nks

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

NKS-115
ISBN 87-7893-176-2

Traceability and Communication of Requirements in Digital I&C Systems Development Final Report

Terje Sivertsen, Rune Fredriksen, Atoosa P-J Thunem
Institute for Energy Technology, Halden, Norway

Jan-Erik Holmberg, Janne Valkonen, Olli Ventä
VTT, Finland

Jan-Ove Andersson
Ringhals AB, Sweden

October 2005

Abstract

The overall objective of the TACO project has been to improve the knowledge on principles and best practices related to the traceability and communication of requirements in digital I&C systems development. On the basis of experiences in the Nordic countries, the project has aimed at identifying 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 through the different design phases. It is expected that the project will provide important input to the development of guidelines and establishment of recommended practices related to these activities.

The report provides a summary of the project activities and deliverables, discusses possible application areas, and provides a link to its utilization in the project “Management of Requirements in NPP Modernization Projects” (NKS_R_2005_47). In the preparation of the final report, a number of application areas have been identified where the TACO deliverables, first of all the TACO Shell and the TACO Traceability Model, can be utilized. The report aims at facilitating such utilization, by defining the context and main issues, explaining the main aspects of the deliverables, discussing the challenges experienced in the different application domains with respect requirements management, traceability and communication – and how can the TACO results contribute to solving these challenges.

Key words

Traceability, requirements, TACO, change management, digital I&C, systems development

NKS-115
ISBN 87-7893-176-2

Pitney Bowes Management Services Denmark A/S, 2005

The report can be obtained from
NKS Secretariat
NKS-775
P.O. Box 49
DK - 4000 Roskilde, Denmark

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

Traceability and Communication of Requirements in Digital I&C Systems Development
- Final Report -

Terje Sivertsen, Rune Fredriksen and Atoosa P-J Thunem
IFE

Jan-Erik Holmberg, Janne Valkonen, Olli Ventä
VTT

Jan-Ove Andersson
Ringhals AB

Foreword

This document constitutes the final report for the project “Traceability and Communication of Requirements in Digital I&C Systems Development” (NKS-R project number NKS_R_2002_16). The report provides a summary of the project activities and deliverables, discusses possible application areas, and provides a link to its utilization in the project “Management of Requirements in NPP Modernization Projects” (NKS_R_2005_47). In the preparation of the final report, a number of application areas have been identified where the TACO deliverables, first of all the TACO Shell and the TACO Traceability Model, can be utilized. The report aims at facilitating such utilization, by defining the context and main issues, explaining the main aspects of the deliverables, discussing the challenges experienced in the different application domains with respect requirements management, traceability and communication – and how can the TACO results contribute to solving these challenges.

Halden, June 2005

Terje Sivertsen

Table of contents

1. INTRODUCTION 7

2. MOTIVATION 8

2.1 BACKGROUND 8
2.2 OBJECTIVES 9

3. ACTIVITIES AND RESULTS 10

3.1 IDENTIFICATION OF THE MAIN ISSUES (2002) 11
3.1.1 The Preproject Report 12
3.2 FURTHER RESEARCH ON SELECTED MAIN ISSUES (2003) 13
3.2.1 The Project Report 2003 14
3.3 DEVELOPMENT OF THE TACO APPROACH (2004) 14
3.3.1 The Project Report 2004 16
3.4 PREPARATION OF INDUSTRIAL UTILIZATION (2005) 16
3.5 DISSEMINATION 17
3.5.1 1st TACO Industrial Seminar, Stockholm, Sweden, 12th of December 2003 17
3.5.2 Nordic Seminar on Automation, Oskarshamn, Sweden, 5th to 7th of April 2004 18
3.5.3 Enlarged Halden Programme Group Meeting, Sandefjord, Norway, 9th to 14th of May 2004 18
3.5.4 1st NKS-R Activity Leader Meeting, Helsinki, Finland, 19th of August 2004 19
3.5.5 NKS Workshop on Knowledge Management in Nordic NPPs, Halden, Norway, 7th to 8th of October 2004 19
3.5.6 2nd TACO Industrial Seminar, Helsinki, Finland, 8th of December 2004 19
3.5.7 NKS Seminar on Decommissioning of Nuclear Installations, Risø, Denmark, 13th to 15th of September 2005 20
3.5.8 SAFECOMP 2005, the 24th International Conference on Computer Safety, Reliability and Security, Fredrikstad, Norway, 28th to 30th of September 2005 20
3.5.9 Enlarged Halden Programme Group Meeting, Lillehammer, Norway, 16th to 21st of October 2005 21
3.5.10 Other Dissemination Activities 21

4. THE TACO APPROACH 22

4.1 THE TACO SHELL 22
4.2 THE TACO TRACEABILITY MODEL 22
4.3 UTILIZATION 26
4.4 TACO GUIDELINES 26
4.4.1 Validity of Requirements Changes 27
4.4.2 Formal Review and Test of Requirements 28
4.4.3 Correctness of Implementation 29
4.4.4 Requirements Understanding 30
4.4.5 Implementation 31

5. PROSPECTIVE APPLICATIONS 31

5.1 SAFETY DEMONSTRATION 31
5.2 ROLE OF SAFETY AND RISK ANALYSES IN REQUIREMENTS MANAGEMENT 32
5.3 DEFENCE-IN-DEPTH AND DIVERSITY ASSESSMENT 34
5.4 VALIDATING HUMAN-SYSTEM INTERFACES 35
5.4.1 Modelling 36
5.4.2 Data Collection 37
5.4.3 Data Analysis 37
5.4.4 Assessment Phase 38
5.5 SIMULATION-ASSISTED AUTOMATION TESTING 38
5.5.1 Background 38
5.5.2 Automation Delivery Project 38
5.5.3 Potential Uses of Simulation 39

5.6 FRAMEWORK OF PATTERNS 40
5.6.1 Background *40*
5.6.2 Objectives *40*
5.6.3 Utilization *41*
5.6.4 Risks *41*
5.6.5 Schedule *41*
5.7 CONFIGURABLE LIFE CYCLE MODELS 41
5.8 DECOMMISSIONING PROJECTS 42
5.9 KNOWLEDGE MANAGEMENT 43
5.10 PROCEDURES 44
5.11 ALARM SYSTEMS 46
5.12 MODEL BASED RISK ASSESSMENT 48
6. NEXT STEPS: MORE 50
6.1 BACKGROUND 50
6.2 GOALS AND RESULTS EXPECTED 51
6.3 UTILIZATION OF THE RESULTS 51
6.4 FIT TO NKS FRAMEWORK 52
7. REFERENCES 52
8. APPENDIX: PROJECT ORGANISATION 54

Abbreviations

API	Application program interface
CCF	Common cause failure
COPMA	Computerised Procedure System
COTS	Commercial off-the-shelf
D3	Defence-in-depth and diversity
DCS	Digital control system
EHPG	Enlarged Halden Programme Group
FAT	Factory acceptance test
I&C	Instrumentation & Control
IAEA	International Atomic Energy Agency
IEC	International Electrotechnical Commission
IEEE	The Institute of Electrical and Electronics Engineers
IFE	Institute for energy technology
MBRA	Model-based risk assessment
MORE	Management of Requirements in NPP Modernization Projects
NEA	Nuclear Energy Agency
NKS	Nordic nuclear safety research
NPP	Nuclear power plant
OECD	Organisation for Economic Co-operation and Development
PIE	Postulated initiating event
PLC	Programmable logic controller
PSA	Probabilistic safety assessment
SAT	Site acceptance test
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
TLX	Task Load Index
TVO	Teollisuuden Voima Oy
UML	Unified Modeling Language
VTT	Technical Research Centre of Finland
XML	Extensible Markup Language

Summary

The title of the reported project is “Traceability and Communication of Requirements in Digital I&C Systems Development”, abbreviated TACO. The NKS project number is NKS_R_2002_16. The present report is the final report from the project.

The overall objective of the TACO project has been to improve the knowledge on principles and best practices related to the issues concretised in the preproject. On the basis of experiences in the Nordic countries, the project has aimed at identifying 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 through the different design phases. It is expected that the project will provide important input to the development of guidelines and establishment of recommended practices related to these activities.

The overall aim of the preproject, which was carried out in the second half of 2002, was to identify the main issues related to traceability and communication of requirements in digital I&C systems development. By focusing on the identification of main issues, the preproject provided a basis for prioritising further work, while at the same time providing some initial recommendations related to these issues. The establishment of a Nordic expert network within the subject was another important result of the preproject.

The project activities in 2003 constituted a natural continuation of the preproject, and focused on the technical issues concretised in the preproject report. The work concentrated on four central and related issues, viz.

- Representation of requirements origins
- Traceability techniques
- Configuration management and the traceability of requirements
- Identification and categorisation of system aspects and their models

The results from the preproject and the activities in 2003 were presented at the first TACO Industrial Seminar, which took place in Stockholm on the 12th of December 2003. The seminar was hosted by SKI.

In 2004, the work focused on providing a unified exposition on the issues studied and thereby facilitating a common approach to requirements handling, from their origins and through the different development phases. Emphasis was put on the development of the TACO Traceability Model. The model supports understandability, communication and traceability by providing a common basis, in the form of a requirements change history, for different kinds of analysis and presentation of different requirements perspectives. Traceability is facilitated through the representation of requirements changes in terms of a change history tree built up by composition of instances of a number of change types, and by providing analysis on the basis of this representation. Much of the strength of the TACO Traceability Model is that it aims at forming the logic needed for formalising the activities related to change management and hence their further automation.

The work was presented at the second TACO Industrial Seminar, which took place in Helsinki on the 8th of December 2004. The seminar was hosted by STUK.

On basis of previous TACO work and responses received at the first and second TACO Industrial Seminar, the activity in 2005 has concentrated on producing the final report of the TACO project and making preparations for industrial utilization of the research results. The TACO project was scheduled for completion on the 30th of June 2005.

To facilitate the utilization of the results from the TACO project, a follow-up activity MORE (Management of Requirements in NPP Modernization Projects, NKS_R_2005_47), was scheduled for initiation on the 1st of July 2005. The MORE project will aim at the industrial utilisation of results from the TACO project. The proposed new activity will build on and add to the results from the TACO project. The overall objective of MORE is to improve the means for managing the large amounts of evolving requirements in Nordic NPP modernization projects. On basis of compiled experiences on the problem of handling large amounts of information in relation to Nordic modernization projects, the MORE project will investigate how the approach to requirements management developed in the TACO project can be utilised to handle large amounts of evolving requirements in NPP modernization projects.

1. Introduction

The title of the reported project is “Traceability and Communication of Requirements in Digital I&C Systems Development”, abbreviated TACO. The NKS project number is NKS_R_2002_16.

The present report is the final report from the TACO project, and summarizes both the achievements and a set of prospective applications. The TACO project has been carried out through a combination of project meetings, coordinated preparation of annual reports, industrial seminars, and other dissemination activities. Each year’s activities have been documented in separate reports, viz. the preproject report, the project reports from 2003 and 2004, and the present, final report. This documentation is extended through the presentations and papers prepared to meetings, workshops, seminars, and conferences. This includes a peer-reviewed paper accepted for presentation and publication at the Safecomp 2005 conference. Together, the documentation of the TACO project facilitates wide dissemination of the research results, to the intended audience.

In the preparation of the present report, particular concern has been given to the identification of potential applications of the TACO deliverables. As a result, the report includes a discussion on a variety of problem areas and how these deliverables, first of all the TACO Shell and the TACO Traceability Model, can be utilized.

Chapter 2 summarizes the background and objectives of the TACO project, partly by emphasizing the importance of clear, complete and stable requirements and the demands this puts on the systems development.

Chapter 3 provides short summaries from each year’s activities and documented results, including the industrial seminars and other dissemination activities.

Chapter 4 presents the TACO common approach to requirements handling, called the TACO Shell, intended as a framework for traceability and communication of requirements.

Chapter 5 introduces prospective applications and possible follow-up activities and topics for the future.

Chapter 6 gives information on the project MORE (Management of Requirements in NPP Modernization Projects, NKS_R_2005_47), aiming at the industrial utilisation of results from the TACO project.

The appendix gives a brief overview of the project organisation and activities.

2. Motivation

Several cases from the nuclear industry indicate the importance of clear, complete, and stable requirements from the beginning of the system development project. Since the safety of digital I&C is a property of the system in which it is embedded, the requirements specification also plays an important role in the safety assessment. In the development of NPP digital I&C systems, it is important to be able to trace the requirements backwards to the safety analysis report and forwards to the implementation (for development and quality control). A practical problem in this context relates to large amounts of documentation that must be read, and on this basis producing a requirements specification of the safety automation systems. An important research task is therefore to identify, develop, or improve techniques that simplify this process.

These and related concerns motivated the initiation of the TACO project, and have provided guidance to three years of Nordic collaborative research within the NKS-R programme. In the following subsections, more details on the background and objectives of the TACO project are provided.

2.1 Background

The system requirements specification collects the functional and non-functional aspects[1] of a system, and is a result of cooperation between the stakeholders of the system. The importance of clear, complete and stable requirements, and their role in the safety assessment, put demands on several phases of the system development, including requirements elicitation, specification and assessment, design, and implementation:

- Due to the high costs associated with defects slipping through the requirements specification phase, formal review and test of the requirements documents are usually highly prioritised activities. Industrial experience shows that very often a significant fraction of the most critical software defects are introduced already in the requirements specification. Of this reason, it is generally recommended to carry out tests on this specification that are as exhaustive as possible, and for this purpose, the use of a formal approach is often advocated.

- While the requirements assessment provides an important basis for systems development, it is also essential that the development ensures traceability to these requirements. The production of code that can be demonstrated to be a correct implementation of the software requirements is therefore also a major issue. In particular, the use of automated techniques for analysis and code generation can significantly reduce the intermediate levels between specification and implementation.

- In the ongoing modernisation NPPs, much effort has been put on data collection on the existing I&C system and elicitation of the original design basis of the plant. The challenge is partly to handle large amounts of documents and partly to harmonize old and new requirements.

[1] In a traditional software engineering perspective, a program is written to provide functions specified in its functional requirements specification. Non-functional requirements are those that do not pertain to the functions of the system, such as performance and scalability [2].

- The most critical area of requirements is related to safety and reliability. It is difficult to license computer-based systems in the highest safety class, e.g., COTS (commercial-off-the-shelf) products are hardly accepted in safety-critical applications. It is also difficult to verify reliability requirements, which can be compensated by a diversified solution. A challenge is to build up the demonstration of safety by linking the requirements, claims and evidence together.

- Safety classification of functions, systems and equipment is decisive for the set of requirements to be applied. Classification can be seen as a method to cost-effectively select an appropriate set of requirements. From a traceability point of view, the justification of the safety class is then the key information.

- To apply standards and regulations is useful and often an accepted way to manage requirements. Main standards and regulations are provided by international organisations (e.g., IEC, IEEE, IAEA) and safety authorities. The applicant needs to select and interpret the standards to follow. Standards are thus key reference material for the requirements database.

- Important challenges to requirements management and traceability are due to changes in software technology: How can graphical computerized methods be utilised in the software requirements definition? What are the possibilities and consequences of partial software modification and exchange? How are qualification and pre-qualification of software-based platforms and components managed? Can validated software be reused? Can off-the-shelf software be used? Can software components be certified?

- Vendors of I&C systems and devices, who operate internationally, need to readjust the requirements specification applied in the development of the product against the national regulatory requirements, when marketing or delivering the product to the utility. On the other side, the utility should in the pre-project phase keep the requirements specification open to several alternatives. In the commercial negotiations, these two sets of requirements specification meet. Ultimately, the utility is responsible for the fulfilment of safety requirements towards the regulatory body. The division of responsibilities between the utility and the vendor is, on the other hand, declared in the contract. The negotiations between vendor, utility and safety authority can be a major source of changes in the requirements specification, which need to be tracked by traceability methods.

In order to ensure correctness and understandability of the requirements assessment, it is essential to facilitate efficient communication between different parties involved, in particular between the customer (utility) and the vendor. This requires good decision-making practices and technical experience to be fused, and is basic to design and implementation of automation systems and programmable devices in general.

2.2 Objectives

The overall objective of the TACO project has been to improve the knowledge on principles and best practices related to the issues described above and concretised in the preproject. The project reviews practices related to:

- *The requirements elicitation process*: Best practices and most important criteria for ensuring effective communication leading up to the requirements specification. Sources of ambiguities, misunderstandings, inconsistencies and defects in these requirements, and how they can be eliminated or their impact reduced.

- *Requirements analysis*: Efficient communication between the experts performing the analysis, and the process experts. Demonstration that the requirements analysis correctly reflects the safety analysis of the plant and other relevant information.

- *Traceability of requirements*: Traceability of requirements from the requirements specification of the total system to the requirements of the computer system, and through the different phases of the total system's life cycle.

- *Understandability*: Effective means to make the requirements understandable to all parties, in particular when a high degree of formalization is employed.

Evidently, these aspects need to be studied in a larger context to ensure consistency with requirements to the completeness and analysability of the specifications, with the software development methods and lifecycle models employed, etc. The TACO project has contributed with information, knowledge, experiences and methods that can be utilized in the development of guidelines and recommended practices related to the elicitation and assessment of requirements, and for the traceability of these requirements through to a correct implementation.

3. Activities and Results

The TACO project has been carried out through a combination of project meetings, coordinated preparation of annual reports, industrial 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 concrete experiences from safety-critical applications. The discussions from the project meetings and industrial seminars, and the progress of the project, have been carefully reported by means of detailed minutes.

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

- January 2003: Preproject report (*completed*)
- December 12th, 2003: Presentations and materials to the first TACO Industrial Seminar (*completed*).
- January 5th, 2004: Documentation of the work for 2003 collected and sent in a suitable form to NKS (*completed*).
- April 5th, 2004: Presentations and materials to the Nordic Seminar on Automation (*completed*).
- December 2004: Presentations and materials to the second TACO Industrial Seminar (*completed*).
- January 5th, 2005: Documentation of the work for 2004 collected and sent in a suitable form to NKS (*completed*).
- June 30th, 2005: Final TACO project report (*the present report – completed*).

The project reports from 2003 and 2004 have been issued as the NKS-reports NKS-91 [13] and NKS-103 [15]. This documentation is extended through the presentations and papers prepared to meetings, workshops, seminars, and conferences. This includes a peer-reviewed paper accepted for presentation and publication at the Safecomp 2005 conference. Together, the documentation of the TACO project facilitates wide dissemination of the research results, to the intended audience.

In the following subsections, short summaries are given from each year's activities and documented results. Short résumés from the industrial seminars and other dissemination activities are given in a separate subsection. The TACO common approach to requirements handling, called the TACO Shell, is discussed in more detail in chapter 4.

3.1 Identification of the Main Issues (2002)

The TACO project was initiated with a preproject carried out in the second half of 2002. The overall aim of the preproject was to identify the main issues related to traceability and communication of requirements in digital I&C systems development. By focusing on the identification of main issues, the preproject provided a basis for prioritising further work, while at the same time providing some initial recommendations related to these issues. The establishment of a Nordic expert network within the subject was another important result of the preproject.

Many of the issues studied in the preproject related to requirements, their specification and engineering. In general, system requirements are capabilities that the system must supply or qualities it must possess in order to fit its intended use. In nuclear safety, the emphasis is on deriving the safety technical requirements traceably from the safety case documentation, standards, etc. In the development of NPP digital I&C systems, it is therefore important to be able to trace the requirements backwards to the safety analysis report and forwards to the implementation (for development and quality control). A practical problem in this context relates to the large amount of documentation that must be read, and on this basis producing a requirements specification of the safety automation systems. An important research task is therefore to identify, develop or improve techniques that simplify this process.

The preproject focused in particular on how traceability and communication could be improved through the use of appropriate techniques. Management of configurations and traceability are closely related, in particular with respect to the management of changes. In general, requirements traceability management should be a part of configuration management. As far as the communication of requirements is concerned, it is closely related to the understanding of the requirements. Difficulties in understanding the notation can be partly compensated for by integrating different levels and styles of description, including formal and informal, and by using some method for cross-referencing between the different requirements. From the above, it can be concluded that communication and traceability contribute to one another's improvement and are central aspects of requirements engineering.

An important part of requirements management is the management of changes. Typically, the requirements for a given 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. The task of managing changing requirements is closely related to requirements traceability. In fact, work on requirements traceability can to a certain extent be seen as a response to the need for keeping track of these changes. One benefit of traceability is the localization of side effects of a modification and the identification of relationships that must be reconfirmed, thereby increasing the assurance that when changes are needed they will be complete and consistent.

3.1.1 The Preproject Report

The preproject report presents the background and objectives to the project, discusses identified challenges and main issues related to the subject matter, and presents, like the subsequent project reports, details with regard to the project organisation, activities, and further plans. The purpose of the preproject report was first of all to provide a technical basis and plan for further work. Particular emphasis was put on relating knowledge on relevant software engineering issues to NPP needs and practice. In this sense, the challenges and issues identified in the report provided a basis and reference point for the more detailed discussions and evaluations to be carried out in the continuation of the project.

A brief overview of the preproject report is given in the following.

- *Introduction*: Introduction to the project, its background, and objectives. Emphasis is given on the need to review practices related to the requirements elicitation process, requirements analysis, traceability of requirements, and understandability.

- *Digital I&C Systems*: Classification of digital I&C systems, the different kinds of requirements and quality assurance aspects related to the development of these systems, and three targets of specific interest: safety automation, software in safety-critical devices, and user interfaces.

- *Requirements*: Important aspects of requirements, including their relationship to the Safety Analysis Report, their traceability, different means to facilitate their communication, components of their understandability, and finally completeness and analysis. Particular emphasis is given on traceability, which is basic to many of the requirements engineering activities discussed later in the report.

- *The System Requirements Specification*: The system requirements specification, the plant life cycles, the relationship between the customer, vendor and other system stakeholders, and finally the organisation of the requirements documentation into a system requirements definition document and a software requirements specification.

- *Requirements Engineering*: Important requirements engineering activities and processes, including requirements elicitation and analysis, design, implementation, development methods, lifecycle models, maintenance and decomposition.

- *Management*: Issues related to the managerial dimension of digital I&C systems development, including applicable standards and quality management models, and elements of requirements management.

- *Experiences*: Experiences from replacement projects in Swedish and Finnish nuclear power plants, and the possibility for transfer of knowledge and experiences from other industries.

- *Evaluation*: An approach to the evaluation of different requirements engineering methods and criteria for their successful use in NPP digital I&C systems development.

- *Regulators' Current Approach*: Regulators' current approach to the licensing of safety critical software for nuclear reactors.

- *Related Work*: Related work being performed by VTT, IFE, and the EU Framework Programme 5 projects CEMSIS (Cost Effective Modernisation of Systems Important to Safety) and BE-SECBS (Benchmark Exercise on Safety Evaluation of Computer-Based Systems).

3.2 Further Research on Selected Main Issues (2003)

The activities in 2003 constituted a natural continuation of the preproject, and focused on the technical issues concretised in the preproject report. The work concentrated on four central and related issues, viz.

- *Representation of requirements origins*: Ideally the requirements management is a process where requirements are elicited, analysed and specified from general ones towards implementation specific descriptions. During the life cycle of the plant or the system, various documents are extracted from the collection of requirements such as overall and detailed requirements specification, safety and reliability assessments, and plans for designated activities. From the knowledge management point of view, the core of the requirements management process is the requirements database where the requirements are stored in a structured way. There are several ways to build this structure. The project studied in particular an approach where three origins or points of views are represented, i.e. the user oriented, objective oriented, and plant oriented perspectives.

- *Traceability techniques*: The activities on traceability focused partly on identifying some basic concepts related to requirements traceability: definitions, tools and techniques – and how these can be used to facilitate traceability documentation and management. Of particular interest was the use of Topic Maps, which enable multiple, concurrent views of sets of information objects.

- *Configuration management and the traceability of requirements*: The activities on traceability also focused on the role of configuration management in ensuring traceability of requirements. In relation to these activities, a case study was initiated on the formal specification of fine-grained traceability, which in the 2004 activities was utilized in the establishment of the TACO Traceability Model.

- *Identification and categorisation of system aspects and their models*: The activities on system aspects focused on requirements engineering and management in general, and integration of systems engineering into (development) process engineering in particular. Due to the fact that knowledge on system aspects and their modelling has a crucial role in suggestions on traceability and communication of requirements in digital I&C systems development, previous efforts on modelling system aspects were refined and used.

The work was presented at the first TACO Industrial Seminar, which took place in Stockholm on the 12th of December 2003. The seminar was hosted by SKI (see section 3.5.1).

3.2.1 The Project Report 2003

The project report 2003 discusses the main issues covered in the project's research activities in 2003, and presents details with regard to the project organisation, activities, and further plans. The purpose of the report was to document the continued research work and related activities within the TACO project, including the First TACO Industrial Seminar (Stockholm, 12 December 2003). Particular emphasis was put on relating knowledge on relevant software engineering issues to NPP needs and practice. The report provided a basis and reference point for the work and activities to be carried out in the further continuation of the project, including the project's contribution to the Nordic Seminar on Nuclear Automation (Oskarshamn, 5th to 7th of April 2004) and the Second TACO Industrial Seminar (Helsinki, 8th of December 2004).

A brief overview of the project report 2003 is given in the following.

- *System aspects*: Systems aspects and their modelling, in particular with respect to the integration of systems engineering into (development) process engineering.

- *Requirements hierarchy*: Origins, views, and hierarchical structuring of the collection of requirements, and how this is related to the modelling of safety functions and related automation functions.

- *Life-cycle models – Presentation in TACO Industrial Seminar*: Requirements changes with respect to three different life-cycle models: The Waterfall model, the Incremental model, and the Spiral model.

- *Use cases in requirements elicitation*: *Use cases* and their application in requirements elicitation, with an emphasis on their potentials as a common method and language for developers, end users, and domain experts.

- *Requirements traceability*: Requirements traceability, its relationship to software configuration management, and the management of changes. A summary of the TACO case study on the formal specification of fine-grained requirements traceability.

The report also contains the minutes from the First TACO Industrial Seminar, arranged in the premises of SKI, 12th of December 2003.

3.3 Development of the TACO Approach (2004)

On basis of the activities in 2003 and responses received at the first TACO Industrial Seminar, the TACO activity in 2004 started by preparing a contribution to the Nordic Seminar on Automation, Oskarshamn, 5th to 7th of April 2004. The further activity focused on providing a unified exposition on the issues studied and thereby facilitating a common approach to requirements handling, from their origins and through the different development phases. Emphasis was put on the development of the TACO Traceability Model. The model supports understandability, communication and traceability by providing a common basis, in the form of a requirements change history, for different kinds of analysis and presentation of different requirements perspectives. Traceability is facilitated through the representation of requirements changes in terms of a change history tree built up by composition of instances of a number of change types, and by providing analysis on the basis of this representation. Much of the strength of the TACO Traceability Model is that it aims at forming the logic needed for formalizing the activities related to change management and hence their further automation.

The TACO common approach to requirements is represented by the concept of the TACO Shell (see Figure 1). The idea is that the shell is a framework for traceability and communication of requirements, which can be filled with different contents to reflect the needs in different application areas. To facilitate its practical use, the TACO Shell is provided with guidelines, comprising ingredients and recipes, for filling and utilizing the TACO Shell. The role of the TACO Traceability Model is to facilitate the representation of the introduction, changes, and relationships between requirements, design steps, implementations, documentation, etc. By complementing the model with appropriate terminology, data structures and guidelines for use, the model can be adapted to the different needs related to the management of changes in computer-based systems, including safety-critical and safety-related systems. By way of example, the model can organize communication and analysis of requirements by generating subsets of the change history showing the backwards and forwards traceability of given requirements. The TACO guidelines help to utilize these possibilities in practical work.

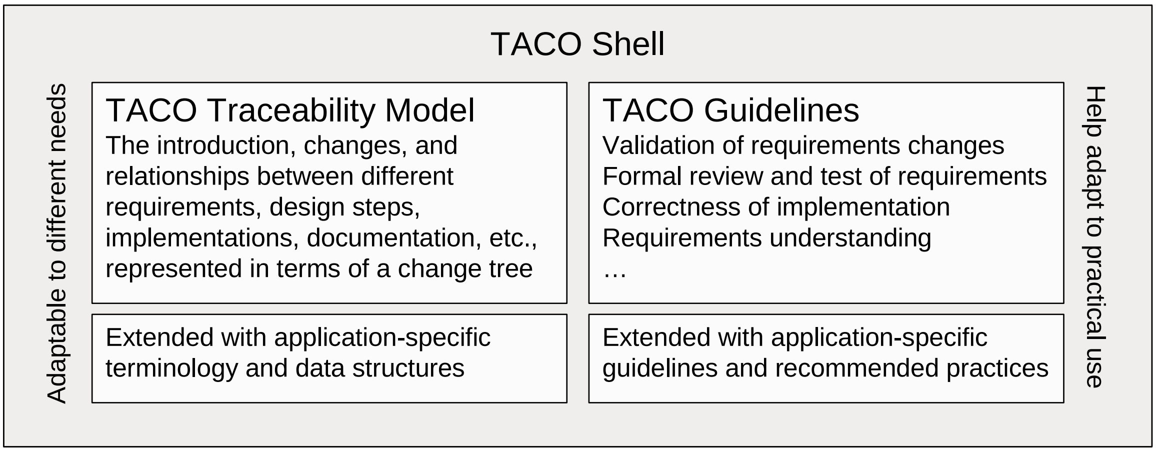

TACO Shell
Adaptable to different needs
TACO Traceability Model
The introduction, changes, and relationships between different requirements, design steps, implementations, documentation, etc., represented in terms of a change tree
TACO Guidelines
Validation of requirements changes
Formal review and test of requirements
Correctness of implementation
Requirements understanding
…
Extended with application-specific terminology and data structures
Extended with application-specific guidelines and recommended practices
Help adapt to practical use

Figure 1. The TACO Shell

By varying the ingredients and recipes, the TACO Shell can be used for the development of different kinds of target systems, with different requirements origins, different emphasis on quality attributes, and different selection of dependability factors. The TACO guidelines can be developed on a continual basis to fit the use, implementation, and verification of the different change types. The guidelines should include descriptions on how different techniques can be applied, such as the use of formal specification and proof for demonstrating the correct derivation of requirements, coding standards for implementation of specific design features, etc.

The TACO common approach to requirements handling is discussed in more detail in chapter 4.

The work was presented at the second TACO Industrial Seminar, which took place in Helsinki on the 8th of December 2004. The seminar was hosted by STUK.

3.3.1 The Project Report 2004

The project report 2004 discusses the main issues covered in the project's research activities in 2004, and presents details with regard to the project organisation, activities, and further plans. The purpose of the report was to document the continued research work and related activities within the TACO project, including the Second TACO Industrial Seminar (Helsinki, 8 December 2004). Particular emphasis was put on providing a unified exposition on the issues studied and thereby facilitating a common approach to requirements handling, from their origins and through the different development phases. Together with the preproject report and the project report for 2003, the report provided an adequate basis for the present final report of the TACO project.

A brief overview of the project report 2004 is given in the following.

- *Computer-based systems in nuclear power plants*: The general challenge of handling requirements of computer-based systems in nuclear power plants.

- *The TACO Common Approach to Requirements Handling*: The TACO common approach to requirements handling, called the *TACO Shell*. How the shell utilizes the *TACO Traceability Model* as a basis for communication and understanding of requirements, and how different aspects of requirements can be handled within this model.

- *TACO guidelines:* Guidelines to the practical use of the TACO Shell in activities related to the different lifecycle phases.

- *Mathematical underpinnings:* Mathematical underpinnings of the TACO Traceability Model in terms of an algebraic specification of the change history tree, the different change types, and different kinds of analysis that can be performed on basis of this representation.

The report also contains the minutes from the Second TACO Industrial Seminar, arranged in the premises of STUK, 8th of December 2004.

3.4 Preparation of Industrial Utilization (2005)

On basis of previous TACO work and responses received at the first and second TACO Industrial Seminar, the activity in 2005 concentrated on producing the final report of the TACO project and making preparations for industrial utilization of the research results. The TACO project was scheduled for completion on the 30th of June 2005.

In the preparation of the final report, particular concern was given to the identification of potential applications of the TACO deliverables. A number of application areas have been identified where these deliverables, first of all the TACO Shell and the TACO Traceability Model, can be utilized. An important goal has been to make it clear to the users, and to the readers of the report in general, how the different applications can utilize the results from the project. A question with respect to the applications is: What are the challenges from a requirements management, traceability and communication perspective – and how can the TACO results contribute to solving these challenges? Discussions on this are given in the report. Considering the large number of possible applications, it has also been attempted to put these into context, partly by refining the description of the background of the TACO project.

To facilitate the utilization of the results from the TACO project, a follow-up activity MORE (Management of Requirements in NPP Modernization Projects, NKS_R_2005_47), was scheduled for initiation on the 1st of July 2005. The MORE project will aim at the industrial utilisation of results from the TACO project. To facilitate a smooth start of the project, the initial planning has therefore been done as part of the 2005 activities of the TACO project. The proposed new activity will build on and add to the results from the TACO project. The overall objective of MORE is to improve the means for managing the large amounts of evolving requirements in Nordic NPP modernization projects. On basis of compiled experiences on the problem of handling large amounts of information in relation to Nordic modernization projects, the MORE project will investigate how the approach to requirements management developed in the TACO project can be utilised to handle large amounts of evolving requirements in NPP modernization projects.

3.5 Dissemination

The TACO project has been presented at a number of meetings in the Nordic countries, and is also scheduled for several presentations during the autumn 2005. These meetings include the TACO industrial seminars, other NKS seminars/meetings/workshops, Enlarged Halden Programme Group meetings, the OECD NEA/Halden Reactor Project Summer School, the Safecomp 2005 conference, IAEA technical meetings, and dissemination within Finnish nuclear regulatory research. The purpose of the different dissemination activities has been twofold; to present the TACO project and its deliverables, and to identify opportunities for industrial utilization. The different activities are briefly discussed below.

3.5.1 1st TACO Industrial Seminar, Stockholm, Sweden, 12th of December 2003

The intention with the First TACO Industrial Seminar was to present and discuss the work within the TACO project with a wider audience representing actors in the nuclear sector in the Nordic countries. In this way, the seminar would contribute to the dissemination of the research results to intended end-users, and also to providing input to further work within the project, reflecting priorities set by end-users. Background and questions for discussion were presented in the agenda.

The seminar had 15 participants from Finland, Norway, and Sweden, including the following organisations: Institute for energy technology, SKI, Ringhals AB, Forsmarks Kraftgrupp AB, Oskarshamn Kraftgrupp AB, VTT Industrial Systems, TVO, and Fortum.

In addition to an introductory overview of the TACO project, presentations were given on requirements traceability, requirements communications, understanding and analysis, and on requirements engineering and management. There were also presentations on regulatory aspects on software based safety systems and on requirements engineering and traceability within the MOD-project at Oskarshamn 1 NPP. The latter project involved the development of systems in all the classes A, B, and C, and hence with certain differences in how they were handled. An important basis for discussing and handling the requirements in the project was established through the subproject SCR (Safety Concept Report).

The following presentations were disseminated after the seminar: “TACO: Introduction”; “TACO: Requirements traceability”; “TACO: Requirements communication, understanding, and analysis”; “TACO: Requirements engineering and management - Integration between systems engineering and process engineering; “TACO: Requirements engineering and management - Requirements and life-cycle models - theory vs. practise”; “Requirements engineering and traceability within the Oskarshamn 1 - MOD-project”. In addition to slide sets, minutes of the seminar (included in [13]) were disseminated to the participants.

3.5.2 Nordic Seminar on Automation, Oskarshamn, Sweden, 5th to 7th of April 2004

The Nordic Seminar on Automation was hosted by The Nordic Nuclear Safety Research (NKS) and Oskarshamn Kraftgrupp AB and arranged in collaboration with the Technical Working Group on Nuclear Power Plant Control and Instrumentation of IAEA (TWG-NPPCI).

There were 85 experts and managers from Nordic countries and beyond, participating in open discussions between regulators, utilities, vendors and researchers. Presentations at the seminar covered the following issues:

- Modernisation of automation systems
- Replacement of equipment in automation and electrical systems
- Project (including quality) management
- Harmonisation of requirements on the plant, system and equipment levels
- I&C solutions for new nuclear power plants.

The TACO project seminar presentation consisted of an introduction to the project, results achieved so far, further activities, and some questions to the participating experts as a basis for discussion. The presentation also included a summary of the first TACO Industrial Seminar, covering the main topics and questions discussed.

TACO presentation slides were disseminated along with the seminar material.

3.5.3 Enlarged Halden Programme Group Meeting, Sandefjord, Norway, 9th to 14th of May 2004

The Enlarged Halden Programme Group (EHPG) meeting at Sandefjord was the 31st in a series of EHPG meetings arranged by the OECD Halden Reactor Project. The Sandefjord EHPG meeting was a good opportunity for the TACO project to introduce its results and to raise interest among the participants. In the sessions for the Man-Technology-Organisation (MTO) sector, more than sixty papers were presented along with fruitful conversations.

The TACO project was presented in the session under the topic “System safety and reliability”. To support the presentation, a paper [14] was prepared and included in the proceedings.

3.5.4 1st NKS-R Activity Leader Meeting, Helsinki, Finland, 19th of August 2004

The purpose of the first NKS-R Activity Leader meeting was to present the progress of the activities, discuss the remaining/future work, and to plan the possible continuations of the current activities in the Call for Proposals that started in mid-August 2004. The meeting comprised information given by the NKS-R Programme Management on the NKS-R program, the results of the Activity Leader inquiry, and the Call for Proposals 2005, as well as status reports and results given by the activity leaders of current NKS-R activities. This included a presentation on the TACO project, covering project background, objectives, and activities, as well as a brief overview of some of the main issues studied.

3.5.5 NKS Workshop on Knowledge Management in Nordic NPPs, Halden, Norway, 7th to 8th of October 2004

The workshop included a TACO-presentation with the title "The TACO Traceability Model – can it be used for KM?". The workshop found that the overall objective of the TACO project – to improve the knowledge on principles and best practices related to requirement traceability and communication – resembles the concerns related with adequate knowledge management:

- There is a knowledge elicitation process preceding the externalization of knowledge that should be handled in an appropriate manner.

- There is a need to be able to verify the knowledge thus capitalized.

- Not only requirements are dynamic, but most kinds of knowledge are dynamic and the evolution process should be controlled and documented.

- Finally, all kind of knowledge should be available in a form that helps apprehension. This close correspondence is not surprising, since requirements are just one type of knowledge.

With respect to utilizing the TACO results for knowledge management purposes, the project suggested to explore the applicability of the TACO shell and the TACO traceability model for general knowledge management, i.e. to see if they can be used to control the dynamic development of knowledge. For several reasons, the totality of applicable knowledge will be changing as time pass by. New knowledge will emerge, some of it replacing obsolete knowledge. Also erratic knowledge may also substantiate and later on there will be a need to retract to previously established knowledge.

The workshop discussions and conclusions are reported in a separate NKS-R report [8].

3.5.6 2nd TACO Industrial Seminar, Helsinki, Finland, 8th of December 2004

Similarly to the first seminar, the intention with the Second TACO Industrial Seminar was to present and discuss the work within the TACO project with a wider audience representing actors in the nuclear sector in the Nordic countries. In this way, the seminar would contribute to the dissemination of the research results to the intended end-users, and also to providing input to further work within the follow-up project MORE - Management of Requirements in NPP Modernization Projects.

The seminar had 20 participants from Finland, Norway, and Sweden, including the following organisations: Institute for energy technology, SKI, Ringhals AB, Oskarshamn Kraftgrupp AB, VTT Industrial Systems, VTT Processes, STUK, TVO, and Fortum.

In addition to introducing the TACO project and its achievements, TACO's relationship to other projects, the Finnish radiation and nuclear safety authority perspective, and safety I&C system reliability requirements were discussed.

The second part of the seminar included several simultaneous table discussions on the follow-up activities of TACO, industrial experiences, and requirements change management.

The following presentations were disseminated after the seminar: "TACO: Introduction"; "TACO: The TACO Common Approach to Requirements Management"; "Finnish Radiation and Nuclear Safety Authority perspective"; "Relationship to other activities"; "Safety I&C System Reliability Requirements - Verification - Life cycle". In addition to slide sets, minutes of the seminar (included in [15]) were disseminated to the participants.

3.5.7 NKS Seminar on Decommissioning of Nuclear Installations, Risø, Denmark, 13th to 15th of September 2005

The seminar is organised by NKS, with the Danish Decommissioning as co-organiser. The purpose of the seminar is to contribute to better understanding of and thus knowledge about decommissioning of nuclear power plants. The seminar aims also at establishing a Nordic network within the area of decommissioning. Finally, an important purpose is to collect suggestions for future NKS activities towards decommissioning of nuclear facilities. The seminar targets actors within the nuclear field as well as authorities and consultancy bodies. The seminar treats four topics:

1. National and international recommendations and requirements regarding decommissioning of nuclear facilities
2. The authorities' experiences with inspection of decommissioning activities
3. Decommissioning of nuclear facilities in Nordic countries and in Europe
4. R&D results

The seminar includes a visit to the test reactor of Risø, DR1, already subject to decommissioning, and some group work.

The participants/speakers so far represent major nuclear facilities, R&D environments and authorities from Denmark, Finland, Norway and Sweden.

3.5.8 SAFECOMP 2005, the 24th International Conference on Computer Safety, Reliability and Security, Fredrikstad, Norway, 28th to 30th of September 2005

Safecomp 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 focuses on dependability of critical computer applications and is a platform for knowledge and technology transfer between academia, industry and research institutions.

A TACO paper produced and submitted for presentation at the Safecomp 2005 conference was accepted by the conference programme committee. The paper and presentation, with the title “The TACO approach for traceability and communication of requirements” emphasises the main deliverable from the project, i.e. the TACO common approach to requirements handling – the TACO Shell – comprising the overall methodology, the TACO Traceability Model, and the different guidelines related to its contents and use.

3.5.9 Enlarged Halden Programme Group Meeting, Lillehammer, Norway, 16th to 21st of October 2005

The Enlarged Halden Programme Group (EHPG) meeting at Lillehammer will be the 32nd in a series of EHPG meetings arranged by the OECD Halden Reactor Project. The sessions related to the Man-Technology-Organisation (MTO) programme of the OECD Halden Reactor Project covers a number of items, including digital instrumentation and control systems in NPPs, dependable software systems, system aspects, quality assurance, risk assessment, etc.

One of the presentations at the Lillehammer EHPG meeting will have the title “TACO – a framework for traceability and communication of requirements”. The results of the project and prospective applications along with future plans will be introduced. Also the follow-up project MORE (Management of Requirements in NPP Modernization Projects, NKS_R_2005_47) will be introduced. The TACO project will be extended through the production of a Halden Work Report with the same title, summarizing the results from three years of activities in the project.

3.5.10 Other Dissemination Activities

In addition to the above, the following events are included in the dissemination plans for the TACO project:

- IAEA Technical Meeting on Impact of Modern Technology on Instrumentation and Control in Nuclear Power Plants, EDF R&D, Chatou, France, 13th to 15th of September 2005.

- International Summer School, OECD NEA – OECD Halden Reactor Project, Fredrikstad, Norway, 22nd to 27th of September 2005.

- IAEA Technical Meeting on Implementing and Licensing Digital I&C Systems and Equipment in NPPs, VTT Industrial Systems, Espoo, Finland, 22nd to 24th of November 2005.

- Dissemination within Finnish nuclear regulatory research.

4. The TACO Approach

The present chapter presents the TACO common approach to requirements handling, called the TACO Shell. For more details, the reader is referred to the project report 2004 [15].

The TACO shell is intended as a framework for traceability and communication of requirements which can be filled with different contents to reflect the needs in different application areas. To facilitate its practical use, the TACO Shell is provided with guidelines, comprising ingredients and recipes, for filling and utilizing the TACO Shell. The TACO approach to requirements change management is based on a mathematically well-founded traceability model, called the TACO Traceability Model, where the introduction, changes, and relationships between different requirements, design steps, implementations, documentation, etc. are represented in terms of an extended change history tree. The traceability model adopted aims at forming the logic needed for formalising the activities related to change management and hence their further automation. By complementing the model with appropriate terminology, data structures and guidelines for use, the model can be adapted to the different needs related to management of changes in computer-based systems, including safety-critical and security-critical systems.

4.1 The TACO Shell

The TACO Shell is the overall TACO framework for requirements handling, and represents a generic approach to lifecycle-oriented, traceability-based requirements management. The TACO Shell comprises the overall methodology, the TACO Traceability Model, and the different guidelines related to its contents (ingredients) and use (recipes). By varying the ingredients and recipes, the shell can be used for the development of different kinds of target systems, with different requirements origins, different emphasis on quality attributes, and different selection of dependability factors.

4.2 The TACO Traceability Model

The TACO Traceability Model adopts several of the ideas to fine-grained traceability presented in [7]. Accordingly, traceability is facilitated by representing the requirements changes in terms of a change history tree built up by composition of instances of seven different change types, and providing analysis on the basis of this representation. The change types correspond to the following generic actions performed on requirements, or more generally, paragraphs (from [7]):

- Creating a new paragraph with no prior history.
- Deleting an existing paragraph.
- Splitting an existing paragraph, thereby creating a number of new paragraphs.
- Combining existing paragraphs by a new paragraph.
- Replacing existing paragraphs by a new paragraph.
- Deriving a new paragraph from existing paragraphs.
- Modifying a paragraph without changing its meaning.

The change history can be represented by a tree where the paragraphs constitute the nodes. The tree representation constitutes an appropriate basis for different kinds of analysis, including finding

- all initial paragraphs;
- all deleted paragraphs;
- all applicable paragraphs;
- the complete history of a paragraph;
- the complete backwards traceability from a set of paragraphs;
- the complete forwards traceability from a set of paragraphs;
- the legality of a proposed requirements change.

The possibility to find the backwards or forwards traceability from a set of requirements facilitates backwards and forwards branch isolation and analysis of the change history. The versatility of the representation can be further improved by extending the representation of the paragraphs to include different parameters that classify the requirements, provide additional information, etc. Possible parameters are discussed later in the report.

When it comes to the representation of the actual parameters, it is important to distinguish between (1) the information that is essential to identify the paragraph, and (2) the various information associated to this parameter. Conceptually, and from a perspective of modularity, it is useful to let the nodes in the change history tree represent the necessary and sufficient information related to the identity of a paragraph. In the TACO Traceability Model, a paragraph is represented by the combination of a unique identifier for this paragraph and a version number to distinguish several versions of the same paragraph. At any time, only the latest version of a paragraph can be an applicable paragraph. That is, a new version of a paragraph is introduced only if this replaces old versions. In any case, it is possible to make duplicates of a paragraph when these are treated as different paragraphs. This can also be used for representing different variants of the same requirement, possibly with “application conditions” attached as guidelines to every single variant. Each variant will however be represented with a separate paragraph.

It is important to note that concepts similar to those described above for the TACO Traceability Model can be found in commercial tools for version control and configuration management. Although the change types might have other names, they typically resemble those defined here. In general, however, these tools do not offer an identifiable, formally defined traceability model, and leave to the user to define the actual semantics underlying the different change types. The strength of the TACO Traceability Model is that it aims at forming the logic needed for formalising the activities related to change management and hence their further automation.

Conceptually, we can think of a node of the change history tree as a versioned paragraph, represented by a pair of a paragraph identifier and a version number. In the following we will use the change history in Figure 1 as an example.

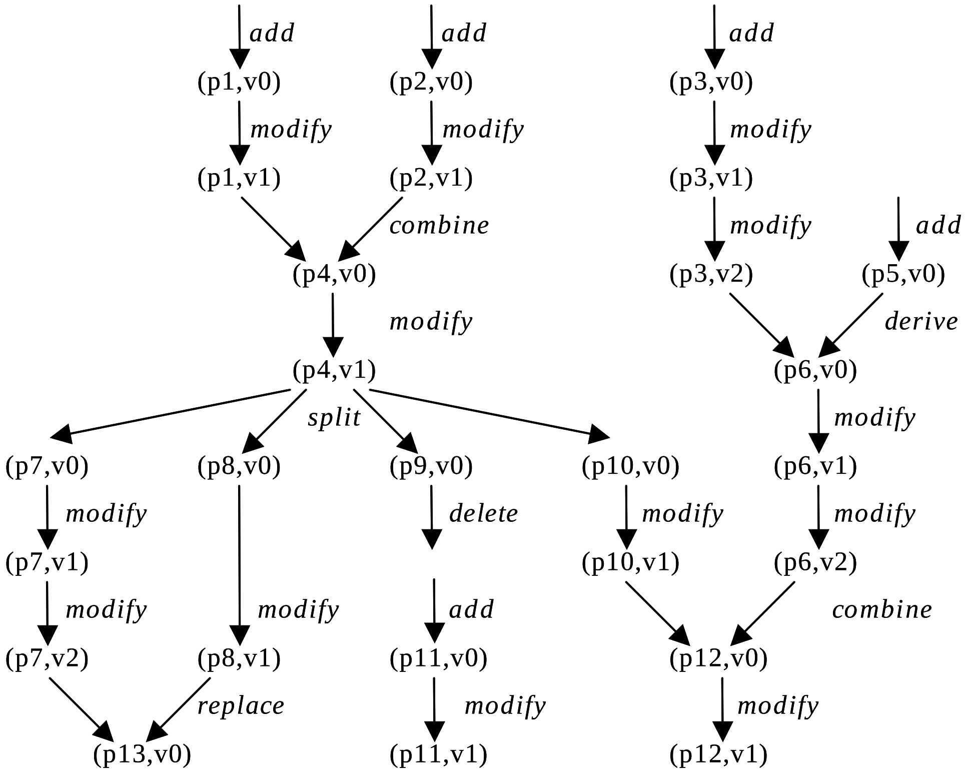


Figure 2. The example change history.

The development of the requirements in Figure 1 starts with the introduction of the paragraphs p1, p2, and p3. At later stages, another two new paragraphs are introduced, viz. p5 and p11. All the other paragraphs are developed on basis of these five paragraphs. Paragraphs p1 and p2 are first modified and then combined into a new paragraph p4. After a modification, this paragraph is split into four separate paragraphs p7 to p10. The latter of these paragraphs is modified and then combined with p6, originally derived from paragraphs p3 and p5, giving paragraph p12. Note that, at any point in the development of the paragraphs, at most one version of a paragraph is applicable (in the sense that it is the valid version of the paragraph). It is certainly possible to represent the change history tree textually in such a way that the temporal relationships between the different changes are maintained.

Let us now consider the other information attached to a paragraph. As has been argued in the foregoing, it is not necessary to represent this information in the change history tree. The purpose of the tree is to give a complete representation of the changes and how they are related to each other. What about the other information, including the actual text of the paragraph? Formally, we can think of these relations in terms of some basic mathematical concepts:

- *Sets*: These are finite collections of objects of some type, and can be used for representing subsets of the paragraphs. By way of example, the classification of paragraphs with respect to Business plan, Requirements document, Design specification, etc, can be represented by means of separate, maybe overlapping sets corresponding to the different classification terms. Finding, say, all Business plan related requirements is then trivial, since they are given by the corresponding set. Checking whether a requirement belongs to the Business plan is also easy and can be done simply by checking whether the given paragraph is a member of the corresponding set. On the other hand, finding the class of a given paragraph cannot be done by simple look-up but involves checking all the different sets for membership.

- *Mappings*: These are functions from a source set to a target set, and can be used for assigning information to the paragraphs in a simple look-up fashion. With this solution, e.g. the classification of paragraphs can be represented by mappings from the paragraphs to their classification. Finding the classification of a requirement is then simple, since it reduces to looking up the classification of that requirement. Finding all requirements is possible, but less trivial than for sets, as it involves selecting all requirements that are mapped to a certain term. On the other hand, the concept of relation is more convenient if there may be more than one class for a requirement.

- *Relations*: These are more general than mappings, since they allow an element in the source set to be associated to more than one element in the target set. With this solution, finding the classification of a requirement involves finding all elements in the target set (the classes) that are related to the given requirement. Finding all requirements related to a certain class can alternatively be understood as the inverse relation.

Sets can be considered as being implemented as simple lists. Mappings and relations can be considered as being implemented as tables. As we will see in the continued discussion, these representation concepts will suffice for representing all information associated to the requirements. It is of course possible to represent the same information in other ways as well, as long as consistency is maintained.

A basic piece of information related to a requirement is certainly the statement (phrasing) of the requirement. Assuming that (at most) one statement is associated to each requirement, we may think of this information as being available by means of a mapping from versioned requirements to their statements, see Table 1.

Requirement	**Statement**
(p1,v0)	<Statement of version v0 of paragraph p1>
(p1,v1)	<Statement of version v1 of paragraph p1>
(p2,v0)	<Statement of version v0 of paragraph p2>
...	...
(p13,v0)	<Statement of version v0 of paragraph p13>

Table 1. Mapping from requirements to their statements.

As is evident from Table 1, the statement of a given requirement can be found by simple look-up in the table implementing the mapping. The table can be utilized in different ways. By way of example, finding all relevant requirements can be found by filtering the mapping with respect to the applicable paragraphs to find the subset of the mapping that relates to applicable paragraphs only. Filling in the relevant information is an obvious task of an information system designed to support the use of the model.

Other useful information can be represented in the same way. By way of example, a recurrent problem with modernization projects is the difficulties of recapturing both the “what” and the “why” of a requirement. In the TACO Traceability Model, the “what” is covered by Table 1. In a similar way, the “why” of the requirements can be covered by a similar mapping from requirements to comments giving information on the background, motivation, reasons, etc. for including the requirements.

4.3 Utilization

A possible utilization of the TACO Traceability Model is in the identification of relative influences, correlations, and conflicts between safety/security countermeasures and other dependability factors. On this basis, guidelines to the use, implementation, and verification of the different change types can be developed. These guidelines would have to reflect the identified relative influences, correlations, and conflicts in the sense that they provide a better basis for controlling the effects of changes. The guidelines should include descriptions on how different techniques can be applied for this purpose, such as the use of formal specification and proof for demonstrating the correct derivation of requirements, coding standards for implementation of specific design features, etc.

The utilization and applicability of the TACO Traceability Model will be further explored and documented by cooperation with other projects and partners. The results will be collected within the framework of the Nordic project MORE (Management of Requirements in NPP Modernization Projects).

4.4 TACO Guidelines

The TACO project aims at providing input to the development of guidelines and establishment of recommended practices related to requirements elicitation and analysis, understandability of requirements to all parties, and traceability of requirements through the different design phases. In this section, guidelines will be presented to the practical use of the TACO Shell in activities related to the different lifecycle phases. The guidelines can be seen as comprising *ingredients* and *recipes* for filling and utilizing the TACO Shell. By gradually complementing the TACO Shell and the TACO Traceability Model with appropriate terminology, data structures and guidelines for use, the model can be adapted to the different needs related to management of changes in computer-based systems, including safety-critical and security-critical systems. By way of example, the model can organize communication and analysis of requirements by generating subsets of the change history showing the backwards or forwards traceability of given requirements. The TACO guidelines help to utilize these possibilities in practical work.

By varying the ingredients and recipes, the TACO Shell can be used for the development of different kinds of target systems, with different requirements origins, different emphasis on quality attributes, and different selection of dependability factors. The TACO guidelines can be developed on a continual basis to fit the use, implementation, and verification of the different change types. The guidelines should include descriptions on how different techniques can be applied, such as the use of formal specification and proof for demonstrating the correct derivation of requirements, coding standards for implementation of specific design features, etc.

The mathematical underpinnings of the TACO Traceability Model is described in the project report 2004 [15] in terms of a functional specification of the change history tree, the different change types and different kinds of analysis that can be performed on basis of this representation. The TACO Traceability Model is specified in two layers, reflected in a hierarchy of two specifications. In the "lower" specification, the different change types are specified inductively as generators, thus providing a data structure for the change history. At the top of this specification, the different change types are specified as operators, checking that the given change is legal and producing a lower layer representation together with the set of applicable paragraphs. By applying these operators, only legal change histories are represented.

4.4.1 Validity of Requirements Changes

Software development needs to deal with changes to the requirements, also after the requirements specification phase ideally is completed and the requirements frozen. The evolutionary nature of software implies that changes will have to be anticipated. Other changes may be necessary due to our evolving understanding about the application under development.

One of the lessons learned in the software engineering area is that software should be designed for change. The focus in the present report is on how to manage the evolution of the requirements in this situation. The present section deals with how the TACO Traceability Model can be utilized in the validation of the changes representing this evolution.

The TACO Traceability Model is based on a number of change types that can be employed to manage requirements changes throughout the life cycle of a system. Each change introduced in the life cycle should in principle be validated. Depending on the level of rigidity or formality employed, the validity of a change can be done in a variety of ways, from a simple inspection to a formal mathematical proof. Notwithstanding these differences, we will in the following concentrate on what validity in general means for the different change types. Validity should not be confused with the legality of changes. While validation concerns the semantics of the changes, the legality of a change can be checked mechanically from the structure of the change history tree.

Creating: Applied on requirements, creating a new paragraph with no prior history involves introducing a new requirement. The validity of the requirement involves both its *correctness* with respect to its intended meaning, its *completeness* with respect to its coverage of its intended meaning, and its *consistency* with other requirements. In short, the validity of a new requirement requires that it faithfully reflects the intended meaning and that it is not in conflict with other requirements. This is the only change type that is allowed to introduce new requirements or new aspects of requirements that are not already covered by existing paragraphs.

Deleting: Deleting an existing paragraph involves that a requirement in fact is withdrawn from the set of requirements. A requirement can be deleted if either the requirement in itself is no longer valid, or it is covered by other requirements. To demonstrate the validity of the change therefore either involves showing that it is the intention to withdraw the requirement as such or showing that it can be derived from other requirements.

Splitting: Splitting an existing paragraph involves creating a number of new paragraphs that collectively replaces the given one. Applied on requirements, a paragraph split is valid only if the requirements given in the new paragraphs together cover the replaced requirement, but not more. In other words, splitting a paragraph is not valid if the new paragraphs require more or less than the replaced paragraph.

Combining: Combining a set of existing paragraphs involves creating a new paragraph on basis of the existing ones, without deleting any of the existing paragraphs. Applied on requirements, a combination of paragraphs is valid only if the new paragraph covers the given paragraphs, but not more. In other words, combining a set of paragraphs is not valid if the new paragraph requires more or less than the given paragraphs.

Replacing: Replacing a set of existing paragraphs involves creating a new paragraph that replaces the existing ones. The validity criterion is identical to that of combination. Replacing a set of paragraphs and splitting an existing paragraph are inverse changes.

Deriving: Deriving a new paragraph from a set of existing paragraphs involves creating a new paragraph on the basis of the existing ones, without deleting any of the existing paragraphs. Applied on requirements, deriving a new paragraph is valid only if the requirement is *one* of the possible results/consequences of the requirements it is derived from.

Modifying: Modifying a paragraph should involve no changes to its meaning. The new requirement should therefore cover the replaced requirement, but not more.

Attempts on demonstrating the validity of individual changes may reveal flaws in the requirements management, such as introducing new paragraphs in a paragraph split that actually adds new requirements that are not covered by the replaced requirement. Detecting such flaws can be utilized in the requirements change process to produce an appropriate requirements change history, such as specifying such added requirements in terms of separate changes of type *creating new paragraphs with no prior history*. Similarly, insufficient coverage of the replaced requirement in a split change can be made “clean” by complementing the split with separate changes of type *deleting an existing paragraph*. In this way, an invalid change can be replaced by a set of valid changes, and the need for demonstrating the validity of the different changes can be made explicit.

4.4.2 Formal Review and Test of Requirements

Due to the high costs associated with defects slipping through the requirements specification phase, formal review and test of the requirements documents are usually highly prioritised activities. Industrial experience shows that very often a significant fraction of the most critical software defects are introduced already in the requirements specification. Of this reason, it is generally recommended to carry out tests on this specification that are as near as exhaustive as possible, and for this purpose, the use of a formal approach is often advocated.

Requirements analysis and requirements validation have much in common, but the latter type of activity is more concerned with checking a final draft of the requirements document which includes all system requirements and where known incompleteness and inconsistency has been removed, see [5]. As such, it should be planned and scheduled in the quality plan for the project, and be carried out in accordance with good quality assurance practice.

One of the theses behind the present report is that the TACO Traceability Model can be used for revealing and correcting several kinds of shortcomings discovered during the validation of the requirements document. This is true in particular for problems related to lack of conformance with the standards employed. The validation of the requirements against a given standards can be carried out by utilizing the information included about the origins of the requirements.

Such a validation could include the following steps:

1. Add all the requirements from the given standard by creating new paragraphs. If certain requirements are found irrelevant, the exclusion of these can be made explicit by deleting these paragraphs. This also makes explicit the need to validate their exclusion.

2. Check that the applicable and deleted paragraphs together constitute the complete set of requirements given in the standard. This can partly be automated by keeping these requirements on file.

3. Validate the change history related to the applicable paragraphs originating from the standard, utilizing the guidelines listed in section 3.1.

4. Validate the deletion of paragraphs originating from the standard, utilizing the guidelines listed in section 3.1.

Using the TACO Traceability Model in validating the requirements document may be done in the context of a formal requirements review meetings, in accordance with general guidelines to such meetings. Requirements validation may also take other forms, like prototyping, model validation, and requirements testing, but the focus in the TACO project has been on the utilization of the requirements change history in the review meetings. For further reading on formal review meetings, see [5].

Requirements reviews are conventionally carried out as a formal meeting involving a group representing the stakeholders. The general idea is that the system stakeholders, requirements engineers and system designers together check the requirements to verify that the requirements adequately describe the system to be implemented. Traceability and requirements changes are of course only part of the concern at such a meeting. The TACO Traceability Model may however provide important assistance for discovering requirements problems related to requirements conflicts or lack of conformance to standards and other requirements origins.

In the end, the requirements traceability is itself a concern of the requirements review. As discussed in [5], the requirements should be unambiguously identified, include links to related requirements and to the reasons why these requirements have been included. Furthermore, there should be a clear link between software requirements and more general systems engineering requirements. This relates to the obvious fact that the software engineering activity is part of the much larger systems development process in which the requirements of the software are balanced against the requirements of other parts of the system being developed [2]. Furthermore, the software requirements are usually developed from the more general system requirements, and thus the traceability and consistency with these requirements is a basic premise for a successful process and its resulting product.

4.4.3 Correctness of Implementation

The correctness of implementation is a quality that characterizes the ability of the application to perform its function as expected [2]. Reasoning about correctness therefore requires the availability of the functional requirements, and we say that the application is functionally correct if it behaves according to the specification of these requirements.

In principle, correctness is in this context a mathematical property that establishes the equivalence between the software and its specification. In practice, the assessment of correctness is done in a more or less systematic manner, depending on how rigorously the requirements are specified and the software developed. In any case, the assessment requires that the requirements can be traced forward to their implementation, and vice versa.

The TACO Traceability Model supports the assessment of correctness by relating the requirements and their implementation through the change history tree. This relationship can be utilized in both a forwards and backwards fashion. The TACO shell provides both forwards and backwards traceability analysis, without requiring separate links for forwards and backwards traceability. The different types of analysis can be defined on the basis of one and the same representation of the change history tree.

In general, a forward traceability approach to assessment of correctness would take the specified requirements as starting point, and then demonstrate that all the requirements have been correctly implemented. Analogously, a backward traceability approach would take the implementation as starting point and check the consistency with the requirements. Of these two, the forward approach probably fits better with respect to a conventional approach to correctness assessment.

In practice, using the TACO Traceability Model for assessment of functional correctness can be done in terms of the following steps.

1. For each requirement introduced, indicate whether it is a functional requirement. This can be done by means of mappings.

2. For each implementation of a requirement, indicate - by means of mappings - that it is an implementation.

3. For each functional requirement introduced, check that the forward traceability leads up to an implementation of this requirement. This can be done by:

4. For each functional requirement, check that the requirement is correctly implemented by validating the sequence of changes leading from the requirement to its implementation.

4.4.4 Requirements Understanding

One important aspect of the requirements understandability relates to the understanding of the interface between the application to be developed and its external environment (such as the physical plant). This requires that the software engineers understand the application domain and communicate well with the different stakeholders. To facilitate this communication, it might be necessary to specify the requirements in accordance with the different viewpoints the stakeholders have to the system, where each viewpoint provides a partial view of what the system is expected to provide. As a consequence, the requirements specification will cover different views on the same system, giving an additional dimension to the question of consistency between the different requirements. An important task of the software engineers is to integrate and reconcile the different views in such a way that contradictions are revealed and corrected.

In order to cope with the complexity of the resulting set of requirements, it is advisable to classify and document the requirements in accordance with the views they represent. This way of separating the concerns can provide a horizontal, modular structure to the requirements. Modularity provides several benefits in the requirements engineering process, including the capability to understand the system in terms of its pieces. This first of all relates to the fact that modularity allows separation of concerns, both with respect to the different views represented by the different stakeholders' expectations to the system and to different levels of abstraction. This makes it easier for the different stakeholders to verify their requirements, while at the same time providing a means for handling the complexity of the full set of requirements. The TACO Traceability Model can be adopted to facilitate this separation of concerns by relating requirements to the views they reflect. This can be utilized in different kinds of analysis of the requirements throughout the development of the system.

Some of the stakeholders may be unable to read the types of specifications preferred by the software engineers or mandated for the application. In such cases, the needs of the different stakeholders can be reconciled by providing (horizontal) traceability links between the, possibly formal, specifications used by the software engineers and more informal, natural language based expression of the same requirements. One could even consider providing links between the requirements and the user manual within the same traceability model. This could be utilized both for communication purposes and for the purpose of developing the user manual in parallel to the engineering of the requirements, which in some cases may be a recommended practice.

4.4.5 Implementation

The TACO Guidelines can be implemented in a variety of commercial or non-commercial tools extending the tools' capabilities by supporting relationship to diverse requirements sources in a formalized way and not only support the software development process from the specified requirements.

5. Prospective Applications

This chapter introduces prospective applications and possible follow-up activities and topics for the future. A number of application areas are identified where these deliverables, first of all the TACO Shell and the TACO Traceability Model, can be utilized. The exposition aims at indicating how the different applications can utilize the results from the project. A question with respect to the applications is: What are the challenges from a requirements management, traceability and communication perspective – and how can the TACO results contribute to solving these challenges? Discussions on this are given in this chapter. The MORE project, which will aim at the industrial utilisation of results from the TACO project, is discussed in chapter 6.

5.1 Safety Demonstration

A fundamental purpose of requirements managements is to support the demonstration of safety of the plant. The overall safety demonstration is an intricate task involving technical dimension (plant-system-equipment), organisational dimension (stakeholders of the plant), time dimension (life cycle), and methodological dimension (approaches, analyses, assessments, activities to be performed). It is a process where the utility must have confidence in itself and in the vendor's ability and equipment, and where it can transform this confidence to the authority.

Figure 3 presents an overview of elements of a safety demonstration in a construction or modernisation project. Seen from a requirements analysis point of view, basic requirements for the part of the plant under consideration (e.g. automation system) are derived from the design basis of the plant and plant operation. The safety and risk assessments form the basis for determining the safety importance of different automation systems. The implementation of the safety demonstration is divided into three areas: demonstration of technical design features, quality management of the implementation project and consideration of system operation and life cycle [10].

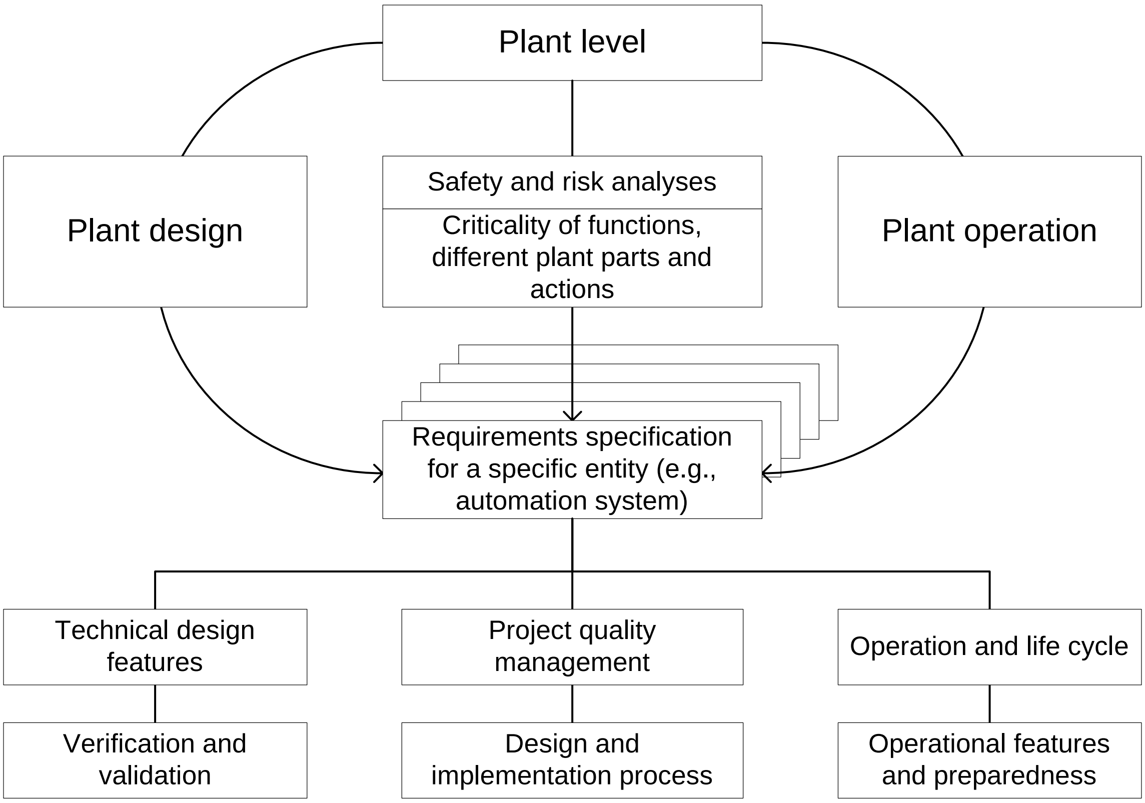

Plant level
Plant design
Safety and risk analyses
Criticality of functions, different plant parts and actions
Plant operation
Requirements specification for a specific entity (e.g., automation system)
Technical design features
Project quality management
Operation and life cycle
Verification and validation
Design and implementation process
Operational features and preparedness

Figure 3. Safety demonstration framework [10].

5.2 Role of Safety and Risk Analyses in Requirements Management

In safety-critical environments and applications, the safety and risk analyses play a central role in the specification of requirements. Analytical methods like probabilistic safety assessment (PSA) are needed to interpret, identify and define, first of all, the overall level of criticality of the plant and, secondly, the criticality of the particular part of the plant under consideration (e.g. a subsystem to be modified).

Figure 4 illustrates an ideal picture of the analysis flow starting from scratch, i.e., the concept of the plant, continuing down to smallest manageable detail, i.e., purchasable object. In parallel to detailed design, the safety assessments go into details and requirements are specified. Analogically to the V-model, the verification process goes into the opposite direction. The lowest block in the diagram refers to the situation at operating power plants. There is an ongoing process to improve the operation and design of the plant, which leads to repeated plant modification projects and corresponding requirements management tasks.

The important traceability links presented in

Figure 4 are 1) horizontally between the requirements specification and plant safety analysis and 2) vertically between the different levels of, not only requirements specification, but also between the different levels of plant safety analysis.

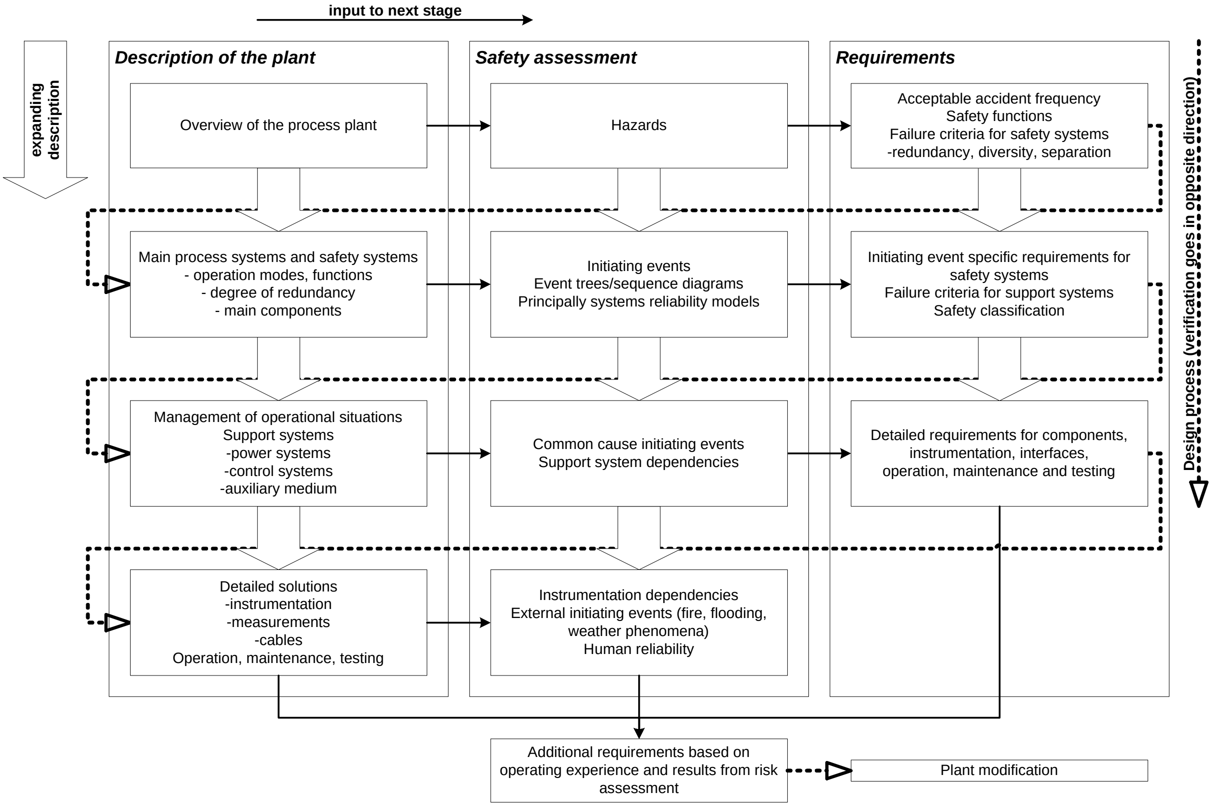

input to next stage
expanding description
Description of the plant
Safety assessment
Requirements
Overview of the process plant
Hazards
Acceptable accident frequency
Safety functions
Failure criteria for safety systems
-redundancy, diversity, separation
Main process systems and safety systems
- operation modes, functions
- degree of redundancy
- main components
Initiating events
Event trees/sequence diagrams
Principally systems reliability models
Initiating event specific requirements for safety systems
Failure criteria for support systems
Safety classification
Management of operational situations
Support systems
-power systems
-control systems
-auxiliary medium
Common cause initiating events
Support system dependencies
Detailed requirements for components, instrumentation, interfaces, operation, maintenance and testing
Detailed solutions
-instrumentation
-measurements
-cables
Operation, maintenance, testing
Instrumentation dependencies
External initiating events (fire, flooding, weather phenomena)
Human reliability
Additional requirements based on operating experience and results from risk assessment
Plant modification
Design process (verification goes in opposite direction)

Figure 4. Hierarchical structure and analysis flow between description of plant description, safety assessment and requirements analysis. From left to right: safety assessment is based on description of the plant and safety requirements are based on a safety assessment of the plant. From top to down: the specification of each description takes place stepwise. Verification of fulfilment of requirements goes in opposite direction. For an operating plant, the requirements management process is ongoing and iterative due to new findings based on operating experience and safety analyses, as well as due to ageing of systems and development of new technical solutions.

5.3 Defence-in-depth and Diversity Assessment

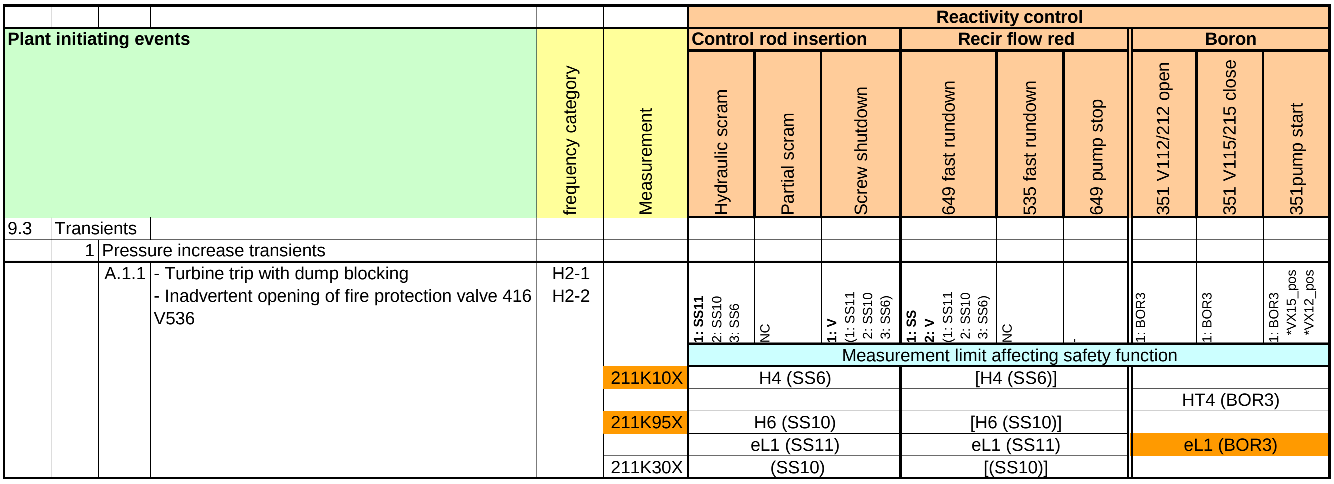
The defence-in-depth strategy presumes that every aspect of the plant's safety includes several levels of protection [4]. These levels of safety functions are meant to either prevent or mitigate accidents; or both. In this way no single human or component failure will lead to harm to the public, and even combinations of failures that are extremely rare would lead to little or no harm. From an automation point of view, the strategy means a requirement to separate automation functions into:

- normal operation control functions;
- preventive functions;
- safety functions;
- diverse safety functions (for high risk scenarios); and
- accident management functions.

The above list of function categories can be regarded as successive barriers that can react in a plant disturbance. If the functions are accomplished by different systems and in particular with different technical solution, the probability of a severe accident is minimal provided that each function is reasonably reliable. In fact, the designer can to some extent make trade-offs between the reliability of a single system and the number of successive system barriers protecting the plant. However, the plant processes are complex and there are interdependencies between systems so that without a systematic analysis, it is impossible to demonstrate the safety level of the plant. Further, an analysis and related decision making criteria are needed for the above mentioned trade-off considerations. The crucial thing is, not the reliability of a single automation system, but the level of independence (or dependence) between automation systems responsible for different barrier functions. Therefore the most interesting reliability requirements concern with the probability of a common cause failure, i.e., a failure which is the result of one or more events, causing coincident failures of two or more separate channels in a multiple channel system, leading to a system failure [IEC 61508].

Figure 5 illustrates how I&C functions can be analysed in order to identify dependencies between them. For safety demonstration purposes, the entire signal processing path from the sensors to the actuators needs to be considered. Such an analysis must be made for all thinkable plant initiating events. The frequency and potential consequences of the initiating event determines whether preventive functions, safety functions, diverse safety functions or accident management functions are required. In this example, a survey was made of primary and back-up safety functions available in different PIEs (functional diversity) fulfilling a safety function and of available activation signals of process components in a safety system (system diversity). The defence-in-depth and diversity features of systems were evaluated using numerical indexes that express, in the simplest form, the number of barriers: 1 = one barrier function, 2 = two barrier functions, etc.

The defence-in-depth and diversity assessment is valuable input for the safety classification of I&C systems and their equipment. Consequently, it provides the basis not only for the system and equipment requirements but also for intersystem independence requirements, and it forms a traceability link between system and function level requirements. It should be noted that, in reality, to show independence between two software products (from a CCF risk point of view) can be a difficult task.



						Reactivity control								
Plant initiating events						Control rod insertion			Recir flow red			Boron		
				frequency category	Measurement	Hydraulic scram	Partial scram	Screw shutdown	649 fast rundown	535 fast rundown	649 pump stop	351 V112/212 open	351 V115/215 close	351pump start
9.3	Transients													
	1	Pressure increase transients												
		A.1.1	- Turbine trip with dump blocking - Inadvertent opening of fire protection valve 416 V536	H2-1 H2-2		**1: SS11** 2: SS10 3: SS6	NC	**1: V** (1: SS11 2: SS10 3: SS6)	**1: SS** **2: V** (1: SS11 2: SS10 3: SS6)	NC	-	1: BOR3	1: BOR3	1: BOR3 *VX15_pos *VX12_pos
						Measurement limit affecting safety function								
					211K10X	H4 (SS6)			[H4 (SS6)]					
												HT4 (BOR3)		
					211K95X	H6 (SS10)			[H6 (SS10)]					
						eL1 (SS11)			eL1 (SS11)			eL1 (BOR3)		
					211K30X	(SS10)			[(SS10)]					

Figure 5. A method to analyse defence-in-depth and diversity features of automation systems. An example from Olkiluoto 1/2 nuclear power plant. For each initiating event, the responsible safety functions and related I&C functions are defined. Red marked blocks (here dark grey) indicate system functions that lack diversification [9].

5.4 Validating Human-System Interfaces

The trend to employ ever more digital control systems in NPP automation addresses the issues of human-system interaction as a central part of safety demonstration. What seems to be available today for industry is a selection of standards and guidelines that provide vast lists of issues that should be covered in system evaluation. An extensive study is underway at VTT, in a growing cooperation with, e.g., the OECD Halden Reactor Project, to develop a new framework for the evaluation of the usability of complex information and control systems. The current status of the framework is described below. A more comprehensive description can be found in [11]. The framework combines effectively and consistently the essential elements of requirements for both design and validation together with the actual validation stages leading to final assessment of system usability.

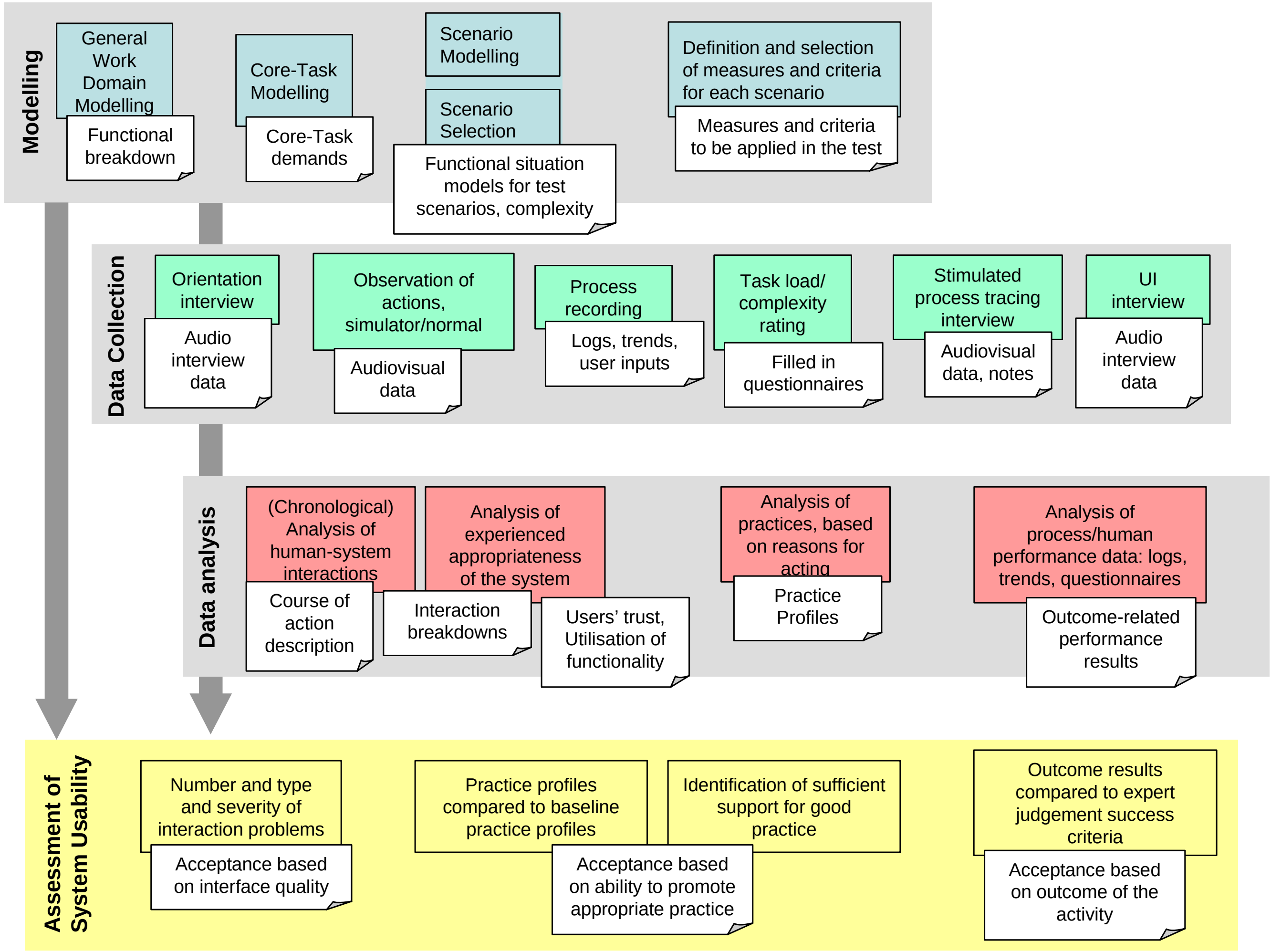

Modelling
General Work Domain Modelling
Functional breakdown
Core-Task Modelling
Core-Task demands
Scenario Modelling
Scenario Selection
Functional situation models for test scenarios, complexity
Definition and selection of measures and criteria for each scenario
Measures and criteria to be applied in the test
Data Collection
Orientation interview
Audio interview data
Observation of actions, simulator/normal
Audiovisual data
Process recording
Logs, trends, user inputs
Task load/ complexity rating
Filled in questionnaires
Stimulated process tracing interview
Audiovisual data, notes
UI interview
Audio interview data
Data analysis
(Chronological) Analysis of human-system interactions
Course of action description
Analysis of experienced appropriateness of the system
Interaction breakdowns
Users' trust, Utilisation of functionality
Analysis of practices, based on reasons for acting
Practice Profiles
Analysis of process/human performance data: logs, trends, questionnaires
Outcome-related performance results
Assessment of System Usability
Number and type and severity of interaction problems
Acceptance based on interface quality
Practice profiles compared to baseline practice profiles
Identification of sufficient support for good practice
Acceptance based on ability to promote appropriate practice
Outcome results compared to expert judgement success criteria
Acceptance based on outcome of the activity

Figure 6. A framework for the evaluation of the usability of complex information and control systems.

The process view of the framework is depicted in Figure 6. The activities and their results (deliverables) are briefly described below.

5.4.1 Modelling

Functional Domain Modelling (FDM): Functional domain modelling produces a functional breakdown of the system, on a general level.

Core-Task Modelling: Produces a similar deliverable to the FDM but the functions are modelled from an operative perspective. Core-task model denotes what is the essential content of a particular work, what are the demands on the worker and what are the contradictions between the different demands that the workers have to balance between.

Functional Situation Models (FSM) and Scenario Selection: In the functional situation modelling, the domain models are given a situational meaning. The functional situation model is constructed chronologically and it thus provides the sequence of process phases taking place during the particular scenario.

Establishment of Performance Indicators and Acceptance Criteria: An activity to establish performance indicators for the selected scenarios.

5.4.2 Data Collection

Evaluation is conducted in full-scale simulator conditions but may be organised also in real work environments. The users in an evaluation session are normal NPP operators. No further expertise should be required from the test users.

Orientation interview: In the beginning of the evaluation session some basic information is gathered from the users. The aim of the orientation interview is to define the users' work orientations so that they can be taken account of when the users' practices in the tasks are analysed.

Observation of Human-System Interaction: The simulator run is carried out as any other simulator run in the operator training process. The users follow their standard procedures and operate the plant as they are instructed. The data collection is conducted with many different tools.

Task Load and Complexity Measurement: After the completion of the scenario, the operators are presented with the TLX (Task Load Index) measurement questionnaire.

Stimulated Process Tracing Interview: In the process tracing interviews the main phases of the simulation are discussed through together with the users. The aim of the de-briefing is to find out what events did the users consider most important in the simulator run, and what kind of information did they use to handle these events.

User Interface Interview.

5.4.3 Data Analysis

Analysis of Human-System Interactions: Analysis of the human system interactions during the scenario is carried out with course of action analysis. The description of the *courses of action* consists of a sequential-temporal representation of the operator-process and operator-operator interactions as perception action cycles. Data from de-briefing *process-tracing interviews* are primary in structuring the course of action in meaningful phases.

Work practice analysis: In this methodology operator practices are analysed and evaluated with regard to two aspects of practices situational and habitual. The situative aspect refers to the particular actualisation of operator performance which we have called course of action. The habitual aspect refers to the dispositional features that are identifiable in the actualisation in a reason-based analysis orienting to reveal the significance or meaning of these actions.

Analysis of Process Data: Primary information source for the analysis of process data are the logs and trends gathered during the simulated scenario.

Analysis of Human Performance Data: The task load data is manipulated according to the NASA-TLX method [3].

5.4.4 Assessment Phase

The assessment phase is the part of the human factors evaluation in which the acquired results are compared to the acceptance criteria. This is done for all the categories of performance data collected and analysed in the tests.

5.5 Simulation-assisted Automation Testing

The contents of this section have been adapted from [6].

5.5.1 Background

Requirements of the automation system delivery are tightening. The organisations involved in the delivery should achieve even higher productivity without compromising the quality of the automation system. The testing of the automation system has an essential role when aiming at these goals. However extensive testing of the automation system is challenging. Automation systems are wide and they are tightly coupled to the process, and all information required is available only at the time of the installation. In traditional testing the functionality of the process is emulated using signal generators and automation system modules. To get more realistic process responses including all interdependencies a simulator is a very attractive alternative.

Computation power has rocketed in relation to the price: modern PC's are capable of running plant-wide models in real time. PC-based DCS and PLC emulation software products, also known as virtual automation systems, have been released, with basic simulation features (start/stop/save/load). Industrial standardisation efforts have produced a number of de-facto standards for plug-and-play co-use of simulation and automation software by different providers.

The technology is now being taken up in the industry. During recent years, pilot projects have been carried out using various tools and technologies with promising results. Involving simulators in various phases of NPP modernization or new-build projects seems to be very Scandinavian! This is due to the strong culture of continuous improvement, both in nuclear industry and the respective research.

5.5.2 Automation Delivery Project

Independently of the working practices used in testing, an automation delivery project can be divided in following phases:

1. *Specification*: The end-user specifies the requirements for the new automation system. The choice may be open between several possible automation suppliers.

2. *Design*: The end-user and the automation supplier resolve how the requirements will be met on the selected automation product.

3. *Implementation*: Involves the configuration and/or programming of the automation applications. The phase ends in the Factory Acceptance Test (FAT).

4. *Installation*: The automation hardware and software are delivered and installed to the site. The phase ends in the Site Acceptance Test (SAT).

5. *Commissioning*: Involves the trial runs: cold commissioning and hot commissioning. After the commissioning phase, the plant is taken over by the end-user.

6. *Validation*: The system is evaluated by the end-user and possibly authorities.

7. *Operation*.

5.5.3 Potential Uses of Simulation

Evaluation of automation design: Simulation-assisted evaluation of automation design should be carried out as early in the project as possible. Simulation sequences can be made for evaluating system performance with alternative automation designs. The testing of cross-dependencies and overall system behaviour must be carried out interactively by domain experts.

Evaluation of process design: As processes become faster, the process and automation designs become more iterative and more integrated. The use of dynamic simulation to evaluate alternative process designs can be seen highly beneficial.

Validation of system requirements: Simulation can be used for improving the understanding, what are realistic expectations from the performance of the system, and what are justified limits for alarms and protection logics. For validating the requirements, automatic simulation sequences can well be used in case the criteria for the validity of each requirement are easy to specify. The runs can later be re-used in the comparing of automation products and in verification of system implementation.

Comparing automation products: The testing system can be used for running pilot-scale tests using different automation products.

Verification of automation implementation: Simulation-assisted automation factory acceptance test is generally regarded to have a great potential benefit. Changes made before installation are far less expensive than changes made to a system after installation.

Tuning of automation parameters: Simulation models can be used for pre-tuning of automation parameters. It may be beneficial to tune the automation in both the specification phase, using a simulation model of the automation, and in the implementation phase, using virtual automation.

Tuning and validation of process models.

Estimating system reliability: Simulation can be used for estimating the reliability of the automation application. A set of test cases that correspond to the operational profile are specified and executed. Instead of finding errors, the aim is to demonstrate that the system has the expected degree of reliability.

Verification of operator instructions: The testing tool can send both operator events to the automation system and process events to the simulation model.

Design and Validation of Human-System Interaction: see above.

Testing automation and simulation products at version release: At version change of any system software component, the behaviour of the entire system should remain the same, or the change should be justified. Therefore, the testing environment can be used for testing automation and simulation products at version release.

5.6 Framework of Patterns

This section describes shortly a follow-up activity, which will be in close relation with the MORE project. The intention is not to implement the described framework within the MORE project but to maintain relations and discussions with it while trying to find points of co-operation and mutual benefits.

5.6.1 Background

The rapid development of information technology has increased the number of different working methods used in the industry. In spite of the continuous research and introduction of alternative ways of thinking, there are still many fields where the advances of new IT-driven methods have not been fully applied. An example of this is the lack of utilisation of advanced software development methods in justifying the safety and dependability of computer based systems. From the designer’s point-of-view, there are no generally accepted methodologies for quality management, qualification and licensing procedures. The plan described below concerns mainly design and development of safety critical systems and software, and quality procedures and analysis.

5.6.2 Objectives

The objective of the research is to create a general framework enabling the development of patterns that take safety and dependability issues into account. The basis for patterns will be well-described requirements and source information. At this relation, the concept of pattern must be understood extensively, i.e. a pattern is a solution or guidelines to a frequently occurring problem or situation in a certain context. Patterns of this type have been seldom, if ever, applied systematically in automation application design and even far less in safety critical automation.

Another objective of the research is to extend the concept of patterns to deal with testing, quality management, fault-tolerance, and formal qualification / licensing of safety critical industrial applications. In addition, the claim-evidence technology[2] [1] will be considered and possibly combined with creating patterns.

[2] In general, claim is a demand for something due or believed to be due. In this context the word claim concerns properties of the behaviour of the system implementation and properties of the interactions of the implementation with the environment. In real life, stakeholders of the system do not talk about claims before dealing with licensing the system for a given usage, or before dealing with regulators, safety authorities or their technical support organisations, or before submitting the system to independent assessment.

5.6.3 Utilization

One utilization method of the results would be enabling public, open, and critical discussion and consensus about which solutions or procedures are good and which are not so good. Because problem solving is usually based on already existing solutions and the process is rarely started from the scratch, why don't do it in a structured way and share the information? That way there would be good possibilities to start a positive spin of improving design, qualification and licensing solutions in general and involve more stakeholders to take part in it.

The results of the research will be utilised in assessing the safety and dependability of industrial applications and in designing these kinds of applications.

5.6.4 Risks

One of the biggest risks of such research activity is the lack of source data and real life examples to be utilized in the pattern framework development. To minimize that risk, the TACO/MORE network will be contacted in order to get a reasonable amount of good quality data. Before that, the topic and area of the research must be defined more accurately and there must be a clear vision of what kinds of data and assistance are really needed.

5.6.5 Schedule

The activity described above has already been started within the TACO project group and it will be continued along with the MORE project. The results will be published in various contexts as the research goes on.

5.7 Configurable Life Cycle Models

Usually, the development of large and complex computerised systems used at nuclear facilities is carried out following a standard development process. Whether the process is the V, spiral or RUP life cycle model, its focus has traditionally been on functionality and safety factors. Furthermore, the experiences indicate that safety factors are themselves often defined on the basis of functionality, availability and performance of the constructed system. Taking into account other dependability requirements such as modifiability, reusability, mobility and security, and their influence on the safety requirements, have not been the concern of available development processes, also called life cycle models. Additionally, all these models are of generic nature, including many elements for each development phase that are not necessarily equally important for all projects.

As the importance of dependability requirements for complex systems differs from one project to another, and as the awareness about accounting for various and sometimes contradictory dependability factors becomes more and more crucial in especially the modernisation projects at nuclear facilities, there is a need for configurable life cycle models that are not universal and the same for all development or modernisation projects, but appear custom-made for each single project.

A selective and custom-made integration of dependability factors into a life cycle model can only be accomplished through a comprehensive and systematic approach involving:

1. The establishment of criteria for specification and categorisation of dependability requirements (including functionality requirements) in accordance with all dependability factors relevant for projects at nuclear facilities.

2. The actual specification and categorisation of the dependability requirements based on not only past and current experiences, but also the advances within information and communication technologies imposing new requirements to modern computerised systems.

3. Application of traceability techniques for the management of changing dependability requirements integrated into the configurable life cycle model (thus, also defining the criteria for the reusable elements and development patterns among different "shapes" of the configurable life cycle model).

4. Application of traceability techniques for the management of changing phases, disciplines and iterations for the configurable life cycle model (e.g. a particular discipline or a part of it during the development process can be omitted due to the nature of the project in focus).

The findings of the TACO project and in particular the TACO traceability model will be employed and further developed to accomplish the objective described above, in terms of the activities during the MORE project.

To be valid and trustworthy, the development of a configurable life cycle model will be highly depending on the real-life examples and practical experiences from development and modernisation projects at nuclear power plants, and further maturity of the TACO traceability model. The latter will in particular involve the semantic aspects of the traceability model, i.e., the further development of the model's features for describing relationships between different requirements, hence their classifications, and on that basis describing the relationships between classes of requirements.

5.8 Decommissioning Projects

Decommissioning consists of administrative and technical actions taken to allow the removal of some or all of the regulatory controls from a nuclear facility. The use of the term "decommissioning" implies that no further use of the facility for its existing purpose is foreseen. The actions taken in decommissioning must ensure the protection of the work force and long-term protection of the public and environment, and typically include reducing levels of residual radionuclide so that material and buildings can be safely released and reused. Decommissioning activities also create radioactive waste which needs to be appropriately managed so that the public is protected from the associated radiation hazards. A large number of nuclear facilities worldwide will ultimately require decommissioning. They range from large nuclear power reactors and complex reprocessing plants to small research laboratories and manufacturing plants. The decommissioning tasks for nuclear facilities can include large-scale decontamination, and destruction of massive concrete structures.

The decommissioning tasks can present many safety challenges and before a decommissioning programme is started, these challenges must be anticipated, evaluated and given satisfactory solutions. In all cases, the decommissioning tasks must be well planned and arrangements must be made to ensure that sufficient resources will be available when needed. Without proper arrangements being made for decommissioning, the facilities subject to shut-down could eventually constitute a radiological hazard to the public and environment in their vicinity.

The above indicates that decommissioning activities constitute a complex life-cycle process, with clear and comprehensive requirements associated with each single activity during the process. The activities can be roughly grouped to relate to the following major topics:

- Project management in a safety culture
- Operational safety
- Decommissioning technologies
- Nuclear engineering systems
- Environmental decision making
- Environmental quality standards

To illustrate, activities related to operational safety can include studying and complying to safety standards, preparing safety cases, specifying safety requirements, continuous safety auditing, assessing the risks involved, and managing legal liability and operating licences. Equally, activities within decommissioning technologies can comprise defining strategies for effective decommissioning (together with planning and economics), investigating and choosing techniques for material cutting and waste minimization, evaluating human exposure and the related protection procedures, assessing and deciding the usage degrees of manual techniques and robotic systems (together with their integration and control), and choosing suitable User Interface (UI) techniques, amongst others, relevant for interacting with the robotics systems.

It is evident that the traceability and communication of requirements established, perhaps altered and finally frozen for each of the activities mentioned, is as essential as for those associated with the construction process of nuclear facilities. The TACO traceability model can therefore be specialised for decommissioning projects, and include facilities for definition, classification and change management of requirements related to decommissioning activities.

5.9 Knowledge Management

The NKS Workshop on Knowledge Management in Nordic NPPs (see section 3.5.5) included a presentation and discussions on how TACO can be utilized for knowledge management. The present section is based on material from the workshop report [8].

For some time, there has been a growing interest in and attentiveness to this field, which eventually has also gained some recognition by the NPP community worldwide. Organisations like IAEA and NEA have defined activities that address issues relevant to the field, and many national research institutes and singular utilities have defined activities of their own.

The reasons for this shift in interest are probably several. However, one of the most important reasons is possibly the concern for knowledge attrition. By and by the competence of the staff will be worn down, sometimes because it is not used but more often because employees either quit or retire. Retirement has become a serious problem in many parts of the world due to the general age profile of NPP staff. This is a critical problem that needs to be dealt with before it becomes too late.

The deregulation of the electricity market is probably another contributing factor. It has created harsher market conditions, which makes it increasingly harder for the single utility to prevail. Knowledge management offers solutions that help companies acquire, preserve and reuse knowledge more efficiently.

With respect to utilizing the TACO results for knowledge management purposes, applicability of the TACO shell and the TACO traceability model for general knowledge management could be explored to see if they can be used to control the dynamic development of knowledge. For several reasons, the totality of applicable knowledge will be changing as time pass by. New knowledge will emerge, some of it replacing obsolete knowledge. Also erratic knowledge may substantiate and later on there will be a need to retract to previously established knowledge.

The applicability of TACO in this field relates partly to the question how knowledge management can facilitate effective communication between people of different background and expertise. In the TACO project, this issue has been addressed in relation to communication in the different requirements management activities. In a requirement/design situation it is often needed that end users communicate with designers. To facilitate this communication, the TACO project suggests introduction of different kinds of perspectives on the same knowledge. This may imply a translation process that will use a dictionary to translate problems formulations belonging to one perspective into the vocabulary of another perspective. It may be a particular challenge to keep the two views consistent. One example is when constructing operation procedures from other types of technical documentation. This extracts the technical information and the implications so that they can be more readily applicable by the operators. Since there is a manual construction, there may be a possibility that the two views on the process may become inconsistent or outdated. More efficient knowledge management would address this maintenance and reusability problem.

5.10 Procedures

NPP plant procedures classify into a series of different categories ranging from highly safety relevant procedures to procedures establishing conditions resulting in a more efficient operation of the plant. Common to the construction of all such procedures is the dependency on the design and construction of the plant itself and other systems supporting the operation of the plant. This means that design decisions taken for other parts must be communicated to the people responsible for procedure construction and maintenance. For example, safety relevant procedures are closely related to requirements such as those described in section 5.2. The safety assessment implemented as part of this process should make procedures a part of their analysis. Safety related procedures will provide an extra barrier to the loss of critical safety functions. The iterative process described in 5.2 will eventually lead up to some proposed plant adjustment. The three phases (description of the plant, safety analysis, requirements development) bring about elements that should be influential also on the content of the procedures. In other words, a procedure must reflect the actual plant components and adjustment of the plant itself must in some cases lead to procedure changes. Thus, the development of the ‘TACO paragraphs’ should not only be associated with the development of safety automation systems but also new versions of the individual plant procedures.

Other classes of procedures will have similar connections to plant construction details. In general, the procedure life-cycle must be coordinated with the life-cycle of the plant and other support systems associated with the plant.

The Halden Project's COPMA project has for an extended period of time investigated the use of computerized procedure handling. Recently there has been a shift of focus from execution of the procedure to the maintenance of the procedures. Integration of diverse information sources (such as plant component databases and requirement specification databases such as TACO/MORE) makes it possible to coordinate and reinforce the procedure maintenance activity.

The COPMA project has this far developed a demo that uses an information coupling to the plant database. There are plans for trying to interface with the TACO tool once the tool is available and provided the needed features are part of the system. The remainder of this section will deal with the expected functionality of such an integration as well as the expected benefits.

The current COPMA based procedure maintenance demo relies on a versioning paradigm where the hierarchical levels of the procedure (such as step and instruction) are associated with revision numbering. One advantage of this approach is that it is easy to extract the latest version of the procedure, or any selected version, by issuing simple query commands to the database. Also the revision history of e.g. an instruction can easily be extracted and presented to the staff that is maintaining the procedures. Still, there is information not provided. The content of a procedure is often a result of requirements that concerns a more complex selection of procedure elements, not necessarily related to the hierarchical procedure. In reference to the discussion above concerning requirements to the critical safety function implementation, there is an obvious need to relate requirements of a general nature to other requirements of a more specific nature and eventually link over to procedures that are part of the in-depth prevention of the critical safety functions.

This principle is illustrated in Figure 7 for the maintenance of critical function preserving procedures. The requirement construction related work processes has been taken out from the model used in section 5.2. There is an association between additional procedure requirements to the procedure-independent plant description and the requirements to the safety automation system. Finally there is an association across the boundaries of the TACO and COPMA tools system providing the link between the procedure details and the associated requirements.

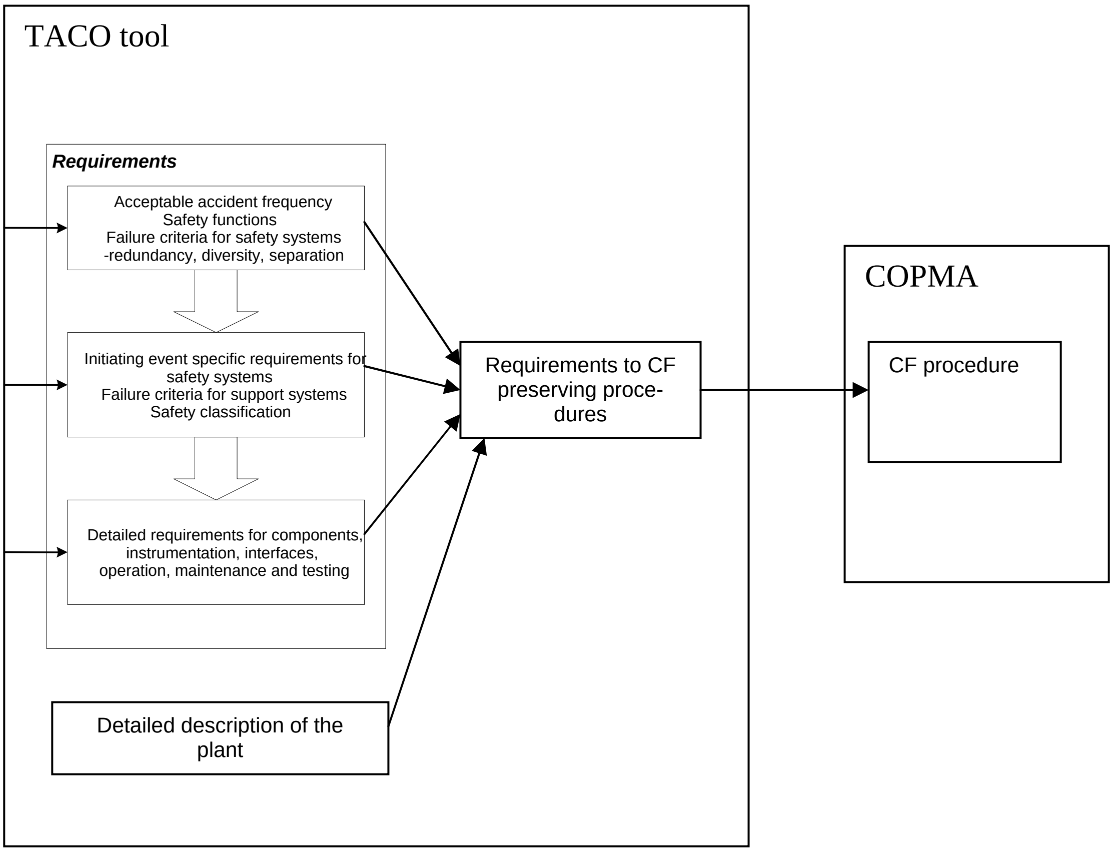

TACO tool
Requirements
Acceptable accident frequency
Safety functions
Failure criteria for safety systems
-redundancy, diversity, separation
Initiating event specific requirements for safety systems
Failure criteria for support systems
Safety classification
Detailed requirements for components, instrumentation, interfaces, operation, maintenance and testing
Detailed description of the plant
Requirements to CF preserving procedures
COPMA
CF procedure

Figure 7. Using the TACO tool to implement part of a procedure maintenance system (CF = critical safety function).

The needed associations between the procedure specific requirements and the more general requirements will presumably be provided by the 'relation' type of association currently defined as part of the TACO tool.

The expected benefits of such a setup might be several. One is a better coordination of general plant maintenance activities and revision of procedures used to operate the plant. Another benefit might be a systematic documentation of the design basis of the procedure construction, making an explicit link between requirements to the procedures and its current content. This is extremely useful in implementing the procedure revision process.

5.11 Alarm Systems

Alarm systems have been a major concern within complex industrial processes for many years. Within the nuclear community, the TMI accident in 1979 was one of the first really serious events that showed also the importance of the man-machine aspects of the systems in general, and the alarm system in particular.

The main purpose of an alarm system is to alert the operator if an abnormal situation is about to develop, and to assist him in identifying and correcting the situation. Modern, advanced alarm systems are designed with focus on the human capabilities and limitations, in particular to avoid information overload, and on the operators' needs in different situations.

Traditionally, a frequent problem with alarm systems is that the root cause rapidly propagates throughout the plant, with the result that the operator is drowned in a large number of alarms. Due to insufficient guidance, suppression, and prioritization by the alarm system, the operator gets too little help in determining the status of the plant and trying to understand what is happening, as alarms are coming from virtually all parts of the plant.

With an advanced and well-designed alarm system, the operator should be alerted at an early stage about which undesirable state is about to develop. By alerting the operator at an early stage, a good alarm system will reduce the frequency with which the safety system is called into action, and therefore reduce the frequency of safety-system failure.

While early recommendations concentrated on alarm suppression requirements and display methods, more recent ones in addition stress the *purpose* and *lifecycle management* of the alarm system. Many years will pass from the designers start their work on an alarm system, followed by a long period of system utilization, maintenance, and updates, until finally the use of the system is discontinued. Bringing the purpose of the system into focus will help keeping the system on the track during this long period. System management issues also are important to ensure that maintenance gives continuous lifecycle improvement rather that degradation. Without good lifecycle management, different members of the design team may pull in different directions, resulting in an incoherent system. After the design period has come to an end, maintenance people may destroy the coherence or other important properties of the system, not intentionally or by bad will, but because of unclear documentation or responsibilities.

Changes to the alarm system are highly probable, in particular to adapt to changes in the properties of the plant. There should therefore be an administrative system for handling access control and documentation of changes made to the alarm system. The objective of such an administrative system would be to prevent unauthorized modifications to the system and ensure that all changes are traceable and properly documented. The system should administer changes and adjustments to the alarm system, such as setting new alarm limits, shelving and inhibiting. An integrated system for documenting changes and adjustments should require certain information to be entered before changes are effectuated. Access control mechanisms should allow non-critical alarms to be easily modified by operators, while changes to critical alarms require special authorization. There should be procedures and systems for reporting incidents, deficiencies, problems, and potential problems related to the alarm system. It should be clearly defined who is responsible for following up these reports.

In a mature technical field, the design process starts by carefully considering the purpose of the system and the requirements that are necessary to fulfil its purpose. All modern sets of recommendations to alarms systems try to promote such a systematic method of work. The importance of lifecycle management, documentation of purpose of the system and the individual requirements, and adequate change control, clearly indicates the potential usefulness of the TACO approach to the design and maintenance of alarm systems. This relates to the general trend towards more mature system engineering as well as to the fact that alarm systems often need to be changed during their lifetime to improve their performance or to reflect changes in the plant. From a systems and requirements perspective, the TACO approach appears to be directly applicable to the design process and lifecycle management. In addition, a topic for possible closer investigation is whether the TACO approach can also help structuring the alarms, their causes and interrelations, and as such improving the means for handling the complexity of the alarm system.

5.12 Model Based Risk Assessment

The EU-funded CORAS project (IST-2000-25031) developed a tool-supported methodology for model-based risk analysis of security-critical systems. The project was initiated in January 2001 and successfully completed in September 2003. The CORAS consortium consisted of eleven institutions from four European countries. SINTEF was responsible for the technical coordination while Telenor AS R&D was the administrative coordinator and responsible partner towards the European Commission.

The CORAS framework is the overall result of the CORAS project since it integrates all the other CORAS results. The framework consists of terminology, languages for system modelling, processes for system development and risk management, methodologies for security risk analysis as well as computerised tools. In particular, the framework provides:

- A methodology for model-based risk assessment integrating aspects from partly complementary risk assessment methods and state-of-the-art modelling methodology.
- A UML based specification language targeting security risk assessment.
- A library of reusable experience packages.
- A computerised integration platform providing two repositories; an assessment repository and a repository for the reusable experience packages.
- An XML mark-up for exchange of risk assessment data.
- A vulnerability assessment report format.

The CORAS methodology for model-based risk assessment (MBRA) applies the standardised modelling technique UML to form input models to risk analysis methods that are used in a risk management process. This process is based on the standard AS/NZS 4360:1999 “Risk Management”. The CORAS methodology for MBRA can be utilised on three abstraction levels, and for each level recommendations and guidelines are provided, as well as templates, questionnaires and supportive descriptions.

The CORAS methodology for MBRA is specialised towards assessment of security critical systems. The CORAS methodology for MBRA has also been tested and turned out successfully on telemedicine and e-commerce systems through several trials. The benefit from using the methodology is that the assessment becomes effective due to a high degree of standardisation in describing the target of assessment and the increased level of reusability. At the same time the results become much easier to communicate to the different stakeholders.

A CORAS UML profile is an extension of the basic UML language targeting security risk assessment. The profile makes the UML diagrams easier to understand for non-experts, and at the same time preserves the well-definedness of UML. The profile for risk assessment provides rules and constraints for risk assessment relevant system documentation.

The CORAS library of reusable experience packages supports reuse of risk assessment experiences and documentation. A significant part of the results of a security analysis carried out on an IT-system will typically have a certain general character. To avoid starting from scratch for every new analysis, it is important to gather these general aspects.

The library of reusable experience packages captures such generic aspects in the form of e.g. UML-diagrams, table-formats, check lists, patterns and plain text. Each experience package is decomposed into experience elements.

An experience package belongs to a domain, but may inherit elements from experience packages of other domains; e.g., an experience package in the telemedicine domain may inherit elements from experience packages in the health domain and the general domain. The experience packages are classified into constructive and supportive packages, which contain constructive and supportive elements, respectively. A supportive package documents methodological aspects like guidelines and recommendations while a constructive package provides formats and patterns for the documentation of assessment results and the assumptions on which they depend.

The CORAS integration platform is the main computerised component of the CORAS framework. The CORAS platform is used to store the results from ongoing and completed security analyses, as well as the reusable elements and experience packages. These are stored in two separate repositories, the Assessment Repository for the analysis results, and the Reusable Elements Repository for the reusable elements. During a security analysis, reusable elements may be instantiated and become part of the security analysis results. The platform GUI provides the end-user with administrative functionality, such as creating new security analysis projects and managing the reusable elements and experience packages. A wide variety of UML modelling tools and risk analysis tools exist and are in use by security analysts and system engineers today. The CORAS platform provides flexible support for integration with such external tools. To this end, the platform provides an integration layer with a defined API which tools can use to integrate with the platform, utilising standardised XML formats for data integration. The CORAS platform comes with full documentation and provides:

- methodological guidelines in electronic form;
- an advanced tool for table-editing;
- automatic procedures for consistency checking;
- support for generating partly filled in tables based on existing data;
- user-guidelines in the form of help functionality.

In the absence of any standardised meta-data format for representing information related to risk assessment, the CORAS consortium has developed an XML mark-up for representing risk assessment information.

Such meta-data description of core risk assessment data are being used for the purpose of consistency checking between different items of the repositories provided by the CORAS integration platform. The XML mark-up is also used to facilitate easy integration of risk analysis tools with the CORAS integration platform. In particular, the mark-up defines information models for the core elements of the different risk analysis methods used in CORAS.

As networks of hosts continue to grow in size and complexity, evaluating their vulnerabilities that could be exploited becomes increasingly more important preventative measure. Periodic network assessment, used to uncover and correct vulnerabilities, is a common intrusion prevention technique. Although the tools that perform those assessments report the same basic information, there are some tool specific differences. Unfortunately, trying to combine output from these tools would require separate parsing tools to address the significant low-level differences. A standard format for representing assessment information in XML would bring with it the same types of benefits to the vulnerability assessment area with the ones that IDMEF and IODEF are going to bring to the intrusion detection and incident handling areas. The CORAS vulnerability assessment report format (VARF) addresses this problem by proposing data formats for sharing information of interest to vulnerability assessment and to facilitate the interaction with the risk management process.

The TACO approach may contribute to several parts of the CORAS framework. An immediate suggestion is to explore the possibility of adding formalised traceability features to the UML based specification language targeting security risk assessment and the library of reusable experience packages.

6. Next Steps: MORE

The purpose of this chapter is to give information on the project MORE (Management of Requirements in NPP Modernization Projects, NKS_R_2005_47), aiming at the industrial utilisation of results from the TACO project. The chapter describes how MORE relates to the NKS-R framework, and gives a description of the activity.

6.1 Background

Experiences from modernization projects at NPPs, in particular in Sweden and Finland, indicate the importance of adequate structure and modularisation of the requirements. It is important to handle the evolution of the requirements and the completeness with respect to the requirement sources, supported by some formalism for structuring the requirements. A particular issue is how to make an evolutionary, iterative software engineering process that reflects the evolving nature of the requirements and their understanding but at the same time satisfies the requirements set by the licensing authorities (e.g. with respect to quality assurance and documentation).

Management of changes is closely related to the maintainability of a software system. Typically, the requirements for a given 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. The task of managing alteration of the requirements is closely related to requirements traceability. As has been demonstrated in the TACO project, work on requirements traceability can to a certain extent be seen as a response to the need for keeping track of these changes. One benefit of traceability is the localization of the side effects of a modification and the identification of relationships that must be reconfirmed, thereby increasing the assurance that when changes are necessary they will be complete and consistent.

The new activity will build on and add to the results from the TACO project. The emphasis within the TACO project has been to facilitate understandability, communication and traceability of software system requirements throughout the different system lifecycle phases, by applying an appropriate traceability model. The TACO Traceability Model supports understandability, communication and traceability by providing a common basis, in the form of a requirements change history, for different kinds of analysis and presentation of different requirements perspectives. The model facilitates traceability by representing the requirements changes in terms of a change history tree built up by composition of instances of a number of change types, and to provide analysis on the basis of this representation. Much of the strength of the TACO Traceability Model is that it aims at forming the logic needed for formalising the activities related to change management and hence their further automation.

6.2 Goals and Results Expected

The overall objective of MORE is to improve the means for managing the large amounts of evolving requirements in Nordic NPP modernization projects. In accordance to this objective, the project will facilitate the industrial utilisation of the research results from TACO. On basis of compiled experiences on the problem of handling large amounts of information in relation to Nordic modernization projects, the MORE project will investigate how the approach to requirements management developed in the TACO project can be utilised to handle large amounts of evolving requirements in NPP modernization projects. While existing configuration management tools typically apply techniques that are file based, the TACO Traceability Model is paragraph based and therefore possibly more adequate for handling requirements (i.e., a requirement, or a composition of requirements, is treated as a single paragraph). The research will study how requirements can be grouped into concepts, and how design patterns can help to achieve this. One possibility is to utilise requirements (or design) templates, with guidance on how requirements can be decomposed or composed. The research will clarify how design patterns and requirements templates can be generated by utilizing the change history trees of the TACO Traceability Model.

6.3 Utilization of the Results

The activity will work explicitly on the issue of utilisation of the results by facilitating the industrial take-up of the research results produced within the TACO project. On the basis of experiences in the Nordic countries, the TACO project has aimed at identifying 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 through the different development phases. The proposed new activity will build on these experiences, and at the same time complement the experience basis by focusing specifically on experiences on the problem of handling large amounts of information and evolving requirements in relation to Nordic modernization projects.

It is expected that the activity will provide important input to the development of guidelines and establishment of recommended practices related to the management of requirements in NPP modernization projects. This kind of input is of high importance to current research and development activities being performed at IFE and VTT, to a common understanding between vendors, utilities, and regulators about the proper handling of requirements in the digital I&C systems development process, and consequently to the successful introduction of such systems in NPPs. By organising the project on the basis of a Nordic expert network, it is expected that the project will contribute to the synthesis of knowledge and experiences, with the aim of enhancing the competence within the Nordic countries on handling large amounts of information and changing requirements.

6.4 Fit to NKS Framework

The proposed activity represents a strategic follow-up activity of TACO (NKS activity NKS_R_2002_16), started in 2002 and scheduled for completion on the 30th of June 2005. The activity relates to DELI/MANGAN in the NKS-R framework, where it functions as a bridge between new technology, safety principles, and human factors. The proposed research is closely related to the topic of the Nordic Seminar on Automation, which was arranged in Oskarshamn, 5th to 7th of April 2004. The interaction with Nordic nuclear industry will be achieved through the extension of the TACO network. Additional interaction and appropriate contact with regulators will be achieved through the organization of industrial seminars and meetings.

Safety advancements: Several cases from the nuclear industry indicate the importance of clear, complete, and stable requirements from the beginning of the system development project. Since the safety of digital I&C is a property of the system in which it is embedded, the requirements specification also plays an important role in the safety assessment. The importance of requirements management to digital systems safety is reflected in the overall objective of the activity, which is to improve the means for managing the large amounts of evolving requirements in Nordic NPP modernization projects. It is expected that the project will provide important input to the development of guidelines and establishment of recommended practices related to the management of requirements in such projects.

Exhange of information: In order to facilitate the identification of best practices and criteria within the Nordic countries, the project will utilise and extend the Nordic expert network on requirements elicitation, specification, and assessment for digital I&C, established in the TACO project, partly through the arrangement of industrial seminars and meetings. The network provides a forum for exchanging experiences and research results on the topics to be addressed by the project. The information is exchanged by means of seminars, meetings, reports, and publications.

Competence and education: The emphasis on industrial utilisation means that the project needs to deal with real modernization projects. The interaction with these projects enhances both the transfer of industrial experiences to the research and the industrial competence and education on requirements management. By organising the project on the basis of a Nordic expert network, it is expected that the project will contribute to the synthesis of knowledge and experiences, with the aim of enhancing the competence within the Nordic countries on handling large amounts of information and changing requirements in NPP modernization projects. Even though the proposed activity will focus on modernization projects, the research topic, and the expected results, will be highly relevant to digital I&C systems development in general.

7. References

[1] P.-J. Courtois, A Dependability Justification Framework for Safety Critical Computer Based Systems, AVN (Association Vincotte Nuclear), Brussels 2004. (Available on-line: http://www2.info.ucl.ac.be/ingidocs/people/PJC/Courtois/framework_v07.2.pdf)

[2] C. Ghezzi, M. Jazayeri, and D. Mandrioli, Fundamentals of Software Engineering, 2nd edition (Prentice-Hall, 2003).

[3] S.G. Hart and L.E. Staveland, Development of NASA-TLX (Task Load Index): Results of Empirical and Theoretical Research, in: P.A. Hancock and N. Meshkati (eds.), Human Mental Workload (North-Holland, 1988).

[4] INSAG/IAEA, Defense in depth in nuclear safety: INSAG-10 / a report by the International Nuclear Safety Advisory Group, International Atomic Energy Agency, Vienna 1996.

[5] G. Kotonya and I. Sommerville, Requirements Engineering: Processes and Techniques (Wiley, 1998).

[6] P. Laakso et. al., Methods of simulated-assisted automation testing, VTT Research Notes, 2005.

[7] P. Lindsay and O. Traynor, Supporting fine-grained traceability in software development environments. Technical Report No. 98-10, Software Verification Research Centre, School of Information Technology, The University of Queensland (July 1998).

[8] S. Nilsen, Knowledge management in Nordic NPPs, Summary report of the findings from the workshop, NKS-102, April 2005.

[9] S. Norrman and J.-E. Holmberg, Automation & Reactor Safety: Requirements Assessment & Concepts (ARRAC). Presented in Nordic Seminar on Nuclear Automation, Oskarshamn, Sweden 5-7 April 2004.

[10] T. Okkonen, Nuclear Power Plant to be Constructed or Modernized — Automation Always Plays a Key Role, In Proc. of Automaatio 03 Seminar, 9–11 September, 2003, Helsinki.

[11] P. Savioja and L. Norros, Performance based human factors evaluation of complex systems, VTT Research report No BTUO62- 041311, 2005.

[12] T. Sivertsen et. al., Traceability and communication of requirements in digital I&C systems development – Preproject report, January 2003.

[13] T. Sivertsen et. al., Traceability and communication of requirements in digital I&C systems development – Project report 2003, NKS-91, March 2004.

[14] T. Sivertsen et. al., Traceability and communication of requirements in digital I&C systems development – The TACO project, in: Proceedings of the Man-Technology-Organisation Sessions, Enlarged Halden Programme Group Meeting, Sandefjord, Norway, May 2004.

[15] T. Sivertsen et. al., Traceability and communication of requirements in digital I&C systems development – Project report 2004, NKS-103, April 2005.

[16] T. Sivertsen et. al., The TACO approach for traceability and communication of requirements, Proceedings of Safecomp 2005, September 2005.

8. Appendix: Project Organisation

The project has been coordinated by Terje Sivertsen (IFE), and has comprised the following organisations and persons:

Organisation	Address	Project participants
IFE	Institute for energy technology P.O. Box 173 NO-1751 Halden Norway	Terje Sivertsen +47 69 212403 (terje.sivertsen@hrp.no) Rune Fredriksen +47 69 212430 (rune.fredriksen@hrp.no) Atoosa P-J Thunem +47 69 212322 (atoosa.p-j.thunem@hrp.no)
VTT	VTT Industrial Systems P.O. Box 1301 FIN-02044 VTT Finland	Olli Ventä +358 20 722 6556 (olli.venta@vtt.fi) Janne Valkonen +358 20 722 6469 (janne.valkonen@vtt.fi) Jan-Erik Holmberg +358 20 722 6450 (jan-erik.holmberg@vtt.fi)
Ringhals AB (Barsebäck Kraft)	Barsebäck Kraft P.O. Box 524 SE-246 25 Löddeköpinge Sweden	Jan-Ove Andersson +46 46 724148 (jan-ove.andersson@ringhals.se)

The project coordinator has been responsible for organising the work within the project and for directing it towards its objectives. This includes

- project planning and tracking;
- establishment and maintenance of the project archive;
- establishment of good communication and cooperation within the project;
- reporting to NKS;
- coordination of activities, in particular the production of the project deliverables;
- follow up of meetings and decisions;
- securing of proper quality control, including review and approval of documents included in the project archive;
- reporting of deviations and implementation of agreed corrections.

All the individual participants have represented important parts of the technical competence within the project, and have been responsible for contributing to the activities in such a way that the project would reach its objectives.

The project organisation has been intended to constitute a Nordic expert network on requirements elicitation, specification, and assessment for digital I&C. The network has provided a forum for exchanging experiences and research results on the questions addressed by the project, and a basis for evaluating the relative merits of the different practices, the relative importance of identified criteria, etc. A related concern has been to facilitate knowledge transfer from other areas applying equipment that are used in NPPs.

The emphasis on best practices and identified success criteria means that the project has needed to deal with real cases involving the development of a digital I&C system. By organising the project on basis of a Nordic expert network, the project has contributed to the synthesis of knowledge and experiences, enhancement of competence on requirements elicitation, specification, and assessment, improved awareness of alternative practices, a basis for assessing current practices, and an incentive to search for best practice.

Title	Traceability and Communication of Requirements in Digital I&C Systems Development. Final Report.
Author(s)	Terje Sivertsen*, Rune Fredriksen*, Atoosa P-J Thunem*, Jan-Erik Holmberg**, Janne Valkonen**, Olli Ventä** & Jan-Ove Andersson***
Affiliation(s)	* Institute for Energy Technology, Halden, Norway ** VTT, Finland *** Ringhals AB, Sweden
ISBN	87-7893-176-2 *Printed report*
Date	October 2005
Project	NKS_R_2002_16
No. of pages	55
No. of tables	1
No. of illustrations	7
No. of references	16

Abstract

The overall objective of the TACO project has been to improve the knowledge on principles and best practices related to the traceability and communication of requirements in digital I&C systems development. On the basis of experiences in the Nordic countries, the project has aimed at identifying 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 through the different design phases. It is expected that the project will provide important input to the development of guidelines and establishment of recommended practices related to these activities.

The report provides a summary of the project activities and deliverables, discusses possible application areas, and provides a link to its utilization in the project “Management of Requirements in NPP Modernization Projects” (NKS_R_2005_47). In the preparation of the final report, a number of application areas have been identified where the TACO deliverables, first of all the TACO Shell and the TACO Traceability Model, can be utilized. The report aims at facilitating such utilization, by defining the context and main issues, explaining the main aspects of the deliverables, discussing the challenges experienced in the different application domains with respect requirements management, traceability and communication – and how can the TACO results contribute to solving these challenges.

Key words: Traceability, requirements, TACO, change management, digital I&C, systems development

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