K. Heljanko, I. Niemelä, D. Sheridan, and R. E. Bloomfield. NPP Safety Automation Systems Analysis - State of the Art. VTT Working Papers 94, 2008.

[30] 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

10. Appendix A: Project Organisation and Activities

The project has been led by Rune Fredriksen (IFE), and has comprised 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 has been subject for extension by involvement of additional industrial partners. In addition, the network represented by the activity organisation has been extended though the arrangement of the industrial seminars.

The project leader has been responsible for organising the work within the project and directing it towards its objectives. This has included:

- 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 have been representing important parts of the technical competence within the project, and have been responsible for contributing to the activities in such a way that it has been possible to meet the objectives of the project.

The funds received from NKS for the work in 2007 are estimated to cover 50% of the overall costs. The remaining 50% are covered through the individual costs and efforts of each participating organisation. Each organisation has been 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 have been allocated for project coordination (IFE). The remaining 80% has been 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 have been split equally between IFE and VTT. The approximate division of costs between work, travel, and equipment is given in the Proposal Summary 2007.

At this point there are no planned activities in the project.

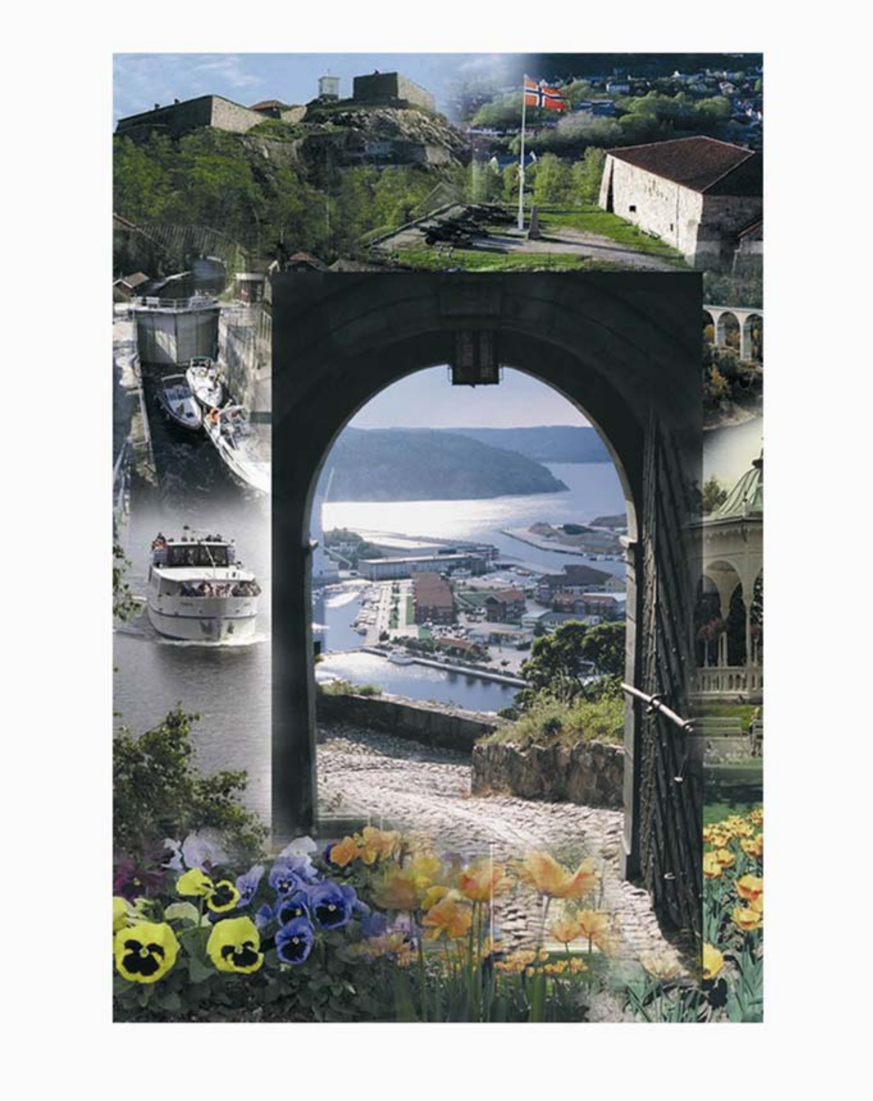
The remaining overall documentation schedule is as follows:

- June 30, 2008: Final report (this report)

11. Appendix B: International Seminar on Dependable Requirements Engineering of Computerised Systems at NPPs

Halden, Norway
November 27-29, 2006

PROGRAMME



Hosted by Institute for Energy Technology (IFE) in Halden
Co-sponsored by NKS (Nordic Nuclear Safety Research)

PRACTICAL INFORMATION

Short CV for the Key Note Speaker

Arndt B. Lindner (diploma in mathematics, Technical University of Chemnitz, 1975; Ph. D. in automation engineering, Technical University of Dresden, 1989) started research for NPP instrumentation and control at the Rheinsberg Nuclear Power Station in 1975, continued this work from 1980 on in the ZfK (Zen-tralinstitut fuer Kernforschung der Akademie der Wissenschaften der DDR) in Rossendorf near Dresden and from 1992 on in ISTec (Institute for Safety Technology) as scientist and since 2002 as head of the I&C department of ISTec. He is member of the RSK (Reactor Safety Commission)-Committee for Electrical Installations and in Working Group 3A (Convenor) of IEC/SC45A. Dr. Lindner is also member in additional national and international working groups. Current interests are in architecture, safety and security and licensing issues of digital safety I&C for NPPs. Dr. Lindner is author of numerous papers in this field.

General Chair

Patrick Isaksson, NKS-R Programme Head

Technical Programme Committee

Atoosa P-J Thunem, IFE/HRP, Norway (Chair)
Bo Liwång, SKI, Sweden
Roman Shaffer, US-NRC, Usa
Thuy Nguyen, EPRI/EDF, Usa/France
Tamas Bartha, SZTAKI/KFKI, Hungary
Arndt Lindner, ISTEC/GRS, Germany
Harri Heimburger, STUK, Finland
Olli Ventä, VTT, Finland

Local Organising Committee

Atoosa P-J Thunem, IFE/HRP, Norway
Grete Bjerkely, IFE/HRP, Norway
Harald P-J Thunem, IFE/HRP, Norway
Rossella Bisio, IFE/HRP, Norway
Vikash Katta, IFE/HRP, Norway
Janne Valkonen, VTT/ IFE/HRP, Finland/Norway

Secretary

The Workshop Secretary, Grete Bjerkely, assisted in practical details during the workshop.

Social Event

Institute for Energy Technology was the host for the seminar dinner, which took place at Park Hotel, Monday, November 27, at 19:00.

DETAILED PROGRAMME
MONDAY, NOVEMBER 27

8:30 to 9:00 **Registration**

9:00 to 9:45 **Opening session**

Welcome to the seminar participants *Session Chair: P. Isaksson / Co-chair: A. P-J Thunem*

- General Chair: NKS-R Programme Manager Patrick Isaksson
- IFE, Safety MTO: Division Head Øivind Berg
- Technical Chair: Atoosa P-J Thunem

Brief explanation of the seminar's structure

9:45 to 10:45 **Key-Note Speech**

Arndt Lindner: The Revised IEC 60880

10:45 to 11:00 **Break**

11:00 to 12:00 **Paper presentations**

Managing SW-intensive environments *Session Chair: H. Heimbürger / Secretary: R. Bisio*

1. *T. Bartha, E. Németh:* Formal Modelling and Verification of Specifications for I&C System Software in NPPs
2. *M. Kropik, M. Jurickovak:* Software Requirements for New Independent Power Protection and Control Systems of VR 1 Training Reactor
3. *K. Juslin:* Requirements on Automation and Simulation Software Platforms for Efficient Design and Testing

12:00 to 12:30 **Discussion**

12:30 to 13:30 **Lunch**

13:30 to 14:30 **Paper presentations**

Modelling dependability factors *Session Chair: T. Bartha / Secretary: H. P-J Thunem*

1. *G. Dobson, P. Sawyer:* Revisiting Ontology-Based Requirements Engineering in the age of the Semantic Web
2. *R. Savola:* Towards Requirement Driven Evaluation of Information Security
3. *G. Sindre, A. Opdahl:* Misuse Cases – Use Cases that Capture Security Threats

14:30 to 15:00 **Discussion**

15:00 to 15:15 **Break**

15:15 to 15:30 **Bus departure to IFE's MTO Lab**

15:30 to 16:30 **Presentations at IFE's MTO Lab**

16:30 to 16:45 **Bus departure to Park Hotel**

19:00 **Social Event: Aperitif and seminar dinner at Park Hotel**

DETAILED PROGRAMME

TUESDAY, NOVEMBER 28

9:00 to 10:00 Paper presentations

R&D work related to requirements engineering at IFE — *Session Chair: A. Lindner / Secretary: J. Valkonen*

1. *A. P-J Thunem:* IFE’s Approach for Dependable and Risk-Informed Requirements Engineering
2. *H. P-J Thunem:* TRACE: A Tool for Traceability of Requirements for Analysable Computerised Systems
3. *V. Katta, A. P-J Thunem:* Improving Model-Based Risk Assessment Methods by integrating the Results of Requirements Engineering into the System Models
4. *R. Bisio:* Dependable Requirements Engineering for WEB Based Systems: A growing experience

10:00 to 10:30 Discussion

10:30 to 10:50 Break

10:50 to 12:00 Paper presentations

The role of standards — *Session Chair: Bo Liwång / Secretary: Ch. Raspotnig*

1. *G. Glöe:* Capturing of Dependable Requirements Engineering of Computer Systems at NPPs
2. *T. Hadler:* Evaluation of the Compliance of Computerised Systems at NPPs with Dependable Requirements

12:00 to 12:30 Discussion

12:30 to 13:30 Lunch

13:30 to 14:30 Paper presentations

The regulator’s standpoint — *Session Chair: G. Glöe / Secretary: V. Katta*

1. *H. Heimbürger:* Overview of Safety and Safety Related I&C Research and Regulatory Activities in Finland
2. *B. Liwång:* Software-based Safety Systems: Some Comments from A Regulator on Documentation and Traceability

14:30 to 16:00 Workshop session: “Coffee Table Discussions”

Main Topic: Aspects of dependable and risk-informed requirements engineering
Sub-topics:

1. *Licensing requirements: How difficult are they to interpret and meet?*
2. *The relationships between systems development process and requirements engineering*
3. *Policies for freezing the requirements and for accepting or rejecting changes*
4. *Approaches for requirements validation and verification (also related to already developed systems and modernisation activities)*
5. *Defining and classifying dependability-related requirements: Do we really have other kinds of requirements?*
6. *Terminologies for specifying discipline-oriented (life cycle levels) and domain-oriented (e.g., industrial branches) requirements*

16:20 to 17:00 Presentations of the results from the workshop session

DETAILED PROGRAMME

WEDNESDAY, NOVEMBER 29

9:00 to 10:00 **Paper presentations**

Empirical observations *Session Chair: P. Isaksson / Secretary: A.P-J Thunem*

1. *T. Lauritsen, T. Stålhane:* An Empirical Study of Introducing the Failure Mode and Effect Analysis Technique to Norwegian Business Critical Software Developers
2. *J. Valkonen:* Requirements Traceability Experiences from SCORPIO Core Surveillance System
3. *H. Miedl:* Qualification of computer-based I&C systems

10:00 to 10:30 **Discussion**

10:30 to 10:50 **Break**

10:50 to 12:00 **Main Messages from the seminar discussions**

Short presentations by session secretaries *Session Chair: P. Isaksson / Secretary: A. P-J Thunem*

12:00 to 13:00 **Lunch**

13:00 to 14:00 **Final session including conclusions**

Summarising the seminar: *Session Chair: P. Isaksson / Secretary: A. P-J Thunem*

- Key issues
- Path ahead

14:00 to 14:30 **Farewell**

List of Participants

Name:	Organisation:	Address:	Country:	Tel.:	Fax:	E-mail:
CZECH REPUBLIC:						
Kropik, Martin	Faculty of Nuclear Sciences and Physical Engineering CTU in Prague		Czech Republic	+420 603 871 795	+420 284 680 764	kropik@troja.fjfi.cvut.cz
Molnar, Jozef	Nuclear Research Institute Rez plc	Husinec-Rez, Cp. 130, 250 68	Czech Republic	+420 38110-3939	+420 38110-4103	Mol@ujv.cz
Denmark:						
Morten Lind	Oersted · DTU, Automation, Technical University of Denmark	Building 326 DK-2800 Kongens Lyngby	Denmark	+45 45253566	+45 45881295	mli@oersted.dtu.dk
FINLAND:						
Heimbürger, Harri	STUK	P.O.Box 14 FI-00881 Helsinki	Finland	+358 9 759881	+358 9 75988382	harri.heimburger@stuk.fi
Kaj Juslin	VTT Technical Research Centre of Finland	P.O.Box 1000 FIN-02044,	Finland	+358 40 500 1254	+358 20 722 7053	kaj.juslin@vtt.fi
Savola, Reijo	VTT	P.O.Box 1100 FIN-900571 Oulu	Finland	+358 40 569 6380	+358 20 722 2320	reijo.savola@vtt.fi
Valkonen, Janne	VTT	P.O.Box 1000 FIN-02044	Finland	+358 20 722 6469	+358 20 722 6027	janne.valkonen@vtt.fi

GERMANY:						
Glöe, Günter	TÜV Nord SysTec GmbH & Co. KG	Grosse Bahnstrasse 31 22525 Hamburg	Germany	+49 40 8557 25 77	+49 40 8557 2429	ggloee@tuev-nord.de
Hadler, Tobias	TÜV Nord SysTec GmbH & Co. KG	Grosse Bahnstrasse 31 22525 Hamburg	Germany	+49 40 8557 2727	+49 40 8557 2429	thadler@tuev-nord.de
Lindner, Arndt	ISTec GmbH	Forschungsgelände D-85748	Germany	+49 89 32004 529	+49 89 32004 300	arndt.lindner@istec.grs.de
Miedl, Horst	ISTec GmbH	Forschungsgelände D-85748	Germany	+49 89 32004 528	+49 89 32004 300	horst.miedl@istec.grs.de
HUNGARY:						
Bartha, Tamás	MTA SZTAKI Computer and Automation Research Institute	Kende u. 13-17 H-1111 Budapest	Hungary	+361 279 6227	+361 466 7483	tamas.bartha@sztaki.hu
NORWAY:						
Lauritsen, Torgrim	NTNU	Sem Sælandsvei 7-9 7491 Trondheim	Norway	+47 3594427 +47 95129557 mob	+47 73594466	torgriml@idi.ntnu.no
Opdahl, Andreas L.	Universitetet i Bergen	Infomedia, UiB Postboks 7800, 5020 Bergen	Norway	+47 55 58 91 00	+47 55 58 91 49	andreas@infomedia.uib.no
Sindre, Guttorm	NTNU	Sem Sælandsvei 7-9 7491 Trondheim	Norway	+47 73594479	+47 73594466	guttors@idi.ntnu.no
SWEDEN:						
Isaksson, Patrick	Vattenfall Power Consultant AB	Box 527 162 16 Stockholm	Sweden	+46 8 739 50 00	+46 8 739 62 26	Patrick.isaksson@vattenfall.com
Liwång, Bo	SKI	SE-10658 Stockholm	Sweden	+46 86988492	+46 8 6619086	bo.liwang@ski.se
United Kingdom:						
Dobson, Glen	Lancaster University Computing Departmetn		UK	+44 1524 510311	+44 1524 510492	g.dobson@comp.lancs.ac.uk
IFE:						
Berg, Øivind	Institutt for energiteknikk OECD Halden Reactor Project	P.O.Box 173 1751 Halden	Norway	+47 69 21 22 71	+47 69 21 24 60	oivind.berg@hrp.no
Bisio, Rossella	IFE, OECD-HRP	P.O.Box 173 1751 Halden	Norway	+47 69 21 22 49	+47 69 21 24 60	rossella.bisio@hrp.no
Gran, Bjørn-Axel	IFE, OECD-HRP	P.O.Box 173 1751 Halden	Norway	+47 69 21 23 59	+47 69 21 24 60	bjorn.axel.gran@hrp.no
Katta, Vikash	IFE, OECD-HRP	P.O.Box 173 1751 Halden	Norway	+47 69 2122 65	+47 69 21 24 60	vikash.katta@hrp.no
Christian Raspotnig	IFE, OECD-HRP	P.O.Box 173 1751 Halden	Norway	+47 69 2122 96	+47 69 21 24 60	christian.raspotnig@hrp.no
Thunem, Harald P-J.	IFE, OECD-HRP	P.O.Box 173 1751 Halden	Norway	+47 69 21 22 78	+47 69 21 24 60	harald.p-j.thunem@hrp.no
Thunem, Atoosa P-J.	IFE, OECD-HRP	P.O.Box 173 1751 Halden	Norway	+47 69 21 23 22	+47 69 21 24 60	atoosa.p-j.thunem@hrp.no

Bibliographic Data Sheet NKS-178

Title	MORE: Management of Requirements in NPP Modernisation Projects, Final Report
Author(s)	Rune Fredriksen[1], Vikash Katta[1], Christian Raspotnig[1] and Janne Valkonen[2]
Affiliation(s)	[1]Institutt for energiteknikk (IFE), Norway [2]Technical Research Centre of Finland (VTT), Finland
ISBN	978-87-7893-244-0
Date	September 2008
Project	NKS-R / MORE
No. of pages	42
No. of tables	12
No. of illustrations	5
No. of references	30

Abstract

This report documents the work and related activities of the MORE (Management of Requirements in NPP Modernisation Projects) (NKS-R project number NKS_R_2005_47) project. This report also provides a summary of the project activities and deliverables, and discusses possible application areas. The project has aimed at the industrial utilisation of the results from the TACO: (Traceability and Communication of Requirements in Digital I&C Systems Development) (NKS-R project number NKS_R_2002_16, completed June, 2005) project, and practical application of improved approaches and methods for requirements engineering and change management. Finally, the report 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