nks

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

NKS-149
ISBN 978-87-7893-212-9

# MORE
# Management of Requirements in NPP Modernisation Projects. Project Report 2006

Atoosa P-J Thunem and Harald P-J Thunem
IFE, Norway

Janne Valkonen
VTT, Finland

February 2007

## Abstract

The purpose of the report is to document the work and related activities in the period January 1 – December 31 in 2006, including dissemination activities. The work in this period has been concentrated on further research for adopting an approach for de-pendable requirements engineering and its supporting tool. The majority of the efforts in 2006, however, was spent on making the researchers, developers, utilities and li-censees more aware of the importance of the area of requirements engineering, and in that respect organising an international seminar on dependable requirements engineer-ing. This seminar was defined as a deliverable in the Activity Plan for 2006 and be-came also the most important deliverable for 2006. Therefore, this report naturally features a detailed summary of the seminar, which proved to be a true success and at the same time a door opener for more initiatives within the topic, proposed by several participants. More efforts within dissemination of the background and objectives of the project MORE within the nuclear community and towards NPPs that do carry out modernisation projects continued to be one important focus.

## Key words

MORE, tracability of requirements, dependable requirements engineering, TRACE, International Seminar on Dependable Requirements Engineering (Summary)

NKS-149
ISBN 978-87-7893-212-9

Electronic report, February 2007

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

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

# MORE
# Management of Requirements in NPP Modernisation Projects
# - Project Report 2006 -

**Atoosa P-J Thunem, Harald P-J Thunem**
**IFE, Norway**

**Janne Valkonen**
**VTT, Finland**

# Foreword

This document constitutes the 2006 report for the project MORE: Management of Requirements in NPP Modernisation Projects (NKS-R project number NKS_R_2005_47, started on July 1, 2005). The project aims at the industrial utilisation of the results from the project TACO: Traceability and Communication of Requirements in Digital I&C Systems Development (NKS-R project number NKS_R_2002_16, completed in June 30, 2005), and practical application of improved approaches and methods for requirements engineering and change management.

The purpose of the report is to document the work and related activities in the period January 1 – December 31 in 2006, including dissemination activities. The work in this period has been concentrated on further research for adopting an approach for dependable requirements engineering and its supporting tool. The majority of the efforts in 2006, however, was spent on making the researchers, developers, utilities and licensees more aware of the importance of the area of requirements engineering, and in that respect organising an international seminar on dependable requirements engineering. This seminar was defined as a deliverable in the Activity Plan for 2006 and became also the most important deliverable for 2006. Therefore, this report naturally features a detailed summary of the seminar, which proved to be a true success and at the same time a door opener for more initiatives within the topic, proposed by several participants. More efforts within dissemination of the background and objectives of the project MORE within the nuclear community and towards NPPs that do carry out modernisation projects continued to be one important focus.

Halden, February 2007

Atoosa P-J Thunem

# Table of contents

# Abbreviations

| | |
|---|---|
| IFE | Institute for energy technology |
| MORE | Management of Requirements in NPP Modernisation Projects |
| NKS | Nordic nuclear safety research |
| NPP | Nuclear power plant |
| SKI | Swedish Nuclear Power Inspectorate |
| STUK | Radiation and Nuclear Safety Authority of Finland |
| TACO | Traceability and Communication of Requirements in Digital I&C Systems Development (NKS project number NKS_R_2002_16) |
| VTT | Technical Research Centre of Finland |

# Summary

This document constitutes the 2006 report for the project MORE: Management of Requirements in NPP Modernisation Projects (NKS-R project number NKS_R_2005_47, started on July 1, 2005). The project aims at the industrial utilisation of the results from the project TACO: Traceability and Communication of Requirements in Digital I&C Systems Development (NKS-R project number NKS_R_2002_16, completed in June 30, 2005), and practical application of improved approaches and methods for requirements engineering and change management.

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

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

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

The purpose of the report is to document the work and related activities in the period January 1 – December 31 in 2006, including dissemination activities. The work in this period has been concentrated on further research for adopting an approach for dependable requirements engineering and its supporting tool. The very focus of the approach is valid and efficient change management related to modernisation activities. The majority of the efforts in 2006, however, was spent on making the researchers, developers, utilities and licensees more aware of the importance of the area of requirements engineering, and in that respect organising an international seminar on *dependable requirements engineering*. This seminar was defined as a deliverable in the Activity Plan for 2006 and became also the most important deliverable for 2006. Therefore, the main part of this report naturally features a detailed summary of the seminar, which proved to be a true success and at the same time a door opener for more initiatives within the topic, proposed by several participants. Institute for Energy Technology (IFE) hosted the seminar, chaired by the NKS-R Programme Manage-

ment and held in Halden, Norway, November 27-29. IFE covered all direct costs associated with the seminar, and the majority of indirect costs, being mainly the technical work done prior to the seminar.

More efforts within dissemination of the background and objectives of the project MORE within the nuclear community and towards NPPs that do carry out modernisation projects continued to be one important focus.

# 1. Introduction

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

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

The purpose of the present report is to document the further research and related activities to the project MORE: Management of Requirements in NPP Modernisation Projects (NKS-R project number NKS_R_2005_47, started on July 1, 2005), and carried out in the period January 1 – December 31, 2006. The work in this period has been concentrated on further research for adopting an approach for dependable requirements engineering and its supporting tool. The very focus of the approach is valid and efficient change management related to modernisation activities. Therefore, the approach advocates a more broad perception of requirements engineering, hence suitable for modelling and handling large amounts of requirements related to all stages of the systems development process and not only those traditionally including requirements at high-level stages. Creating traceability between the requirements from the high-level stages throughout the entire system development process is a prerequisite for valid and efficient change management. The majority of the efforts in 2006, however, was spent on making the researchers, developers, utilities and licensees more aware of the importance of the area of requirements engineering, and in that respect organising an international seminar on *dependable requirements engineering*.

Chapter 2 describes the approach for dependable requirements engineering adopted in the project MORE. Chapter 3 covers the most important components of the tool for

supporting the approach and equally adopted in the project. Chapter 4 presents the references used to compose the report.

Appendix A features the project activity plan and organisation. Appendix B features a detailed summary of the international seminar on dependable requirements engineering, Halden, Norway, November 27-29, 2006.

# 2. An Approach for Dependable Requirements Engineering

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

## 2.1 The Background

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

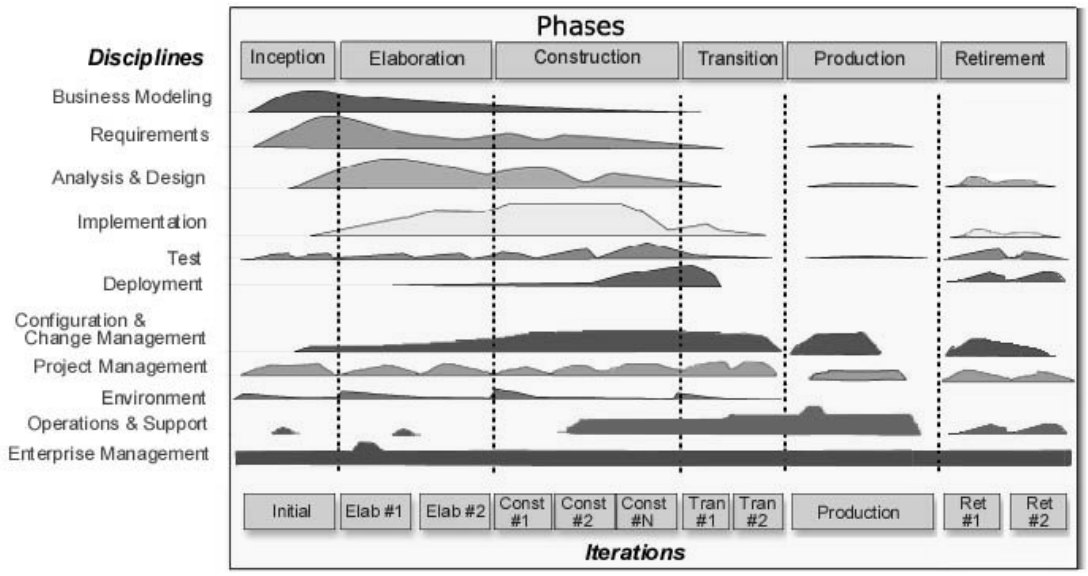



*Figure 1. The Enterprise Unified Process (EUP).*

Nevertheless, despite the availability of detailed guidelines for sub-activities in each discipline and for the number of iterations in each phase, neither RUP nor any other lifecycle models provide guidelines on how to achieve traceability among phases and disciplines. Also, if system properties are addressed at all, the implied concern is al-

most entirely on functional and operational factors, and not other dependability factors such as safety, security, reliability, flexibility and maintainability. To exemplify, there exist no instructions on how the security issues associated with the specific system architecture or application domain can influence the length of a certain phase, or the amount of certain sub-activities during the iterations [4]. The lack of addressing dependability factors in available life cycle models explains also why the concept of risk and risk analysis has not been an issue to take into account for these models.

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

## 2.2 The Four Pillars of the Approach

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

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

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

in accordance with the requirements of system development process and its product a risk analyst is supposed to analyse.

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

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

The next chapter explains the main elements of a tool that aims to support the above approach. As far as traceability is concerned, the tool utilises the traceability model developed in the project TACO. This tool is called *TRACE: Traceability of Requirements for Analysable Computerised Environments* [6].

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

Providing tool support for the main elements of the traceability model suggested in the project TACO was also among the important issues raised by the advisory group behind the project TACO (formed through the industrial seminars arranged by the project). To provide tool support for not only the traceability model but in higher degrees for the approach described in Chapter 2, the first prototype of the tool TRACE was developed in September 2005.

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

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

- Traceability between the requirements at a particular stage of the system lifecycle
- Traceability between the requirements defined for different stages of the system lifecycle
- Traceability of changing or changed requirements throughout the system lifecycle for better change management
- Traceability of dependability-related requirements throughout the system lifecycle for better dependability analysis
- Traceability of failures and risk factors with respect to a certain dependability factors, and thus traceability of all risk-informed requirements related to these risk factors

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

## 3.1 The Main Elements of TRACE

### 3.1.1 Paragraphs

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

| | |
|---|---|
| *id* | Automatically generated unique identifier. |
| *label* | Textual short label. |
| *version* | Version number. A Paragraph can be subject to a number of different Changes, where some will cause the creation of Paragraphs with a new label, and other the creation of Paragraphs with the same label but incremented version number (see description of Change class below). |
| *time* | Time of creation. |
| *status* | Status attribute (see table below for possible values). |
| *description* | Paragraph content, which for e.g. software development will be the textual description of a requirement. The purpose of the traceability approach is to keep a track of all changes to this attribute across different Paragraph versions and across all development phases. |
| *change_in* | The change that caused the creation of the Paragraph. |
| *changes_out* | List of changes performed on the Paragraph causing the creation of other Paragraphs. |
| *origins* | List of paragraph origins. See description of Link (which is the class implementing the concept of origin) below. |

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

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

### 3.1.2 Changes

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

| | |
|---|---|
| *id* | Automatically generated unique identifier. |
| *type* | Type of Change (see description of *ChangeType* class below). |
| *sources* | List of input Paragraphs to this Change. |
| *targets* | List of output Paragraphs from this Change. |

| | |
|---|---|
| *status* | Status attribute (see table above). |
| *user_id* | The identifier of the user responsible for introducing the Change. |
| *time* | Time of Change introduction. |
| *reason* | Textual description of the reason for introducing the Change. |
| *basis* | The basis for introducing the Change (see table below). |

The *basis* parameter is used to provide some description of the basis for applying the Change to one or more Paragraphs:

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

### 3.1.3 Change Types

The *ChangeType* class is used to define different types of Changes. The ChangeType class is associated with the following list of attributes:

| | |
|---|---|
| *label* | Unique label. |
| *para_in* | The number of input Paragraphs (possible values are “0”, “1”, “1 or more” and “2 or more”). |
| *para_out* | The number of output Paragraphs (same as above). |
| *description* | Textual description of change type. |
| *result_status* | Status of output Paragraph(s) (see table above). |
| *update* | How to update the output Paragraphs label and version (see below). |

The *update* value defines how the Paragraph label and version number are determined for a Paragraph resulting from a Change:

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

For use in software development, the default Change types include:

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

An example of a change type is “modify”, where the attribute values are given in the following table:

| | |
|---|---|
| *label* | “modify” |
| *para_in* | 1 |
| *para_out* | 1 |
| *description* | “This change denotes a modification of the paragraph” |
| *result_status* | None |
| *update* | Increment version number |

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

### 3.1.4 Links

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

- a textual reference from a brainstorming meeting
- an IAEA safety standard, suggesting the introduction of a specific safety function
- a web-page with statistical data showing the potential improvements in system reliability by developing in accordance with certain object-oriented metrics
- a link between a Paragraph in the *implementation* phase and a Paragraph in the *design* phase, indicating that the former fulfils the requirements of the latter

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

| | |
|---|---|
| *type* | Type of link |
| *string* | Textual information |

Examples of Links are given in the following table:

**A textual link**

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

**A file link**

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

**A hypertext link**

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

**A Paragraph link**

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

### 3.1.5 History Trees

The *HistoryTree* class is used to hold all required information about one history tree, including all Paragraphs and Changes. An example of a history tree is shown in Figure 2. History trees will show the development of a number of Paragraphs as they are subject to Changes, and for software development projects a typical use is to create one history tree for each development phase.

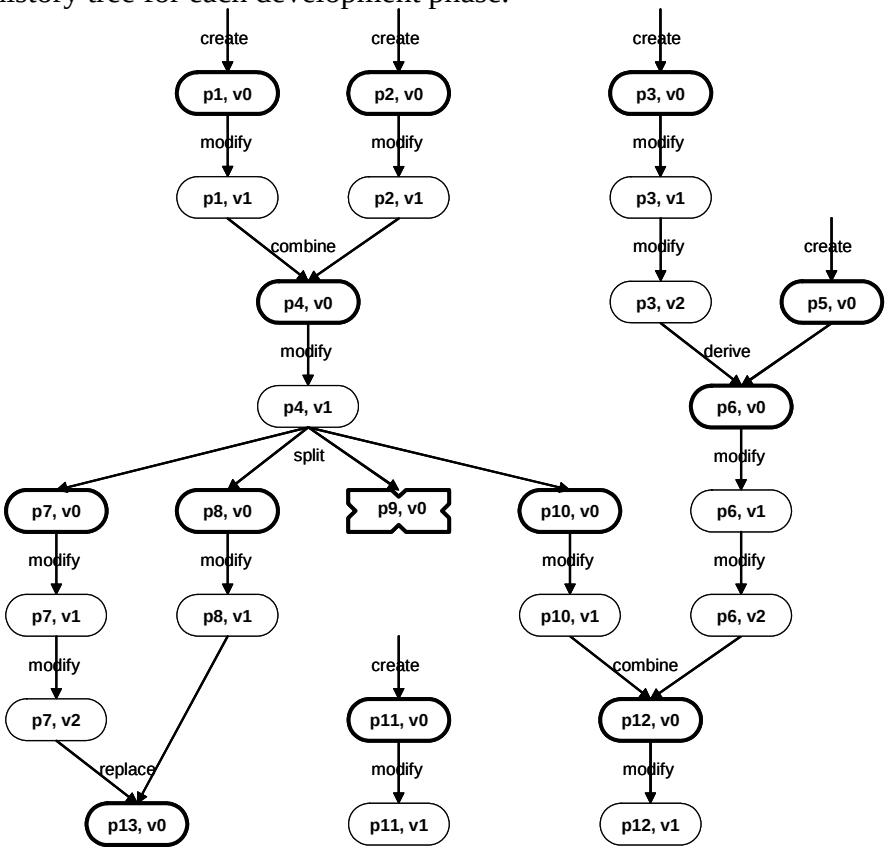



*Figure 2. Example history tree.*

The list of attributes associated with a HistoryTree is:

| | |
|---|---|
| *id* | Automatically generated unique identifier. |
| *label* | Textual label provided by user. |
| *paragraphs* | List of Paragraphs. |
| *changes* | List of Changes. |
| *create_time* | Creation time. |

| | |
|---|---|
| *last_change_time* | Last time history tree was changed. |

### 3.1.6 Sets

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

The list of attributes associated with a Set (in addition to those inherited from the HistoryTree class) is:

| | |
|---|---|
| *sets* | List of subsets. |
| *parent* | Parent set. |
| *child* | Child set. |
| *open* | Indicates whether Set is open or closed. |
| *close_time* | Time the Set was closed. |

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

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

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

## 3.2 Basic analyses

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

| | |
|---|---|
| *Created Paragraphs* | Whenever a new Paragraph is created, either “from scratch” or by certain Changes to other Paragraphs (e.g. derive, split, combine...), the Paragraph is marked as “Created”. |
| *Current Paragraphs* | The current or most recently updated version of a Paragraph is found by iterating through the list of Paragraphs and for each Paragraph label find the Paragraph with the highest version number. (Paragraphs that have been explicitly deleted are not included in this search) |
| *Deleted Paragraphs* | Whenever a Paragraph is deleted, it is marked as “Deleted”. |
| *Paragraph History* | The Paragraph history for any Paragraph can be determined by finding all |

*(forward/ backward)* versions of the selected Paragraph, all Changes affecting these versions, as well as the relevant version of all Paragraphs included in these Changes. This is straightforward, as all *Paragraph objects* contain lists of "incoming" and "outgoing" Changes, and all *Change objects* contain lists of "input" and "output" Paragraphs.

*Paragraph Trace (forward/ backward)*

**Forward:** Forward traceability relates to the development of Paragraphs starting with a selected Paragraph. The result will include all Paragraphs affected by the selected Paragraph (see Figure 3).

The trace is performed by a recursive search through all output Changes starting with the selected Paragraph. The search through a sub-tree is halted once a Paragraph without any output Changes is reached.

**Backward:** Given a Paragraph, we want to find the development of Paragraphs that leads to this Paragraph, i.e. the minimum fragment of the Change history that has influenced the development of the given Paragraph (see Figure 4).

The trace is performed by a recursive search through all input Changes starting with the selected Paragraph. The search through a sub-tree is halted once a Paragraph whose input is a "create" Change is reached.

*Origin Trace*

The *origin* parameter in the Paragraph class provides links to information used when creating a Paragraph. This information could e.g. be a textual description of why the Paragraph should be included, a shortcut to a file, a hypertext link to an IEEE standard used as basis for the Paragraph, or a link to another Paragraph in a different history tree. A typical use of the origin parameter could be during a software development project, where a separate history tree is created for each development phase (requirement, design, implementation, test...). Here, each Paragraph would represent a specific version of a specification, and often a specification in the design phase would be based on a specification in the requirement phase (see Figure 5).

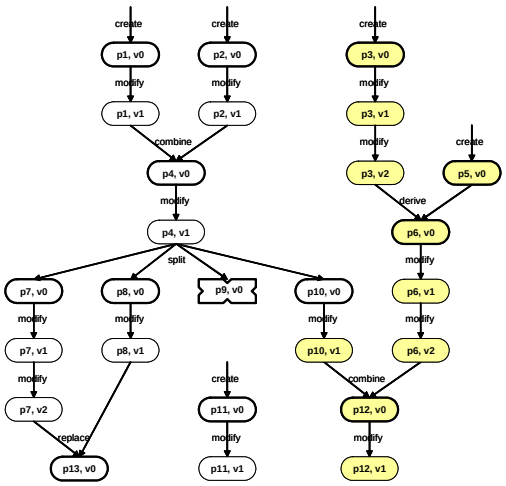



*Figure 3. Forward trace from (p3, v0).*

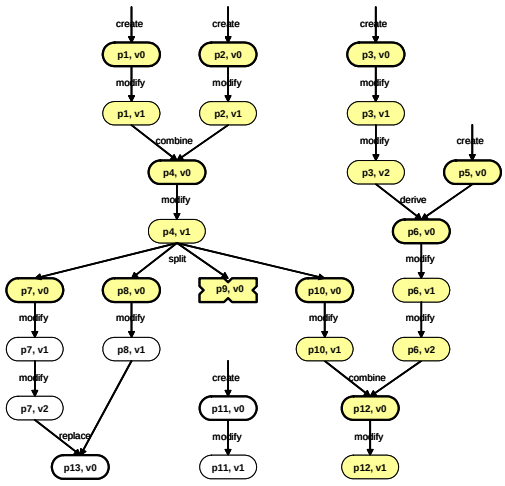



*Figure 4. Backward trace from (p12, v1).*

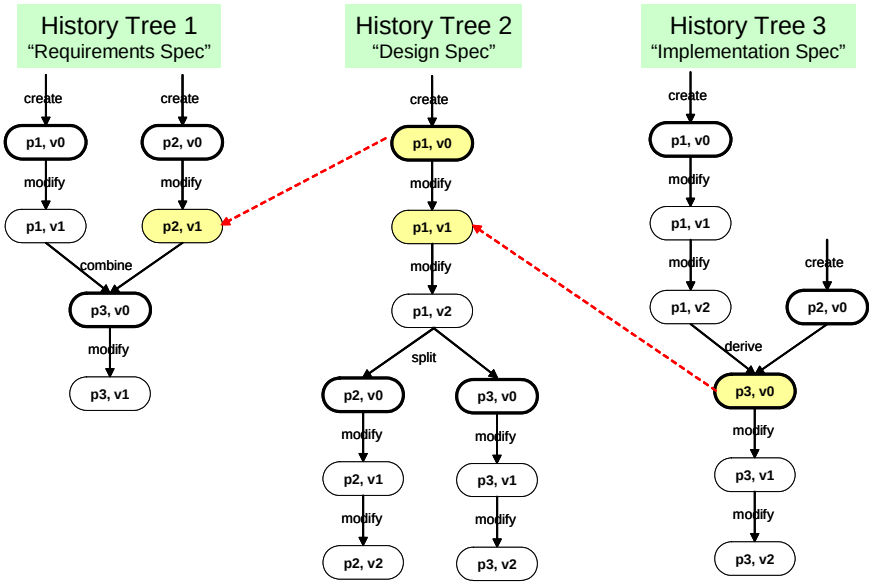



*Figure 5. Origin trace. The dotted lines are links from Paragraphs in one development phase to a previous phase.*

# 4. References


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

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

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

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

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

[6] A. P-J, Thunem, H. P-J Thunem, "TRACE: Traceability of Requirements for Analysable Computerised Environments", IAEA Technical Meeting on Implementing and Licensing Digital I&C Systems and Equipment in Nuclear Power Plants, November 2005, Espoo, Finland.

# 5. Appendix A: Project Organisation and Activities

## 5.1 Project Organisation

The project is led by Atoosa P-J Thunem (IFE), and comprises the following organisations and persons:

| Organization | Address | Project participants |
|---|---|---|
| IFE | Institute for energy technology<br>P.O. Box 173<br>NO-1751 Halden<br>Norway | Atoosa P-J Thunem<br>+47 69 212322<br>(atoosa.p-j.thunem@hrp.no)<br><br>Harald P-J Thunem<br>+47 69 212278<br>(harald.p-j.thunem@hrp.no) |
| VTT | VTT Industrial Systems<br>P.O. Box 1000<br>FIN-02044 VTT<br>Finland | Janne Valkonen<br>+358 20 722 6469<br>(Janne.Valkonen@vtt.fi) |

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

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

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

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

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

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

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

## 5.2 Project Activities

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

The activities in 2006 have been with focus on the following:

- Establishing a strategy and implementation plan for the improvement and industrial take-up and utilisation of the research results from the project TACO. This was done, amongst others, through adopting an approach for dependable requirement engineering and its supporting tool TRACE into the project.
- Compiling experiences on the problem of handling large amounts of information in relation to modernisation projects. This has been an ongoing activity, amongst others, through communication with Nordic NPPs and through dissemination and representation activities. Such dissemination was carried out in terms of the presentation of the results from the project TACO, and the status of the project MORE and its main aspects during the NKS Status Seminar, May 10-11, 2006, in Helsinki, Finland.
- Extending the industrial network from the project TACO. This has been an ongoing and successful activity, also due to the response received with regard to the preparation of the international seminar on Dependable Requirements Engineering by IFE and with NKS co-sponsorship, to be held in Halden, November 27-29, 2006.
- Contacts with NPPs in Finland and Sweden that currently undertake or plan to undertake one or several modernisation activities, in order to prepare for an organised meeting and direct participation of the NPP in the project organisation. Despite efforts by IFE and VTT, an organised meeting with Finish NPPs has so far not been possible, due to the work load at the NPP.

The activities in 2007 and 2008 will carry out the implementation plan in cooperation with an extended network of industrial partners. The network established through the activity organisation and the TACO industrial seminars will be further extended and consolidated through the arrangement of industrial and international seminars.

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

The activities in 2007 will include the following:

- Continuous improvement of the results from the project, on the basis of the received feedback and gained knowledge.
- Identification and application of a couple of case studies from NPP projects and activities in order to initiate and implement the industrial take-up and utilisation of the research results in real modernisation projects.
- Continuing to compile experiences on the problem of handling large amounts of information in relation to Nordic modernisation projects, amongst others, through organised visits to selected plants.
- Extending the industrial network, also through disseminations and presentation of the results in Nordic and NKS related events such as seminars and workshops, and through the results from the international seminar on Dependable Requirements Engineering by IFE and with NKS co-sponsorship, to be held in Halden, November 27-29, 2006.
- Preparing and arranging an industrial seminar on dependable requirements engineering (November - December 2007).

The overall documentation schedule is as follows:

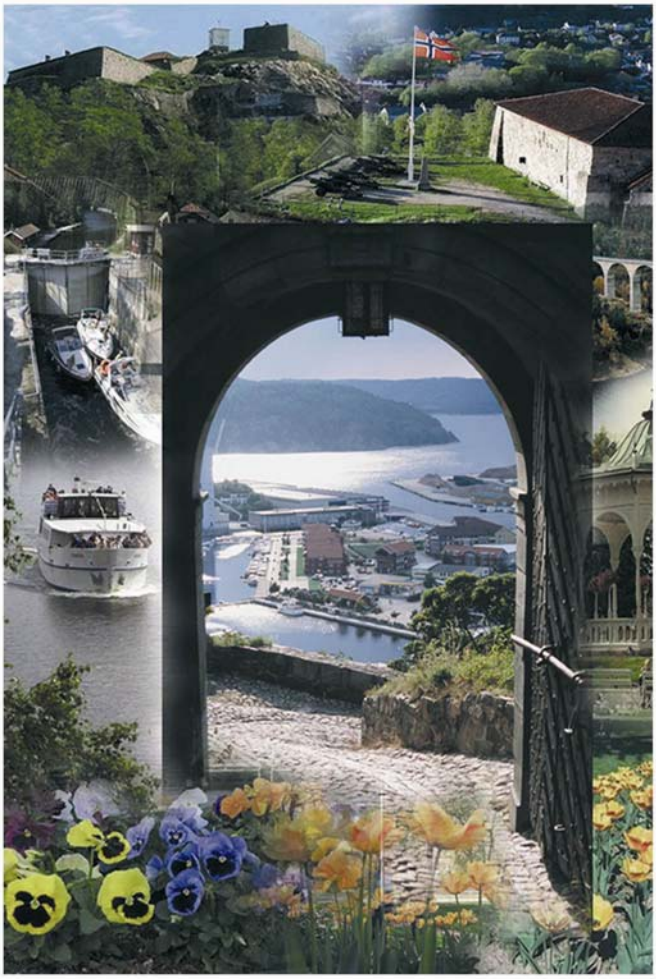
- February 2007: Activity report for 2006, including presentations and materials from the international seminar on Dependable Requirements Engineering, November 27-29, 2006, in Halden, Norway.
- January 2008: Activity report for 2007
- June 30, 2008: Final report, including presentations and materials from the industrial seminar planned for Spring 2008

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

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

**Halden, Norway**
**November 27-29, 2006**

## PROGRAMME



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

## *PRACTICAL INFORMATION*

**Short CV for the Key Note Speaker**

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

**General Chair**

Patrick Isaksson, NKS-R Programme Head

**Technical Programme Committee**

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

**Local Organising Committee**

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

**Secretary**

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

**Social Event**

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

***DETAILED PROGRAMME***
***MONDAY, NOVEMBER 27***

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

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

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

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

Brief explanation of the seminar's structure

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

*Arndt Lindner:* The Revised IEC 60880

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

***DETAILED PROGRAMME***

***TUESDAY, NOVEMBER 28***

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

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

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

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

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

**10:50 to 12:00 Paper presentations**

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

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

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

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

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

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

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

**14:30 to 16:00 Workshop session: "Coffee Table Discussions"**

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

*Sub-topics:*

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

**16:00 to 16:20 Break**

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

***DETAILED PROGRAMME***

***WEDNESDAY, NOVEMBER 29***

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

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

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

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

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

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

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

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

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

*Summarising the seminar:*

- Key issues *Session Chair: P. Isaksson / Secretary: A. P-J Thunem*
- Path ahead

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

## List of Participants

| Name: | Organisation: | Address: | Country: | Tel.: | Fax: | E-mail: |
|---|---|---|---|---|---|---|
| **CZECH REPUBLIC:** | | | | | | |
| Kropik, Martin | Faculty of Nuclear Sciences and Physical Engineering CTU in Prague | | Czech Republic | +420 603 871 795 | +420 284 680 764 | kropik@troja.fjfi.cvut.cz |
| Molnar, Jozef | Nuclear Research Institute Rez plc | Husinec-Rez, Cp. 130, 250 68 | Czech Republic | +420 38110-3939 | +420 38110-4103 | Mol@ujv.cz |
| **Denmark:** | | | | | | |
| Morten Lind | Oersted · DTU, Automation, Technical University of Denmark | Building 326 DK-2800 Kongens Lyngby | Denmark | +45 45253566 | +45 45881295 | mli@oersted.dtu.dk |
| **FINLAND:** | | | | | | |
| Heimbürger, Harri | STUK | P.O.Box 14 FI-00881 Helsinki | Finland | +358 9 759881 | +358 9 75988382 | harri.heimburger@stuk.fi |
| Kaj Juslin | VTT Technical Research Centre of Finland | P.O.Box 1000 FIN-02044, | Finland | +358 40 500 1254 | +358 20 722 7053 | kaj.juslin@vtt.fi |
| Savola, Reijo | VTT | P.O.Box 1100 FIN-900571 Oulu | Finland | +358 40 569 6380 | +358 20 722 2320 | reijo.savola@vtt.fi |
| Valkonen, Janne | VTT | P.O.Box 1000 FIN-02044 | Finland | +358 20 722 6469 | +358 20 722 6027 | janne.valkonen@vtt.fi |
| **GERMANY:** | | | | | | |
| Glöe, Günter | TÜV Nord SysTec GmbH & Co. KG | Grosse Bahnstrasse 31 22525 Hamburg | Germany | +49 40 8557 25 77 | +49 40 8557 2429 | ggloee@tuev-nord.de |
| Hadler, Tobias | TÜV Nord SysTec GmbH & Co. KG | Grosse Bahnstrasse 31 22525 Hamburg | Germany | +49 40 8557 2727 | +49 40 8557 2429 | thadler@tuev-nord.de |
| Lindner, Arndt | ISTec GmbH | Forschungsgelände D-85748 | Germany | +49 89 32004 529 | +49 89 32004 300 | arndt.lindner@istec.grs.de |
| Miedl, Horst | ISTec GmbH | Forschungsgelände D-85748 | Germany | +49 89 32004 528 | +49 89 32004 300 | horst.miedl@istec.grs.de |
| **HUNGARY:** | | | | | | |
| Bartha, Tamás | MTA SZTAKI Computer and Automation Research Institute | Kende u. 13-17 H-1111 Budapest | Hungary | +361 279 6227 | +361 466 7483 | tamas.bartha@sztaki.hu |
| **NORWAY:** | | | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| Lauritsen, Torgrim | NTNU | Sem Sælandsvei 7-9<br>7491 Trondheim | Norway | +47 3594427<br>+47 95129557 mob | +47 73594466 | torgriml@idi.ntnu.no |
| Opdahl, Andreas L. | Universitetet i Bergen | Infomedia, UiB<br>Postboks 7800,<br>5020 Bergen | Norway | +47 55 58 91 00 | +47 55 58 91 49 | andreas@infomedia.uib.no |
| Sindre, Guttorm | NTNU | Sem Sælandsvei 7-9<br>7491 Trondheim | Norway | +47 73594479 | +47 73594466 | guttors@idi.ntnu.no |
| **SWEDEN:** | | | | | | |
| Isaksson, Patrick | Vattenfall Power Consultant AB | Box 527<br>162 16 Stockholm | Sweden | +46 8 739 50 00 | +46 8 739 62 26 | Patrick.isaksson@vattenfall.com |
| Liwång, Bo | SKI | SE-10658 Stockholm | Sweden | +46 86988492 | +46 8 6619086 | bo.liwang@ski.se |
| **United Kingdom:** | | | | | | |
| Dobson, Glen | Lancaster University Computing Departmetn | | UK | +44 1524 510311 | +44 1524 510492 | g.dobson@comp.lancs.ac.uk |
| | | | | | | |
| **IFE:** | | | | | | |
| Berg, Øivind | Institutt for energiteknikk OECD Halden Reactor Project | P.O.Box 173<br>1751 Halden | Norway | +47 69 21 22 71 | +47 69 21 24 60 | oivind.berg@hrp.no |
| Bisio, Rossella | IFE, OECD-HRP | P.O.Box 173<br>1751 Halden | Norway | +47 69 21 22 49 | +47 69 21 24 60 | rossella.bisio@hrp.no |
| Gran, Bjørn-Axel | IFE, OECD-HRP | P.O.Box 173<br>1751 Halden | Norway | +47 69 21 23 59 | +47 69 21 24 60 | bjorn.axel.gran@hrp.no |
| Katta, Vikash | IFE, OECD-HRP | P.O.Box 173<br>1751 Halden | Norway | +47 69 2122 65 | +47 69 21 24 60 | vikash.katta@hrp.no |
| Christian Raspotnig | IFE, OECD-HRP | P.O.Box 173<br>1751 Halden | Norway | +47 69 2122 96 | +47 69 21 24 60 | christian.raspotnig@hrp.no |
| Thunem, Harald P-J. | IFE, OECD-HRP | P.O.Box 173<br>1751 Halden | Norway | +47 69 21 22 78 | +47 69 21 24 60 | harald.p-j.thunem@hrp.no |
| Thunem, Atoosa P-J. | IFE, OECD-HRP | P.O.Box 173<br>1751 Halden | Norway | +47 69 21 23 22 | +47 69 21 24 60 | atoosa.p-j.thunem@hrp.no |
| | | | | | | |

**Seminar secretary:**
Grete Bjerkely
Grete.Bjerkely@hrp.no
Tel: +47 69 21 22 53
Fax: +47 69 21 24 60

## Institute for Energy Technology (IFE)

IFE is an international research institute for energy and nuclear technology. IFE's mandate is to undertake research and development, on an ideal basis and for the benefit of society, within the Energy and Petroleum sector and to carry out assignments in the field of nuclear technology for the nation. The institute will increasingly concentrate on safety and environmental research within these fields.

IFE's nuclear technology comprises all activities that are directly or indirectly related to the Institute's two research reactors, in Halden and at Kjeller. The Institute for Energy Technology was founded in 1948 and is now an independent foundation.

IFE's research and development activities are directed at:

- Develop profitable, safe and environmentally-friendly technology for petroleum extraction, energy production and energy consumption.
- Maintain and further develop national competence within reactor safety, radiation protection and nuclear technology based on the Halden and Jeep II reactors.
- Utilise the Institute's special competence in the field of nuclear reactor safety technology in other spheres of society.
- Conduct basic research in physics based on the JEEP II reactor at Kjeller.

Nuclear technology accounts for about half the Institute's activities, petroleum technology totals about 30 per cent and R&D in alternative energy systems and environmental technology about 20 per cent. Nuclear specialities give IFE a distinctive profile and identity in Norwegian petroleum research. Moreover, the results of the international Halden Project are used in a comprehensive range of assignments for Norwegian industry.

International co-operation characterises our Institute. Collaboration in reactor- and information technology is mainly through the OECD Halden Reactor Project, in which IFE co-operates with about 100 foreign organisations in 20 countries. In the Petroleum sector IFE has wide-ranging collaboration with international oil companies active on the Norwegian continental shelf.

In addition to contract work the Institute also carries out long term research, including basic research in physics. Focus is on projects that are important enough to have a significant impact on industrial innovation and technology renewal. In nuclear related areas IFE assists Norwegian authorities in international projects concerning radiation protection and improved reactor safety.

## OECD

Pursuant to Article 1 of the Convention signed in Paris on 14th December 1960, and which came into force on 30th September 1961, the Organisation for Economic Cooperation and Development shall promote policies designed:

- To achieve the highest sustainable economic growth and employment and a rising standard of living in Member countries, while maintaining financial stability, and thus to contribute to the development of the world economy;
- To contribute to sound economic expansion in Member as well as non-member countries in the process of economic development; and
- To contribute to the expansion of world trade on a multilateral, non-discriminatory basis in accordance with international obligations.

The original Member countries are Austria, Belgium, Canada, Denmark, France, Germany, Greece, Iceland, Ireland, Italy, Luxembourg, the Netherlands, Norway, Portugal, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. The following countries became Members subsequently through accession at the dates indicated hereafter: Japan (28th April 1964), Finland (28th January 1969), Australia (7th June 1971), New Zealand (29th May 1973), Mexico (18th May 1994), the Czech Republic (21st December 1995), Hungary (7th May 1996), Poland (22nd November 1996), the Republic of Korea (12th December 1996) and the Slovak Republic (14th December 2000). The Commission of the European Communities takes part in the work of the OECD (Article 13 of the OECD Convention).

## NEA

The OECD Nuclear Energy Agency (NEA) was established on 1st February 1958 under the name of the OEEC European Nuclear Energy Agency. It received its present designation on 20th April 1972, when Japan became its first non-European full Member. NEA membership today consists of all European Member countries of OECD as well as Australia, Canada, Japan, the Republic of Korea, Mexico and the United States. The Commission of the European Communities also takes part in the work of the Agency. The mission of the NEA is:

To assist its Member countries in maintaining and further developing, through international co-operation, the scientific, technological and legal bases required for a safe, environmentally friendly and economical use of nuclear energy for peaceful purposes, as well as

To provide authoritative assessments and to forge common understandings on key issues, as input to government decisions on nuclear energy policy and to broader OECD policy analyses in areas such as energy and sustainable development.

Specific areas of competence of the NEA include safety and regulation of nuclear activities, radioactive waste management, radiological protection, nuclear science, economic and technical analyses of the nuclear fuel cycle, nuclear law and liability, and public information. The NEA Data Bank provides nuclear data and computer program services for participating countries.
In these and related tasks, the NEA works in close collaboration with the International Atomic Energy Agency (IAEA), with which it has a Cooperation Agreement, as well as with other international organisations in the nuclear field.

**CSNI**

The NEA Committee on the Safety of Nuclear Installations (CSNI) is an international committee made up of senior scientists and engineers, with broad responsibilities for safety technology and research programs, and representatives from regulatory authorities. It was set up in 1973 to develop and coordinate the activities of the NEA concerning the technical aspects of the design, construction and operation of nuclear installations insofar as they affect the safety of such installations. The Committee's purpose is to foster international cooperation in nuclear safety amongst the OECD Member countries. CSNI's main tasks are to exchange technical information and to promote collaboration between research, development, engineering and regulation organisations; to review the state of knowledge on selected topics of nuclear safety technology and safety assessments, including operating experience; to initiate and conduct programs to overcome discrepancies, develop improvements and reach consensus on technical issues; to promote coordination of work, including the establishment of joint undertakings.

**HRP**

The OECD Halden Reactor Project (HRP) is a joint undertaking of national organisations in 18 countries and collaboration with more than 100 nuclear organisations worldwide sponsoring a jointly financed programme under the auspices of the OECD NEA. The HRP is aiming to improve safety in operating nuclear plants. The programmes at the Halden Project address nuclear fuel issues, material performance and man-machine systems research and development and are composed to answer the needs of member organisations and the nuclear community at large.
The organisations participating in the Halden Project are actively guiding the Project's research programmes. They represent a complete cross section of the nuclear industry, including national research organisations, reactor and fuel vendors, utility companies and the licensing and regulatory interests. The joint programme started already in 1958 and is renewed every third year. The programme renewal involves extensive reviews and discussions with Project participants on priorities, programme issues to be addressed and technical means to achieve the programme objectives. The programme results are systematically reported in Work Reports and in Conferences organised by the Project. Special workshops with participation of experts are frequently arranged for in-depth assessments of specific issues, especially when new programme issues are to be established.

## *PROCESSING THE PROGRAMME*
## *(Incl. Q&A and discussions)*

**Monday, November 27**

| | |
|---|---|
| 08:30-09:00 | Registration |
| 09:00-09:45 | Opening session |
| 09:45-10:45 | Key-note Speaker |
| 10:45-11:00 | Break |
| 11:00-12:00 | Paper presentations |
| 12:00-12:30 | Discussion |
| 12:30-13:30 | Lunch |
| 13:30-14:30 | Paper presentations |
| 14:30-15:00 | Discussion |
| 15:00-15:15 | Break |
| 15:15- 16:45 | Visit to IFE's MTO Lab |

**Key-note Speech:**

*Title:* The revised IEC 60880
*Presenter:* Arndt Lindner

**1. Session:**

*Title:* Formal Modelling and Verification of Specifications for the I&C System Software in NPPs
*Presenter:* Tamàs Bartha
*Abstract:* Function Block Diagrams (FBDs) are a widely used specification method in modern I&C systems used in the development of safety-critical software. The need for the integration of automated formal verification in the development process in order to increase software reliability is constantly increasing. This paper presents a Coloured Petri net based approach to the formal verification of Function Block Diagram based specifications. The approach is non-model based; only the control logic of the safety function is modelled and verified. The proof if required properties is based on reachability analysis and model checking. The objective of the work is to demonstrate the possibility of integrating the formal analysis into the control software development process of a nuclear power plant (NPP).

Q (by APJT): More explanation on "non-model-based" approach? Only the control/ monitoring system is modelled? Process model is included in the systems model in model-based approach?

Q (by APJT): Can BBN be used to optimise the models? How about traceability trees as supporting means to avoid explosion?
A: FBD: Function Block Diagram.

Q (by APJT): Is it not difficult to have validation facilities that are automated?

Q: Anything from pre-set case?
A: No, could only look at one scenario.

Q (by AL): Who decides what the reasonable constraints are?
A: This is very much decided by physical conditions, f.ex. a temperature increase takes time, which means we can remove certain unrealistic states.

Q (by AL): How can this be taken into account?
A: There is the possibility to have a simplified model of the context in which the control will operate, this constraint the input reducing the explosion of state problem too.

Q (by AL): When I&C are installed in the real environment they continuously receive signals, and they internal state is influenced by the sequence (I&C have memory). Can this aspect be modelled in the presented approach?
A: Yes, but in the case study considered was not the case.

*Title:* Software Requirements for New Independent Power Protection and Control Systems of VR-1 Training Reactor
*Presenter:* Martin Kropik
*Abstract:* This article deals with software requirements for the upgraded Independent Power Protection system and Control system of the VR-1 training reactor operated by the Department of Nuclear Reactors FNSPE CTU in Prague. The software requirements were prepared as a standard document (MS Word), and the structure of the document reflected requests for the transparency and readability. During the requirements assignment, high attention was put on their correctness, unambiguity, completeness, consistency, verifiability and traceability. Firstly, the safety requirements were established. Next, functional requirements – calculations, control, operational modes and transitions among them were set. The requirements were then thoroughly verified by the reactor specialists. The software for the Independent Power Protection system according to the requirements was manufactured, tested and validated by the Department. The Control system software was developed according to the requirements by DataPartner Company. The complexity of the Independent Power Protection system in comparison to the Control system is lower, and no substantial problems were found in the requirements. During the later Control system testing and operation, some small problems were found in the requirements. The correct software requirements were very important for the successful manufacturing and operation of the software. It was necessary to analyze carefully the safety and operation of the system, and to put attention on special and rare operational modes and situations.

Q (by APJT): “Safety reqs” and “operation reqs”: Is it correct to say that all operation reqs are dependability requirements, but not safety-oriented (this is related to one sub-topic of the workshop session)?

Q (by JV): 100 something pages of the MS Word and many reqs, as you mentioned. How did you ensure traceability also with regard to changes?
A: We did that in terms of amendments. Every time there was change, we made a new version of the document saying that this part and that part have been changed, are not valid, etc. MS Word Track Changes feature was not used.

*Title:* Requirements on Automation and Simulation Software Platforms for Efficient Design and Testing
*Presenter:* Kaj Juslin
*Abstract:* (no paper)

Q (by APJT): Do you think that explicit traceability of the requirements will contribute to better and more trustworthy simulators?

Q (by AL): Simulator tool: will it be possible to have tools for simulating I&C systems consisting of different kinds of PLCs?
A: Should be possible, they should also be more configurable (vendors have interest to show their adherence to standards (ISO) in a competitive market of components)

General comments:

- The terms HMI and MMI are used interchangeably, but as it becomes more common with female operators, suggest using HMI (human machine interface).
- There are a lot of acronyms describing nearly the same things. These must be standardised (terminology).

**2. Session:**

*Title:* Revisiting Ontology-Based Requirements Engineering in the age of the Semantic Web

*Presenter:* Glen Dobson

*Abstract:* There is a long history of research into utilising ontologies in the Requirements Engineering process. An ontology is generally based upon some logical formalism, and has the benefits for requirements of explicitly modelling domain knowledge in a machine interpretable way, e.g. allowing requirements to be traced and checked for consistency by an inference engine, and software specifications to be derived.

With the emergence of the semantic web, the interest in ontologies for Requirements Engineering is on the increase. Whilst efforts have been concentrated upon re-interpreting software engineering techniques for the semantic web, it is interesting to consider what benefits there are to be passed from the semantic web to traditional Software Engineering techniques.

In this paper we give an overview of this emerging research field, suggesting directions that could usefully be taken in the field of dependability requirements. We present our work on a dependability ontology compliant with the IFIP Working Group 10.4 taxonomy and discuss how this, and other ontologies, must interact in the course of Dependability Requirements Engineering. In particular we consider the links between the dependability ontology, an ontology for requirements and domain ontologies, identifying the advantages and difficulties of this approach.

Comments (by APJT): At IFE, we have called our ontology an “approach”. Your presentation indicates that we have common application of the terms, as the impression is that also you relate RE to all levels of the system life cycle.

Requirements Modelling Language is similar to design pattern languages. IFE is also engaged in RE for semantic web.

Q (by TL): I* - what is it?
A: There is a reference in the paper.
Q (by AL?): Hazard = failure, but may not be failure?
A: In UMD-terms only.
Q (by BAG): How about integrating with existing tools?
A: Yes, we will in reality do this.
Q (by HPJT): Do you have, or know of, some standard XML notation for RE and/or traceability?
A: Has not tried making ontology for the requirements, and do not think such one exists.

*Title:* Towards Requirement Driven Evaluation of Information Security
*Presenter:* Reijo Savola
*Abstract:* Digital convergence and diffusion of Information and Communication Technology (ICT) solutions in more traditional fields such as industrial automation is a major source of information security threats. Obviously, there is a need for automated information security validation, evaluation and testing approaches. Unfortunately, there is no practical approach to carrying out information security evaluation in a systematic way. Information security evaluation of software intensive and telecommunications systems typically relies heavily on the experience of the security professionals. Requirements are in the focus of information security evaluation process. Information security requirements can be based on iterative risk, threat and vulnerability analyses, and technical and architectural information. There is a need for more practical ways to carry out this iterative process. We introduce a framework for security evaluation based on security requirement definition, behaviour modelling and evidence collection. The goal of the decision process is to make an assessment and form conclusions on the information security level or performance of the system under investigation.

Q (by APJT): Regarding "measuring information security": Don't you think that that is very much related to the way we define parameters of security? F.ex. measuring security and verifying a system with regard to the measuring framework depends of whether we follow CIA way of thinking or including many other dependability factors (referring to GD's presentation)?

Also: "functional requirements" can be dependability-oriented too.

Also: Don't you think that one problem in ICT is that the definition of security as function of 4 dependability factors has been preserved and does not include other factors.
A: Agreed. The problem is that 3 different communities try to solve the same problems.

Q (by HH): Can we measure security?
A: Maybe in 2025.

Q (AL): The demands for security for I&C systems at NPPs are much more restricted than in telecom environments. In the ICT world, new systems are built on top of old, and nobody understands the old systems. Don't you think this has had its influence on making security management difficult within telecom?
A: Yes, definitely.

*Title:* Misuse Cases – Use Cases that Capture Security Threats
*Presenter:* Guttorm Sindre
*Abstract:* Misuse cases have been proposed and developed by the authors as a technique for early elicitation and specification of security requirements. The technique has been validated and elaborated in a series of Master's theses at the NTNU and University of Bergen. Misuse cases have also attracted interest from other researchers in academia and industry. This paper reviews our research on misuse cases so far, looking both at the conceptual and methodological foundations and on the experiences gained from applying the technique in practice. The paper also outlines paths for future research, both on misuse cases themselves and on how they can be used together with other security-related techniques.

Q (by APJT): So, you are actually using the misuse cases to improve the use cases? How have you managed the “egg and hen” problem?
Comment (APJT): The conclusion on page 11: It implies that there was perhaps not a good idea to compare misuse cases with attack trees for example, because they are developed with different purposes.

Q (BAG): Have you looked into MBRA?
A: No, and we will look into it (misuse cases for safety).

Q (BAG): What about traceability of failures? It seems that misuse cases can be used to improve traceability.
A: Agreed.
Comment (APJT): Traceability can be used for modelling better misuse cases, and then these can reveal some trends that not necessarily at first sight are regarded as failures.

Comment (ØB): Category A systems is the place to start if you want to develop ontologies.
Comment (AL): There is a combination of experts, and it may be difficult for them to "understand" each other. We still use procedural languages to develop critical systems, and not OO.

Q: What abstraction level? If too detailed, explosion of use cases?
A: Yes, no definite answer, because if you have too low level, you have to make design assumptions, and if it is too high level, it becomes too generic.

Q (APJT): In CORAS, we used success-oriented models. Traceability can be used to develop better misuse cases. Seen from the attackers’ point of view, these are use cases.

**General session discussion:**
1. paper, Q (Bartha): Will not get everybody to agree on one terminology.

Q: In SW there are intended and unintended functions. Is it similar to use cases and misuse cases?
A: Yes.

**Tuesday, November 28**

| | |
|---|---|
| 09:00-10:00 | Paper presentations |
| 10:00-10:30 | Discussion |
| 10:30-10:50 | Break |
| 10:50-12:00 | Paper presentations |
| 12:00-12:30 | Break |
| 12:30-13:30 | Lunch |
| 13:30-14:30 | Paper presentations |
| 14:30-16:00 | Workshop session: "Coffee Table Discussions" |
| 16:00-16:20 | Break |
| 16:20-17:00 | Presentations of the results from the workshop session |

**1. Session:**

*Title:* IFE's Approach for Dependable and Risk-Informed Requirements Engineering
*Presenter:* Atoosa P-J Thunem
*Abstract:* (no paper) The presentation introduced IFE's approach for dependable and risk-informed requirements engineering. SElab's activities and main research areas were introduced in the beginning. Some terms and concepts were defined as SElab sees them (which can be remarked as a positive new view and could lead to some interesting discussions). Traceability model was introduced with a short example. An approach for dependable and risk-informed requirements engineering was introduced.

Presentation was followed by a demonstration by Harald P-J Thunem of how the TRACE tool works. Tools functions and features were introduced and explained on the screen.

Q (JV to APJT): Does it mean (slide 13) that you can have traceability between a tree in the design and a tree in the implementation phase?
A: Yes.

Q (JV): Slide 18 says "explicit links between the requirements". Does it mean links as configuration management links and also traceability links for the life-cycle traceability?
A: Yes, it means that.

Q (HH to HPJT): Are there any industrial references for TRACE?
A (APJT): We will appreciate it a lot if you can help us in that area. We have also other possibilities towards other industrial domains than the nuclear to apply the tool.

Q (HH and AL): How about maintainability of the tool? How about 60 years ahead (system lifecycle)? Can we still use the tool?
A (HPJT): The TRACE tool is developed in Java, and obviously the Java specifications will change, and backward compatibility is not guaranteed. However, the tool stores all data in ASCII files with specifically defined XML-formats, so if you have the XML-format specifications and the data files from each project, you can reconstruct the project specifications, including the traceability histories.

Q (AL): Is the tool available for everyone freely or do we have to pay for it if we want to use it?
A (APJT): If someone wants to use the tool, they can contact IFE to get information about the possibilities. As far as the Halden Project member countries are involved, the tool is free of charge, and IFE and the customer can agree on additional /preparation/maintenance job done by the IFE staff.

*Title:* Improving Model-Based Risk Assessment by integrating the Results of Requirements Engineering into the System Models

*Presenter:* Vikash Katta

*Abstract:* (no paper) The presentation was about relationships between requirements engineering and risk analysis and how model-based risk assessment can be improved by considering this relationship.

*Change management of the system is remarkable and should by mentioned in the summary. Requirements traceability could be used for better failure models.*

Q (APJT): What do you mean by traceability between system models?
A: The traceability between different kinds of UML diagrams.
Comment (APJT): In that regard, it is still a problem to formalise the relationships between these different diagrams.
Comment (TB): People behind G2 have managed to do some work towards this.

Question and comment by JV: There has been discussion about modifying the requirements during the development. That perhaps depends on the type of the project and the problem area, so that e.g. web-based software projects have more living requirements and dependable systems have more clear and stable requirements right from the beginning of the project. It would be interesting to hear comments from the representatives of power companies and regulators to this subject. How much are requirements usually changed during the process?
A (BL): Typically requirements are not that clear from the beginning of the development projects. The problem is that requirements are interpreted differently by different groups involved in the project. After agreeing on the terms and their meaning, there are not big changes. What is remarkable is that also small chances have an impact on many things. There is a need to check all the affected parts of the system if even a small thing is changed. At OKG they decided to restart an entire project due to bad docs.

Comment (AL): Our experience shows a lot of changes of the requirements in modernization projects. Often the requirements specification is derived from the existing conventional system in the beginning of modernization projects. Later-on, when the utility realizes the enhanced possibilities and performance of the digital system, the change requests are put on the table.

Q: Trace designs. Traceability between different models... (Tamas Bartha had some suggestions of tools with trace functions...).

*Title:* Dependable Requirements Engineering for WEB Based Systems

*Presenter:* Rossella Bisio

*Abstract:* (no paper) Experiences from WEB based systems as tools for supporting knowledge sharing have shown the need for more structured approach in management of requirements. This is important especially when the system releases stabilize into a more controlled evolution, and in particular requirement traceability has a very important role to play. At the same time experiences from developing such systems can be shared to make best practices to improve quality both of the process and the products a system. Reuse of previous solutions is also an issue. Requirements traceability can have a positive impact not only in the scope of one project, but also in the scope of similar projects.

*The presentation could possibly be considered as a possible application of the techniques presented in the first three papers.*

Q (AL): Sometimes a requirement is found out to be a bad requirement and it is deleted. However, after some time, a similar requirement is introduced again. What means could there be to solve this problem?
A (APJT, HPJT, RB): In the TRACE tool, the whole idea of traceability trees and creating different versions of the trees is that no requirement is deleted. When you modify requirements, new versions of them are always created. Even a minor change creates a new version. Even though you delete a requirement, you still see it and can even undelete it. The whole version history is available. Retrieving similar requirements (based on searching techniques) can help avoiding the problem mentioned in the question.

Comments (HH): In some projects the I&C specification is a living doc, until it is frozen. We must though have milestones.
Comments (HH): "Make a new system similar to old with new tech". This is not enough info to start development.
Comment (BL) about freezing: It is also necessary to freeze the hardware for which you develop the software. There exists an example where the hardware was not “frozen” and then the changes in hardware caused a big mess in the software development side.

**2. Session:**

*Title:* Capturing of Dependable Requirements Engineering of Computer Systems at NPPs

*Presenter:* Günter Glöe

*Abstract:* (no paper) Dependable Requirements on Computerised Systems at NPPs result from two different sources. On the one hand side they result from project or customer needs and on the other hand side from state of the art as e.g. represented by standards. Within the VeNuS project sponsored by the German ministry for economics and work (BMWA) as project 1501282 a tool prototype has been developed to support in capturing the requirements on Computerised Systems at NPPs from standards.

The intended paper will present the approach for this tool prototype and show its capabilities.

The approach has been adopted from commercially available tools. It consists of a database which has been created by IFE and a program giving access to the database. The database includes two IEC standards and a NRC standard.

The capabilities of the prototype are

- to inform the users about the requirements provided by the standards,
- to assist selection of several subsets of requirements and
- to export selected requirements for further usage with commercially available requirements management tools.

Besides this there are support functions as

- offering the possibility to the users for adding notes to the requirements and
- to store selected sets of requirements as template for usage in further projects.

Q (MK): What is the price of the tool?
A: For the research version, it is IFE that handles it. The commercial version is less than 6000 EUROs.

*Title:* Evaluation of the compliance of Computerised Systems at NPPs with Dependable Requirements

*Presenter:* Tobias Hadler

*Abstract:* (no paper) The presentation covered the following main topics:

- Dependency of Quality and Requirements
- VeNuS approach
- Example of VeNuS approach
- VeNuS Model
- Linking the requirements
- Linkvalues
- Tool: VeNuS Embedded Quality

Q (by BL): On what criteria do you define the target value that the system should fulfil?
A: Target values are important for the quality characteristics, in the range 0 to 1. We say normally that 0.5 is the normal degree for security. We give SIL4 the value 0.9, SIL3 0.7 and so on. Experts suggest using 0, 0.25, 0.75 or 1 as achieved values.

Q (by APJT): So, this is basically a profile ready-to-be-used that is given to the user and user fills in the actual numbers, and then these numbers are compared with the ones required by (interpreted from) the standard.
A: Yes.

Q (by BL): Page 10 (derived target values), how do you get to the 0.8 in readable code?
A: Layer 2 target values multiplied with link values and takes the maximum value.

Q (by GG): Tool presentation, what are the reqs.?
A: Look at the exported file, shows the exported file.

Q (by BL): Tool presentation, Look at the requirement 913, why the 0?
A: The testers go and test it and bring back the value, so it is an observational value.

Q (by BL): Tool presentation, how could the function be fulfilled, when there are no parameters?
A: Looking at the sub-characteristics, so look at the reqs and see if they are fulfilled. Look if they are enough to fulfil.

Q (by BL): Looks like BBN, in practice seen a lot of doc and interpretation of standards. Is such a discussion on interpretation?
A: You only get the req out and will interpret it yourself. Link to the pdf is available.

Q (by AL): Did you also make experiments with the logic?
A: BAG - Had a lot of error in this way.

1. step network
2. values

Calculation is pure mathematics, one way down, another up, hard to fit what we expected to see. No static rules, Bayesian approach not applicable when 0 and 1. Good documentation through the project. It also expresses the experience

Q: Relationships presented, is it user oriented knowledge. Is it the user who “gives”.
A (BAG): Play-ex. how to go up and down. Layer one and two are towards the standards. No expert judgement.

Q (by AL): SW standards: 60880 62138, can you express sub-set of requirements?
A: Can choose between linear and iterative.

Comment (BAG): Looking at the forth level, some reqs can measure with automatic tools (CATS and Reveal), impossible tools and have checklists.

Q (by BL): Some reqs are not coming from standards. How about implementing these reqs to get the overall picture?
A: Another work package, looking on source code, and for that it exists a document as a standard. Built a new RiskCAT Nuc. with the doc.
Comment (BL): What level of the expert judgement is not reusable? It is necessary to modify it?

Q (HH): Confidence building, enough testing, how to combine all these?
A: It is a tricky situation. You have high safety req. on systems. Some in Sweden tried to make safety case, they ended up with over 2000 reqs. from standards. The problem was that they couldn't get the link, to see that they fulfilled the top level reqs.
Comment (AL): Not put too much on the tool, but look at the benefit. One can look at the decisions. If found out reqs on high level, the tool will give hint on low levels

Comment (APJT): A general question (not to the tool used in VeNuS): Revisions are certainly needed towards standards. So, what if the "phases" defined by the standard giving input to safety are different at the user's site, the way their system and its safety reqs are met? And next: What to do if there are improvements at the user site that could be used to revise the standard?
BL: This is a general problem, but this tool can actually be used to identify what portions are not complying and from there to ask why. The answer to this why can reveal improvement potentials for the standard itself.

Comment (BL): An example of the application of the tool is tracing back what did not fulfil the standard, and then making arguments on that basis.

**3. Session:**

*Title:* Overview of Safety and Safety Related I&C Research and Regulatory Activities in Finland

*Presenter:* Harri Heimbürger

*Abstract:* (no paper) Some Finnish activities were discussed in context of some technical case studies like NPP I&C (automation) including main control room (MCR) modernizations. Some examples of application of the new IEC-standards in Finnish NPP-projects were discussed from requirements point of view. The presentation included the following main topics:

- A brief summary of recent I&C Requirements Specification and Tracing research activities?
- Standards and Guidelines as basic requirements and recommendations
- Examples of some large I&C and MCR modernization projects at NPPs in Finland
- Some examples of new IEC-NPP I&C-standards in Finnish NPP-projects from requirements point of view
- A summary of I&C including MCR requirements written in Finnish YVL-guides issued by STUK
- What is ASAF (Automation Safety Forum)? Deliverables in safety and security areas

The framework concerning national safety research during the years 2007-2010 within the area of automation (I&C) and human system interfaces (HSI in

MCR) was briefly described. The on-going research program SAFIR will finish by the end of this year. The name of the new program is called SAFIR 2010. For more information: www.stuk.fi , www.tvo.fi, www.vtt.fi.

Q (by ØB): Good to see standards for alarm systems. Are there standards for procedures? New plants will use electronic procedures.
A: No new standards. But in the new plant they will be applying new computerised procedures.

Q (GG): Has requirement management improved after introducing 60880?
A: Yes, definitely.

*Title:* The Excavation of Software Systems Properties
*Presenter:* Bo Liwång
*Abstract:* (no paper) The presentation gave comments from a regulator on Documentation and Traceability, and included the following main topics:

- The properties of software
- Smart devices
- Definition of Safety Case
- Experiences from Ringhals 2 Modernisation project R2 TWICE
- Overall experiences from Sweden
- Success story (Sweden-Denmark connection)
- International Activities

Q (by MK): About the Forsmark accident, July 2006: Did the operators loose control over plant status?
A: No, they lost control over state of electrical system. The protection system still worked, but some status values could not be read, so the situation was very tricky.

## WORKSHOP SESSION: COFFEE TABLE DISCUSSIONS

A workshop session was arranged covering one general topic about licensing requirements and 5 special topics. Initially, the groups where arranged as given in the figure below. After 15 minutes discussion, the members of the groups were "randomly" switched, while the moderators remained. In the end, the moderators presented the main points raised during the discussions.

| **Group 1**<br>Subtopic 4 | **Group 2**<br>Subtopic 3 | **Group 3**<br>Subtopic 5 | **Group 4**<br>Subtopic 2 | **Group 5**<br>Subtopic 6 |
|---|---|---|---|---|
| Bartha (*)<br>Kropic<br>Opdahl<br>A. Thunem | Heimburger (*)<br>Molner<br>Lauritsen<br>Isaksson<br>H. Thunem | Lindner (*)<br>Savola<br>Dobson<br>Bisio | Liwång (*)<br>Valkonen<br>Katta<br>Berg<br>Miedl | Glöe (*)<br>Hadler<br>Sindre<br>Rasputnig |

(*) Group Moderator

**Topics:**

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

**Subtopic 1, Group 4: Licensing requirements: How difficult are they to interpret and meet?**

There must be knowledge management early in the projects to have the right competence and staffing from the beginning on different topics:

- Planning of the different phases of the project
- Interpretation of different standards. The interpretation depends on the specific project and the context.
- Staff experienced in the different phases shall participate in the overall planning as a input for the transition between phases

Top management must be aware of the importance of:

- Planning (different types: Licensing plans, Requirement Engineering plans, V&V plans, Implementation plans etc.)
- Requirement Engineering and Change Management
- Documentation and Traceability
- Structures of Arguments and Evidences

Licensing issues has so far been much too focused on technical matters and too little on strategies and planning.

Tolls can help with the structuring and traceability of requirements (both licensing requirements and project specific requirements)

It is important to plan the licensing activities depending on different licensing culture, licensing strategies and regulatory context:

- Goal Based Regulation
- Process Based Regulation
- Technical Oriented Regulation

**Subtopic 2, Group 4: The relationships between systems development process and requirements engineering**

The definition of Requirement Engineering is important as well as a defined relationship to the System Design Process:

- An initial requirement engineering followed by a separate continuing requirement activity, or
- An initial requirement engineering followed by requirement activities inside the system design process.

The use of tools for requirement refinement and traceability can be very important.

It is necessary with repeated evaluation of requirement fulfilment in the different phases of the development process.

The separation of initial requirements to requirements on software and requirements on hardware.

An important issue is the requirement change management during the development process. What impact will a change of a specific requirement have on other requirements and on work done in earlier performed design phases. Traceability?

The initial requirement engineering shall incorporate staff skilled in the different development phases.

**Subtopic 3, Group 2: Policies for freezing the requirements and for accepting or rejecting changes**

The "Coffee table" recognized the following ***actors*** in the work process:

- Utilities/Licensees (investor customers)
- Vendors/Product developers
- Regulators (Law and safety requirements)
- Consultants (Independent assessors)
- Marketing/Financial actors
- Certificators

Typically a project has limited time and limited resources and limited amount of money. If a change is needed due to any reason, it means always changes in budget, time-schedule etc. If a resource leaves the project, a lot of changes are required and probably a new time-schedule and more money or something must be rejected or done free of charge temporarily.

***Type and quality of the requirements*** - issue resulted the following:

- Traceability!

- Possible conflicts with other requirements
- Amount of rework? affecting the time-schedule
- Effect of quality (QC and QA)
- Req. spec. = Living document?

***Product type*** was the following discussion theme:

- One product/Mass product (competition/market situation)

***Project- phases*** arose to the key issues for a successful work process (project):

- Very first:
  - Pre-project and/or pilot study
  - Demo
  - Feedback from the users and analysis → Conclusions
- Next phase:
  - A very good contract including e.g.
    - Rules and policies for changes
    - Responsibilities
- Development project:
  - Freeze but be flexible → Flexibility if living requirements spec. document
  - Avoid chaos?
  - Testing, testing and testing (Reserve enough time)
  - Regression testing due to the changes, how much, what, costs, resources…
  - Impact analysis of changes
  - Meetings, meetings…

***Project type*** affect to the work process:

- Waterfall-model
- Spiral-model including waterfall-model in the 4th quadrant
- Turn-key-model (Fixed amount of money and time and product)

**Subtopic 4, Group 1: Approaches for requirements validation and verification (also related to already developed systems and modernisation activities)**

The use of validation and verification

Validation is interpreted as the proof of that the developers specified and implemented "the right system", whereas verification is the proof of that the development process is correct in the sense "the system is built in the right way".
The responsibilities for the validation and verification tasks are not equally distributed between the customer/user (utilities, licensors) and the implementer (developers, vendors).

- Validation is the job of the customer/user
  - The customer must have a sufficient trust in the relevance of the developer's own requirement specification as compared with the customer's initial requirement specification
  - The customer must make sure that the implemented system corresponds to the customer's initial requirement specification
    - On the other hand, validation is not just an Acceptance Test

    - The developers must support the customer in doing the validation activities, as their level of understanding the implemented system is deeper than that of the customer
    - What is to be done is there is no identifiable user? (Examples from the car industry.) Who does the evaluation? The user must be represented by independent departments of the vendor. Usually the Marketing or Sales departments take this role.
        - The trade-offs of the new/revised system must be accounted for
        - Prioritization is a very important issue
        - If it is a modification, feedback from previous models must be used in the process
        - Wrong representation of the user can lead to big failures (such as the WAP protocol in mobile communication) or unexpected successes (e.g. the SMS functionality again in mobile communication)
        - This issue is not relevant in nuclear environments: there is always an identifiable user in these applications

- Verification is the job of the developer
    - The developer must initially check the correctness and completeness of its own requirement specification, and continuously analyse the correctness of the refinement steps and the refined models/specifications during development

There is often a problem with requirement completeness. Can it really achieved in complex systems? We need to define a "feasible completeness". Selecting the right level of detail in the requirements capture process is also an important factor. Tools for filtering capabilities help to show only parts of large-scale complex systems.
Well-formedness of the requirements is another factor to be verified.
During software development the effect of hardware changes cannot be overlooked. There is a "feedback loop" between SW and HW. The problem of hardware upgrades (changed/extended functionality, altered timing, etc.) must be handled.
V&V should be performed incrementally as well

- It must be done as early as possible
    - But there is the problem that the "big picture" is hard to see at the early stages
- Therefore again prioritization is very important
    - Selecting the critical requirements, safety cases

Development could start from a set of core requirements. Then the system would be built up incrementally, while extra care would be put into not violating the core requirements, and the requirements the earlier stage already fulfilled.

- This could also facilitate validation. The core requirements would be validated first, then the development process that lead to the next stage would be verified. Then, in the subsequent stage only the new, additional requirements would be validated while taking care of the verification of the development process. This should guarantee that the already validated requirements would not be violated in the subsequent stages.

In the case of modernization project a very thorough requirement elicitation is a must. If there are several, parallel modernization activities and projects, it is also very important to "harmonize" these activities. That is, to try to be consistent among these projects.

Formal methods in validation and verification

Formal methods (FM) in V&V are difficult to use if the system is very complex and has not been developed by formal specification techniques, so that the system properties are modelled already in an unambiguous manner.

- Simple systems on the other hand usually do not require formal methods
    - They can be covered well enough by traditional approaches, so that sufficient trust can be placed on the system

Formal specification languages such as SDL (and the new extended versions of UML are also converging in this direction) help the analyst to start creating formal models of success stories.
Nevertheless, (exclusive) use of FM and automated code generation from verified formal specification has not become widespread as it was expected and forecasted several years ago. There are many factors contributing to this.
There is a great problem with FM regarding its relationship with natural language ("informal") descriptions. First, formal experts are needed to transform natural language requirements to a formal description. Second, the created FM representation is very hard to understand (if at all) by nuclear experts.

- Suggestion: in the future automated translation processes should be used to convert the formal requirements into natural language
    - Doubts: it is probably very hard to do, but it might not be achievable at all. FM descriptions are concise because they are relying on a vast amount of background knowledge. Leaving this background knowledge out of the created natural language text will make it not much more interpretable as the original FM description. Including it in the created natural language text will make the created text very long and hard to read and thus useless.
    - A limited vocabulary can/needs to be used, but then the expressiveness will be probably too limited
    - There is a problem of separate, not shared knowledge domains between nuclear experts and formal experts
        - Nuclear experts find it hard to interpret the created FM description of the initial user requirements, because of the lack of formal background
        - Formal experts find it hard to interpret the initial textual user requirements, because of the lack of nuclear background
        - This information loss is dangerous to the success of V&V

Automated code generation still helps a lot in V&V:

- It guarantees that after verification was performed properly in every stage of the refinement process, the software product is created in a certified process
- It helps early validation by enabling the customer to examine the future system by simulation before it would be integrated and installed

Not all requirements can be represented formally.

- Some dependability factors are more suitable for formal analysis than others
    - For example, user friendliness is hard to represent formally
- We need to break down the systems according to aspects, functions, modules, components, and identify which ones are suitable for formal analysis, then select the most appropriate formal description/analysis method for that particular problem

**Subtopic 5, Group 3: Defining and classifying dependability-related requirements: Do we really have other kinds of requirements?**

First of all we discussed the second part of the question: Do we really have **other kinds of requirements?**

The answer was a clear "yes, we have". Examples are (without claim of completeness):

- Efficiency
- Portability
- “Outfit” (the design should look good)
- Extra functionality (“gimmicks”)
- Functionality (to a certain extend e.g. a trip-function (measure a value and open a breaker when a set point is violated) can be performed by a toy. If you add dependability requirements the toy can not be used.)

Regarding classes (or may be groups) of dependability-related requirements we identified generic ones like

- Maintainability
- Usability
- Security (including protection from internal attacks, sabotage)

From the example of security, we derived that these requirements may be domain specific. That can hold also for other dependability-related requirements. A bank or an Internet-Shop has other security requirements than a NPP.

There may be also a clustering or a hierarchical order of dependability-related requirements.

**Subtopic 6, Group 5: Terminologies for specifying discipline-oriented (life cycle levels) and domain-oriented (e.g., industrial branches) requirements**

The purpose of this discussion was to clarify whether some common terminologies can be established both across the disciplines related to the development/operation/maintenance process of a specific system (disciplines such as design, implementation, test, maintenance, licensing, operation and decommissioning), and across the industrial domains. The latter was particularly discussed in a more extensive manner. Some participants had examples of activities and projects towards various branches and yet based on common definitions and terms. Other participants believed that this is in practice not possible, as at a certain level, things get too detailed to be relied on a common basis and need to be specialised, also when it comes to definitions and terms. These participants believed also that such common terminology is not needed, or is not the main problem.

**Wednesday, November 29**

09:00-10:00 Paper presentations
10:00-10:30 Discussion
10:30-10:50 Break
10:50-12:00 Main Messages from the seminar discussions
12:00-13:00 Lunch
13:00-14:00 Final session including conclusions
14:00-14:30 Farewell

**1. Session:**

*Title:* An empirical study of introducing the Failure Mode and Effect Analysis Technique to Norwegian business critical software developers

*Presenter:* Torgrim Lauritsen

*Abstract:* This article describes an experiment with three Norwegian IT companies, who develop business critical software. The goal of the experiment was to evaluate if it is beneficial to use safety analysis techniques when developing business critical software. The participants in the experiment tried to identify possible failure modes from a class diagram. Half of the participants used the Failure Mode and Effect Analysis (FMEA) method that is widely used in the development of safety critical systems, while the other participants used ad hoc brainstorming. The number of failure modes is used as an indicator for the effectiveness of each technique. Our experiment showed that the participants that used ad hoc brainstorming wanted a method that could help them to reveal more problems. The participants who used the FMEA method found the method useful because it was easy to understand and helped them to identify failure modes in a structured way.

Q (by APJT): Your results are very dependent on the criteria you have chosen. The results would have been different if FMEA was compared with other techniques or hybrid techniques.
A: Agreed, but the purpose here was to introduce the use of failure modelling techniques and to compare the results to those gained by ad hoc reasoning (no explicit failure modelling), and in that way to convince the potential users on the benefit of failure modelling techniques. It was in that context that FMEA was used (comparing FMEA with "nothing at all" and not with "other failure modelling techniques").

Comment (by APJT): FMEA cannot identify failures. It can only model what you already know about the system. Generally, requirements engineering from the very beginning of a project can contribute to better identification and therefore modelling of the possible failures.
A: Agreed.

*Title:* Requirements Traceability Experiences from SCORPIO Core Surveillance System

*Presenter:* Janne Valkonen

*Abstract:* (Excerpt) The purpose of this paper is to analyse the documentation produced during the development of SCORPIO-VVER core surveillance system for the Dukovany NPP in Czech Republic. The main idea was to search through the documents produced during the different life-cycle phases of the system development and try to analyse how requirements were transferred to design and further on to implementation and testing. The purpose was to examine the traceability of requirements and draw conclusions of the way how the project was carried out from the requirements engineering – especially requirements traceability – point of view.

Comment (JM): It was a very successful project in 1996. We received acknowledgements from the licensing authorities. But we had lots of requirements and lots of back and forth changes, so at the end we lost the track and only focused on the latest and actual requirements.

Comment (ØB): It was a very honest presentation. We decided to limit the number of documents, because of other experiences, that led to that we couldn't deliver the product on time.

Comment (BL): I think it is important to also ask the actual stakeholders about their experience with the progress of the project. Their opinion can be very useful.

*Title:* Qualification of computer-based I&C systems
*Presenter:* Horst Miedl
*Abstract:* (no paper) The project - "Qualification of Integrated Tool Environments (QUITE) for the Development of Computer-Based Safety Systems in NPP" is engaged in the topic of the qualification of computer-based I&C systems.
For the development of safety-related computer-based I&C systems Integrated Tool Environments (ITE) are frequently used. Most of these ITE were not conceived originally for the implementation of nuclear specific applications. The ITE may be proven and certified for industrial applications but the qualification for the nuclear application has to be demonstrated.

For the assessment and qualification of ITE methodical foundations are produced in the view of their application to generate safety-related software for NPP. Therefore different I&C platforms have been analysed and classified with respect to their properties (e. g. safety, security) and services (e. g. code generator, verification and validation tools).

An assessment framework has been developed to qualify ITE in a efficient and transparent manner. The assessment of the ITE's properties and services is carried out in three main steps. In a first step compliance with general requirements for the design of ITE are analysed. Aim of that analysis is the earliest possible determination of its basic suitability. After an affirmative result a detailed investigation of the ITE's properties and services is performed in order to locate potential deficiencies and to evaluate compensating measures.
In the second step requirements on the selection and use of ITE are taken as assessment basis. Dependent on the safety category of the target system implemented by the ITE the international standards, e.g. IEC 62138, supplies these requirements.

In a final step, after successful termination of the second step, a systematic approach is defined to weight the safety relevance of the ITE's properties and services. It can be assumed that services that have an impact on the target system can be classified as pre-developed software. The analysis is based on the requirements and the procedure for pre-developed software as described in the international standard IEC 62138.

The assessment framework is validated with an ITE of an I&C platform. During the validation a lot of heterogeneous information will be obtained, which should be used in an appropriate way for an integral assessment conclusion for the ITE. It is intended to apply Bayesian Belief Networks (BBN) as a means suitable to this end.

Q (by APJT): Are you also evaluating the software development process? Are you using BBN for this? Are you suggesting some metrics for evaluating the development process?
A: Well, we would also like to evaluate them, but it depends on their application and the purpose of using them.

Q (by GG): Why haven't you used available tools for qualifying ITEs?
A: Because we didn't focus on requirements.

Q (by HH): How about internet features with developers distributed around the world?
A: We have not considered this, but we may have security problems with that.

## MAIN MESSAGES FROM THE SESSIONS

### MONDAY:

**Session 1**
*Q to KJ by AL*
ØB: Simulators are typically developed in parallel with project/plant.
BL: Agreed, there should be simulators 1 year ahead of start of operation.

**Session 2**
*Q to GD by BAG*
APJT: The problem with the tool integration is that we often do not have access to the tools in its full shape. One example is CORAS: Although we were project partners and the tool is officially open source, we do not have access to the examples and models developed by other partners (including those developed during the project period). Also, some tools cannot be integrated, due to very different purposes.

ØB: TRACE – a follow-up tool for a project. This is in addition to ITE. It is not clear how to integrate with other tools.
HPJT: Difficult to get vendors to agree on module framework, since they are in competition.
HM: Experience with ITE – users and vendors want independence.
HPJT: Common file formats (XML-based) is a starting point.
HH: Old idea – req. framework for different domains.
APJT: TRACE – common core --> specialisation towards different applications/branches. What we need now are good references.

*Q to RS*
HH: VTT have measurements methods (info security?). Possible to combine safety & security, boundaries between zones... SW must be developed --> zones, onion model, DMZ. Smart devices can cause problems ("I need to update my driver, connecting to internet for download...").
APJT: Common understanding: "we know safety, but security is new". However, many security issues will affect safety.
HH: How to integrate in req.spec. phase?
APJT: Very difficult, especially in beginning of project. Security for I&C systems? "Easy" now, but this may change as systems become more complex.
GS: Disagree with "hen and egg". Both misuse cases and attack trees will have similar problems for large systems, but misuse cases may stimulate creativity, while attack trees are very systematic.
APJT: You model success as seen from attacker's point-of-view.
GS: Level of abstraction, which we haven't solved. Finished system: penetration testing (hacking, social engineering, break-in...). Can we develop a paper-based penetration "system"/guidelines?

APJT: Combination of traceability models + misuse cases can be used to identify level of abstraction.

**TUESDAY**

**Session 1**
*Q to VK by APJT*
APJT: Traceability between techniques/tools... formalise relationship.

*Q to VK by JV*
APJT: How to freeze requirements during the development process? How much dependable requirements are changed during the development process?
ØB: Changes – you know they will come, so the whole design should plan for them.

**Session 2**
No further closing comments.

**Session 3**
ØB: We wrote an HPR on procedures...
BL: An operator may work differently if they have the procedures as paper or in electronic format, even if the procedures are identical.
HH: Good research topic!
ØB: John O'Hara wrote NUREG on this... Must be included in req.spec.
RB: Should keep same layout between paper and electronic.
ØB: Periodic testing, in future self-test built into system, but must have balance.
HH: Must have paper for backup.
BL: General – during licensing process: game with different stakeholders. My view as regulator...

**WEDNESDAY**

**Session 1**
TL: In business critical systems they don't analyse diagrams, but we/they learn from each experiment. They are so focused on success that they forget possible failures.
APJT: Introduce methods gradually (HazOp, FMEA...).
ØB: SAP could be a relevant test system.
APJT: BL's comment very important (ask stakeholders).
HM: No break from req.spec. to target system. Internet: no experience, not feature of tools to be used in distributed way.
APJT: The petroleum industry use tools in distributed manner (eField).

**FINAL SESSION (FOCUS ON THE WORKSHOP SESSION)**

**1. Licensing / certification of reqs.**
BL: It is necessary with good management involvement. What are the licence reqs that should go into overall plan? Branches: what type of lic./cert. strategies? Some goal-based, some process-oriented (both must be converted into activities to satisfy safety cases), some technical-oriented (tech.reqs.).
APJT: IFE is involved with different authorities. It is possible to define common lic.reqs. for comp.systems. When you have your common reqs, then it is easier to develop branch-specific lic.reqs.

**2. System development process (system lifecycle) and req.eng.**
BL: Necessary to present the different initial req.eng. and follow-up req.eng.
APJT: The types of activities are very different for different phases (design, implementation, maintenance...).
HH: ISO 9000: No licensing authority believes in this!
APJT: Oversold, but underused.

**3. Policies for freezing reqs.**
(No comments)

**4. Requirements Validation & Verification**
HM: A formal method does not need to be mathematical. No general solution.
APJT: Different communities use different means.
HH: Semi-formal methods are used.
BL: The basis for a good formal V&V should be a good formal specification. It is difficult to use formal techniques, because specs are not in formal format. Also, if the system is simple, you don't need formal V&V at all..
HH: Authorities will not accept formal V&V, except for control purposes. They regard the application as waste of time and money. 20 years ago, military standard for formal/semi-formal methods was developed and used.
APJT: Clear impression that strength of formal specification methods is more and more accepted within nuclear. Tools with GUIs have been used in many other industries with very good results (telecom, automation and car industry).
BL: Not as pessimistic as HH. I think we can come longer by using semi-formal methods in a structured way.
HM: In Korea, universities do a lot of research on formal methods, but don't know how much is used in industry.

**5. Defining/classifying dependability-related reqs.**
BL: (list a number of factors) All can be defined as dependability-factors, but some may not work without others, or cannot work together (simplicity does not work well with flexibility). Which are most important for a specific project?
GS: Must have terms people can agree on.
APJT: Some factors may be default for all systems, so one does not need to include them.
BL: Safety case --> dependability case.

**6. Discipline/industrial-oriented reqs.**
BL: Possible to develop standard set of reqs for different systems for different domains, just remember it is a subset of the reqs and you must add project-specific reqs.
HM: That is the way we work (generic reqs). All other depend on safety categories etc.
BL: Want real experience/lessons learned on interactions between all "actors". Where are the barriers of misunderstanding between actors?
HH: A 15 year old report is a good model (I&C). Experiences can be gained.
ØB: what should we look at? Also divide into life cycles.

**Bibliographic Data Sheet** **NKS-149**

| | |
|---|---|
| Title | MORE - Management of Requirements in NPP Modernisation Projects. Project Report 2006. |
| Author(s) | Atoosa P-J Thunem[1)], Harald P-J Thunem[1)]<br>Janne Valkonen[2)] |
| Affiliation(s) | [1)]IFE, Norway and [2)]VTT, Finland |
| ISBN | 978-87-7893-212-9 *Electronic report* |
| Date | February 2007 |
| Project | NKS_R_2005_47 / MORE |
| No. of pages | 54 |
| No. of tables | 1 |
| No. of illustrations | 6 |
| No. of references | 6 |
| Abstract | The purpose of the report is to document the work and related activities in the period January 1 – December 31 in 2006, including dissemination activities. The work in this period has been concentrated on further research for adopting an approach for dependable requirements engineering and its supporting tool. The majority of the efforts in 2006, however, was spent on making the researchers, developers, utilities and li-censees more aware of the importance of the area of requirements engineering, and in that respect organising an international seminar on dependable requirements engineer-ing. This seminar was defined as a deliverable in the Activity Plan for 2006 and be-came also the most important deliverable for 2006. Therefore, this report naturally features a detailed summary of the seminar, which proved to be a true success and at the same time a door opener for more initiatives within the topic, proposed by several participants. More efforts within dissemination of the background and objectives of the project MORE within the nuclear community and towards NPPs that do carry out modernisation projects continued to be one important focus. |
| Key words | MORE, tracability of requirements, dependable requirements engineering, TRACE, International Seminar on Dependable Requirements Engineering (Summary) |

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