International Seminar on Dependable Requirements Engineering of Computerized Systems at NPP's
November 27 – 29, 2006
Halden, Norway

Janne Valkonen, VTT Technical Research Centre of Finland

Requirements Traceability Experiences from SCORPIO Core Surveillance System

1. INTRODUCTION

1.1 Background

In software projects, requirements engineering plays an important role right from the beginning of the development process. The requirements engineering process includes requirements elicitation, requirements analysis and negotiation and requirements validation. While following a certain development process, the communication and relations between requirements and different development phases become important issues, which can be called requirements traceability. Requirements traceability can be defined as "the ability to describe and follow the life of a requirement, in both forwards and backwards direction" (Gotel & Finkelstein, 1994). It is the ability to trace requirements in a specification to their origins and descendants via a documented set of linkages (see also Sivertsen et. al 2004).

There are lots of guidelines for requirements engineering process in the literature (e.g. Swebok 2004, Kotonya & Sommerwille 2000). Usually in the descriptions of requirements engineering and software processes, traceability is seen as very important part affecting the ease of maintenance and upgrading of systems. However, the practical world does not always work like described in the books. No matter how well defined a project is, there are always some deviations and things which could not be taken into account in the planning phase.

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.

1.2 Initial assumptions

The initial assumption was that it could be possible to find a clear and well-formed path of development activities, which could be followed throughout the development life cycle. The available documentation covered documents related to: requirements specification, system specification, design specification, unit development folder, and test documents. The contents of these documents are described more detailed in the following chapters.

Due to the large amount of documentation, it was decided to select a quite well-defined (but still extensive) example to start with, instead of exploring the whole system's documentation at the same

time. Based on discussions with people knowing the system well, the man-machine interface (MMI) in the core follow mode was selected as an example.

From the viewpoint of MMI, there are three different user groups:

- Reactor operators
- Reactor phycisists
- System supervisors

All these groups have slightly different needs and preferences what comes to the contents and layouts of user interfaces. From these user groups, the reactor operator's MMI was specified to be the case example, because the other ones were only complementing its contents. The following chapters introduce the documentation that was available for the analysis.

2. THE SCORPIO SYSTEM

2.1 Introduction

The on-line core surveillance system SCORPIO developed at the OECD (Organisation for Economic Co-operation and Development) Halden Reactor Project (HRP) provides capabilities to evaluate the state of the reactor core with respect to operational margins and to predict the future state of the core in power manoeuvres.

SCORPIO provides capabilities to·

- Capture on-line plant signals from the station's data logging system.
- Manage the automatic tracking of the evolution of the core through time using a 3D reactor model – both irradiation and xenon are followed.
- Evaluate the state of the reactor with respect to operational margins.
- Predict the future state of the core in power manoeuvres.
- Present all information to desk operators via a sophisticated graphical interface.

By the end of year 2005, the SCORPIO system has been installed at the Ringhals PWR in Sweden, at Nuclear Electric's Sizewell B PWR in UK, at 7 NPPs of Duke Power Co. in USA, at Dukovany NPP in Czech Republic, Bohunice NPP in Slovakia, and Kola NPP in Russia.

Firstly the SCORPIO system was implemented only for the western PWRs, but later it was developed also for VVERs. The development of the VVER version of SCORPIO was carried out in co-operation with the Czech partners Nuclear Research Institute (NRI), Skoda and Chemcomex, with the NPP Dukovany as the target plant. The goal was to adapt the functionality of SCORPIO to address the particular needs in VVERs. The project was initiated and partly funded by the Science and Technology Agency (STA), Japan through the OECD NEA assistance program.

The core surveillance system has two operation modes: core follow mode and core prediction mode. In the core follow mode, the present core state is calculated based on a combination of instrument signals and a theoretical calculation of the core power distribution. In the predictive mode of operation, the operator can forecast the reactor behaviour under power transient during the coming hours.

More information about SCORPIO-VVER core surveillance system can be found e.g. from (Zalesky, 1997).

2.2 Documentation of the SCORPIO-VVER MMI in Dukovany

During the development process of the SCORPIO-VVER, the following documentation of "Core follow mode MMI for reactor operators" was produced:

- Project and Quality Plan (PQP)
- Specification of requirements for Core-Follow mode of SCORPIO-VVER concerning MMI for reactor operators (Specifikace požadavků SPZ 02.96)
- System Specification Document - VVER Core Surveillance system (Dokovany target plant)
- System Design Document - VVER Core Surveillance system (Dokovany target plant)
- Unit Development Folder - Man Machine Interface VVER Core Surveillance system (Dukovany target plant)

The following subsections will go through the documentation and the parts of them, which are related to the core follow mode's MMI for reactor operators.

2.2.1 System specification document

The system specification document gives a general description of the core surveillance system for VVER reactors. The document defines the project goal and describes the main features expected from the system. The document says that NPP Dukovany will introduce the basic requirements. The document called "Specification of requirements for Core-Follow mode of SCORPIO-VVER concerning MMI for reactor operators" is that one and it is introduced in the next section.

System specification document gives a system function definition defining the necessary system modules, which are presented in a block diagram. The system is divided into two parts: 1) the core follow mode and 2) the core predictive mode. This analysis will concentrate on the core follow mode.

The system specification document also defines the computer environment and platforms, on which the system should run. The document does not talk much about MMI. It only defines 3 different user groups for the system and lists the most important information related to them. The user groups are 1) operators, 2) reactor physicists, and 3) system supervisors. This analysis concentrates only on the operators' MMI. The system specification document lists the contents of the overview displays as follows:

- Summary of key parameters related to core monitoring
- Summary of information from the primary circuit
- Distinguish between validated data and bad values, measured values, calculated values
- Diagnostic information on sensors and data acquisition system (Hindukus[1])
- Margin to limits
- Radial power distributions

[1] Hindukus is the name of the old core surveillance system replaced by SCORPIO.

- 2D distribution of temperature rises, margins to limits
- All new calculated limits associated with 2D distribution presentation
- Trends of key variables
- Specific display of axial power distribution
- Summary of information from PES (PCI-margin calculation) and PEPA (Primary Coolant Activity Prediction)
- Standard output display for key results of power transients and critical parameters, margins to limits, e.g. critical boron concentration during start-up.

2.2.2 Specification of requirements for Core-Follow mode of SCORPIO-VVER concerning MMI for reactor operators

The document called "Specification of requirements for Core-Follow mode of SCORPIO-VVER concerning MMI for reactor operators" was written by the representatives of the Dukovany nuclear power plant in Czech Republic, where the system was delivered after the development project. The document introduces the general concept of MMI for reactor operators and presents the basic requirements for the hierarchy and type of displays.

The document describes the main ideas concerning MMI but it is lacking explanations. There is a structure of headings describing the most important topics but the text itself is a bit unclear. The actual requirements are among the text describing the features expected from the system. Basically, the text has to be read carefully and requirements have to be collected from it, because they are neither numbered nor expressed very clearly.

The reader gets an impression that the document is written only by the engineers from Dukovany and there has not been many discussions between the authors and the system developers at that stage. The specification gives an impression that it is written as a first vision of the system and it is meant to be the first draft of the requirements document. The revision history of the document is missing, which implies that there have been no revision rounds and iterations with the document.

2.2.3 System design document

The system design document first introduces the scope of the system and its main modules. In addition to rough top-level design description, there are detailed module interface and data processing descriptions of different parts of the system.

The general MMI philosophy is described in the document with definitions of screen layout, screen input, operation modes, and MMI's of different user groups (operator, reactor physicist, and system supervisor). The design document doesn't go deep into the details of MMI but it introduces the main principles of screen layouts and the contents of different parts of screens. The document called "Unit Development Folder - Man Machine Interface VVER Core Surveillance System (Dukovany target plant)" deals with MMI more accurately and basically collects all the information to a one document. It is introduced in the next section.

2.2.4 Unit development folder

The unit development folder (UDF) is a document gathering the most important things related to a specific module meaning that all information (or references) related to that module will then be found

in one document. The document is named “Unit Development Folder - Man Machine Interface VVER Core Surveillance System (Dokovany target plant)” and it begins with references to requirements specification. It unfortunately does not list the actual requirements again with better accuracy than the requirements specification.

The design of MMI is introduced in UDF in a more detailed level than in the System design document, which concentrates more on general issues like module interface and processing descriptions of different parts of the system. UDF describes the detailed design of MMI with all necessary information about the data structures, variables, colours, fonts, objects, screen layouts and pictures.

UDF also gives descriptions of directory structures, configuration files, window definitions and picture properties. The tests of MMI are done by using pictures, which means checking that correct signals are displayed and operational functions inside the pictures are according to the specifications. Also the soundness of layouts is checked. The following tests are included:

- Unit test
- Integration test
- Function test
- System test
- Acceptance test (Factory Acceptance Test)
- Installation test (Site Acceptance Test)

2.3 Timeline of documents

As described in the sections above, many documents were produced during the development of SCORPIO-VVER. The documents which are dealing also with the MMI can be set on a time line according to the start point of writing. The first document started was the “Project and Quality Plan (PQP)”, which describes the general issues related to the project organization, quality inspections and also defines the schedule of the project. After PQP document, the Dukovany engineers had written the requirements specification, which was followed by the system specification. A long with writing the system specification, the Unit evelopment folder (UDF) of MMI was established and updated almost until the end of the project a long with the development. After finishing the system specification, two parts of the system design document were started concurrently. The last documents related to the MMI were test plans and test reports written at the end of the project.

3. TRACEABILITY ANALYSIS

Requirements traceability is of prime importance to activities such as ensuring that the system and the software conform to their changing requirements. Practitioners consider it often as a problem area. Another typical problem area is the lack of ability for locating and addressing the requirement sources and the work done before the current project at hand. That is mainly because projects are large and there are huge amounts of documentation as a basis of producing a requirements specification.

3.1 Scale of the SCORPIO-VVER MMI development project

Developing the SCORPIO-VVER was a large project which involved five companies including the end user Dukovany NPP and the system’s main developer IFE/HRP. The project comprised of more than

ten man years during three project years, out of which almost one year was used only for maintenance, inspection and fixing small errors. This gives an impression how large the project was and how much documentation there was produced. The next section gives some comments and analysis about the MMI module of the SCORPIO-VVER system. The other modules of the system are not included in the analysis.

3.2 Analysis and comments

As the previous sections mentioned, there are some typical problems related to traceability, which are emerging especially in large projects. Some of these problems came true also with this Dukovany case. Even though the project was successful, both financially and within the results, examination of the project material reveals some things, which could have been done better in other ways.

In this Dukovany case, the starting point for the MMI development is the requirements specification, which is written on a quite superficial level. It can be seen easily that the document is like a first draft of ideas describing only how the customer would like to see the system. There is no numbering of requirements because the document is written in prose. The specification is like a general description of desired features of the MMI rather than a well-defined requirements specification. The requirements are neither expressed very clearly and extensively nor following the good practise of writing requirements specifications. It can also be seen that the requirements specification document has not been written with iteration rounds and there has not been many discussions and negotiations between the stakeholders before finishing the specification. This became clear also after discussions with a person who participated in the development of the SCORPIO-VVER.

The system design document's MMI section has clearly some connections with the requirements specification of MMI. Design document sums up the available operation modes and different user groups. It also defines roughly how user input can be inserted by using mouse and keyboard. However, these things have not been mentioned in the requirements specification, which breaks the traceability links already in the very beginning.

The unit development folder finally clarifies the MMI design and explains the window and screen layouts, colours, fonts and functions under soft keys. It also defines accurately the information presented in different pictures with variable labels, limit values and sizes of data structures. The detailed design part of the unit development folder offers more information about MMI than the requirements specification and design specification. In addition, the information is more detailed and better structured.

It is obvious that there have been many undocumented work phases between writing the requirements specification and unit development folder documents of MMI. An interview of a member of the development group reinforced this idea: Customer's needs and requirements had been discussed in several meetings and emails during the development process. The final version of the unit development folder is thereby a result of several iterations, which can be seen also from the document's revision history. The refinement of requirements, which had taken place after writing the requirements specification document, had been taken into account during the design phases of MMI. That explains partly why it is difficult to find traceability from requirements to design.

The requirements specification document was not updated during the project due to lack of resources. There simply had not been enough time to do that along with the development. The changes of requirements were documented in meeting minutes and emails or they remained as tacit knowledge. Unfortunately the unofficial documentation (notes, memos, emails) was not available for this analysis because the old archives were already destroyed.

The problem of undocumented information is typical in large projects. In general, it is not difficult to see which option is selected in most cases, if the options in a project are: 1) Finish in time and stick to the budget without internal documentation. 2) Finish the internal documentation and deliver late with exceeded budget.

4. CONCLUSIONS

The analysis of this case shows that the practise is quite often far from the theory. There are several methods and processes for requirements engineering and requirements traceability in the literature, but their practical utilization in real life projects is not always easy or possible. Sometimes the budget or the schedule of the project doesn't allow detailed documenting practises even if there is a risk of loosing time and money later because of the missing documentation. That was partly true in the Dukovany case. One reason for the inadequate level of documentation must be the fact that the core surveillance system itself doesn't have safety significance and there is no regulatory control over the development process. Also different organisation cultures between the customer and the supplier may have affected on the project practices and the ways of changing information and documenting changes.

This Dukovany case was successful with regard to the financial issues and also with regard to the schedule, even if the requirements process seemed to be more or less missing. The skilled and devoted personnel, who took care of the project management and software development, must have been in key role with the success of the project.

The situation with the missing documentation and inadequate reasoning with regard to requirements has not been as bad as it looks like from the first sight. Large parts of the project activities and changes were documented unofficially in the emails and notebooks but e.g. phone conversations are not easy to document unless someone sums up the conclusions right after the conversation. The documentation of the project should be done in a structured way so that the development phases could be easily followed also after the project or by someone not actually involved in the project.

However, it is very difficult to get the idea what the system is about, if one starts reading the requirements specification without seeing the actual system working. Based on that we can ask how much easier it would have been for the developers if there was a sufficient requirements specification as a basis of development. At least they could have avoided some early phase discussions and possibly the trial and error development would have not taken error steps.

5. SUGGESTIONS FOR FURTHER WORK

This paper describes only one example where the requirements traceability was not on a good basis. Still, the project was successful. It might be beneficial to make further research on the subject and take a look at some similar projects with success or failure and try to characterize the building blocks of a successful or disastrous project. Every project is different but the difference between success and failure may be smaller than expected.

6. REFERENCES

Zalesky, K., Svarny, J., Novak, L., Rosol, J., Hornæs, A., (1997), SCORPIO-VVER Core Surveillance System, International Topical Meeting on VVER Instrumentation and Control, Prague, Czech Republic, April 21-24, 1997

Gotel, O., Finkelstein, A., An analysis of the requirements traceability problem, in: Proc. IEEE International Symposium on Requirements Engineering, IEEE Com-puter Society Press, Colorado Springs, Colorado, April 1994, pp. 94-101.

T. Sivertsen, R. Fredriksen, A. P-J Thunem, J-E. Holmberg, J. Valkonen, O. Ventä, Traceability and Communication of Requirements in Digital I&C Systems Development. Project Report, NKS-91, ISBN 87-7893-149-5. Nordic nuclear safety research, NKS, 2004

Swebok, Guide to the Software Engineering Body of Knowledge, Eds. Abran, A. & Moore, J.,W.,IEEE Computer Society, ISBN 0-7695-2330-7, 2004 Version

G. Kotonya and I. Sommerville, Requirements Engineering: Processes and Tech-niques, John Wiley and Sons, 2000