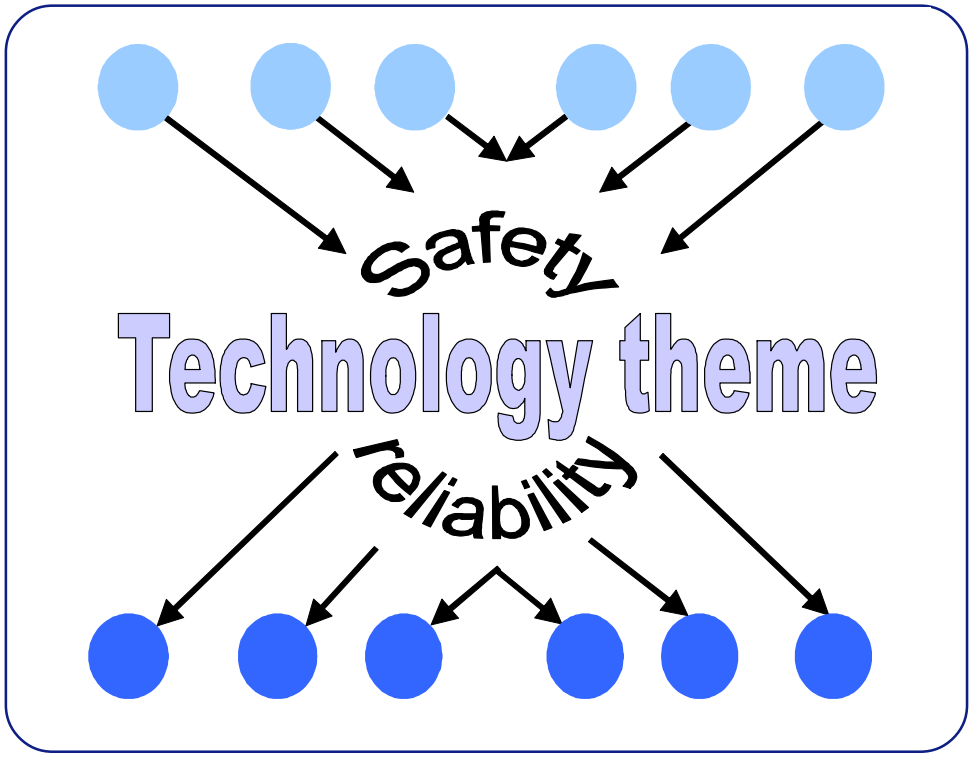

Safety and reliability

Technology Theme,
description of the programme

VTT TIEDOTTEITA – RESEARCH NOTES 2270

Safety and reliability
Technology Theme, description of the programme

Veikko Rouhiainen (ed.)
VTT Industrial Systems

ISBN 951–38–6513–4 (soft back ed.)
ISSN 1235–0605 (soft back ed.)

ISBN 951–38–6514–2 (URL: http://www.vtt.fi/inf/pdf/)
ISSN 1455–0865 (URL: http://www.vtt.fi/inf/pdf/)

JULKAISIJA – UTGIVARE – PUBLISHER

VTT, Vuorimiehentie 5, PL 2000, 02044 VTT
puh. vaihde 020 722 111, faksi 020 722 4374

VTT, Bergsmansvägen 5, PB 2000, 02044 VTT
tel. växel 020 722 111, fax 020 722 4374

VTT Technical Research Centre of Finland, Vuorimiehentie 5, P.O. Box 2000, FIN–02044 VTT, Finland
phone internat. + 358 20 722 111, fax + 358 20 722 4374

VTT Tuotteet ja tuotanto, Tekniikankatu 1, PL 1306, 33101 TAMPERE
puh. vaihde 020 722 3111, faksi 020 722 3282, 020 722 3499, 020 722 3493

VTT Industriella System, Tekniikankatu 1, PB 1306, 33101 TAMMERFORS
tel. växel 020 722 3111, fax 020 722 3282, 020 722 3499, 020 722 3493

VTT Industrial Systems, Tekniikankatu 1, P.O. Box 1306, FIN–33101 TAMPERE, Finland
phone internat. + 358 20 722 3111, fax + 358 20 722 3282, + 358 20 722 3499, + 358 20 722 3493

Technical editing Maini Manninen

Otamedia Oy, Espoo 2004

Safety and reliability. Technology Theme, description of the programme. Rouhiainen, Veikko (ed.) Espoo 2004. VTT Tiedotteita – Research Notes 2270. 79 p.

Keywords safety, reliability, dependability, risk analysis, diagnostics, monitoring

Abstract

"Safety and Reliability" is one of the four strategic Technology Themes of VTT. In this theme, technologies, system models, and measurement, modelling and estimation methods are developed for the Finnish industry's needs. The results are applied to the development of safety and the life-cycle management of socio-technical systems. Under the theme, the know-how encompasses the fields of safety engineering, risk management, system engineering, machine diagnostics and monitoring, psychology, microbiology, and management of safety and dependability knowledge.

The research in the theme will be focused on

- methods for life-cycle management
- Human-Technology Interaction (HTI) and safety
- new technologies and operating principles.

The evaluation of the Technology Themes was carried out in 2004. For this, each project developed a status report describing the research carried out and results achieved. This report compiles the reports developed for the evaluation in the projects of the Safety and Reliability -Technology Theme.

Foreword

"Safety and reliability" is one of the four Strategic Technology Themes of VTT. The Themes are multidisciplinary research programmes initiated by VTT, and aim to achieve significant scientific and technological improvements. The projects of these programmes are representative of a high international standard and are also expected to raise the level of VTT's other projects – paving the way to technological breakthroughs and innovations. The projects of the Technology Themes reached the start-up phase at the end of the year 2001. Ambitious goals have been set for these projects over a period of several years. The aim of the themes is also to promote networking with the best partners and enhance synergetic co-operation within VTT.

As an externally focused innovation organisation, VTT highly appreciates external evaluations as a unique and invaluable source of obtaining new impulses, views and well-considered recommendations. As the projects will have been running for around two years, the year 2004 was chosen for the intermediate evaluation procedure.

This report compiles the reports developed for evaluation in the projects of Safety and Reliability -Technology Theme.

The authors would like to thank all the organisations and individuals who have taken part in the implementation of the projects of the Safety and Reliability theme for their excellent co-operation.

Tampere 14.10.2004

Authors

Contents

1. Safety and reliability – Technology theme; Status report

Veikko Rouhiainen

1.1 Introduction to the safety and reliability theme

1.1.1 Aim and pursued impacts of the theme

The purpose of the theme is the reasonable and safe interaction of humans and technology without surprising disturbances and failures. In the safety and reliability theme, technologies, system models, and measurement, modelling and estimation methods are developed for the Finnish industry's needs. The results are applied to the development of safety and the life-cycle management of socio-technical systems.

The impact of the theme is mainly indirect, seeing that all projects do not themselves develop safer technology. The main focus of the theme is on improved safety and reliability and this is obtained by developing tools, methods and procedures that will help our customers develop the safety and reliability of their technical systems.

VTT is today active in several fields of high safety and reliability related scientific and technical competence, e.g. fatigue testing, reliability analysis, hazard analysis, human behaviour studies, safety analysis, condition monitoring, reliability design, but these fields have mainly developed their skills separate from each other. Improvements in the safety level will require the integration of these competencies, together with modern information technology, in order to meet the future needs and to generate new products for networked large companies and SMEs. Under the theme, our know-how encompasses the fields of safety engineering, risk management, system engineering, machine diagnostics and monitoring, psychology, microbiology and management of safety and dependability knowledge.

1.1.2 Why this theme?

Safety and reliability is an appropriate area to be a technology theme because:

- it addresses major societal needs – to improve the safety and security in a society that is more and more dependant on products and procedures with ever increasing complexity, vulnerability and uncertainty

- it is challenging both from a scientific and an implementation point of view

- it is largely multidisciplinary and needs the critical mass from bringing together the high level research groups and industrial expertise

- the challenging goal of improving safety can only be achieved through the efforts of a large, integrated and multidisciplinary action that contains research and technological development, as well as development of new operating procedures.

In today's society there are several trends and new features that increase the complexity, vulnerability and uncertainty in activities related to the society itself, industrial production, and peoples' use of new products and technologies. The **increasing complexity of technical systems** and products makes them more difficult to understand, monitor and control. They are thus more vulnerable to both internal failures and malfunctions as well as to external destructive attacks.

Financial losses from accidents, damages and unforeseen production interruption may be considerable. Unexpected hazards in technical systems may result in the loss of human life and environmental pollution in addition to impaired industrial competitiveness and image. There have recently been several large accidents in Europe such as the explosions, fires, transportation accidents, aircraft crashes at the airports, and railway accidents. The use of advanced new technologies has resulted in an extensive range of problems, e.g. in some new airports.

The **economic impact of accidents** is huge. The total costs of accidents in the EU is estimated to be about 170 billion Euro for the European societies, and of that is the cost for labour accidents 20 billion Euro. From a ten year perspective, it has been estimated that 10% of these accidents could be avoided.

Major industrial **economic losses** are also due to disturbances and failures resulting in **shutdown of the production and function.** The overall economical losses for lost production due to shutdown and malfunctions have been estimated to be 7% of the turnover. Examples of one day shutdown costs for different commercial functions include: paper plant 500 000 Euro, power plant (coal) 100 000 Euro, oil refinery 500 000 Euro, cargo ship 5 000 Euro, train 2 000 Euro, and design office with 100 employees 4 000 Euro. The overall losses due to lost profit as a result of shutdowns, decreased efficiency and quality (OEE Overall Equipment Efficiency is about 70–80%) in Europe are about 140 billion Euro annually.

1.2 Strategic importance of the theme

1.2.1 Links to VTT's technology strategy

This chapter discusses the general importance of the theme. The focus areas and projects of the theme are described in more detail in Chapter 3.

The safety and reliability theme has a central position in VTT's technology strategy. It has close connections to three focus areas of VTT's strategic research: safety and reliability, tools for information society, and industrial biotechnology. The theme will increase collaboration and links between these focus areas. For example, when developing the methodology for microbiological risk analysis for the paper industry, the expertise from reliability engineering has been complemented with expertise from the field of biotechnology.

VTT's technology strategy highlights nine key technology actions (KTA). The theme has the following close connections to these:

- Human-Technology Interaction (HTI) is one KTA of VTT. HTI and safety is one of the focus areas of this theme, and indicates that that the theme covers this very important part of that KTA.

- The second KTA that has close links to this theme is safety and security of the built environment KTA. This is one of the areas which has been selected to be a possible area for widening the scope of this theme. It will utilise expertise related to systems engineering and probabilistic risk analysis. The leader of this theme is involved in the planning team of this KTA.

- The asset management KTA will also have close connections to life-cycle management, which is another focus area of this theme.

The theme also has many links to the focus areas of different Research Institutes of VTT. In VTT Industrial Systems, such strategic focus areas are, for example, Life-Cycle Management of Structures, Risk Management and Systems Safety, Human-Technology Interaction, and Factory of the Future. This theme has close connections to the focus area Risk Management and Systems Safety, because the theme leader also leads that focus area. Other Research Institutes have also the same kind of connections to this theme.

1.2.2 Extent and volume of the theme

The amount of the financing for the safety and reliability theme may be warranted, when taking into account that the theme does not cover all research carried out in the areas of safety, security and reliability. The total amount of the funding used in these areas is very difficult to estimate. Safety is a very broad area, and much research related to it is carried on outside the theme. This theme concentrates on three focus areas.

When considering the extent and volume of the theme, two questions arise:

- If the research carried on outside the theme would be conducted within the theme, would it be more effective? Should the theme have more focus areas?

- If more financing would be directed to the selected focus areas, would the research be more effective? In some areas the progress would proceed more rapidly, if the projects had more financing. However, the issue of the amount of available experienced resources might be raised, and this might also be problematic.

The Scientific Advisory Board of the theme has discussed the coverage of the projects and stated that more resources could be directed to public safety. For example, very large and complicated systems of society might be vulnerable, e.g. telecommunication systems, electricity networks, etc. The steering committee of the theme has accepted that connecting the following new areas to the theme can be considered and prepared:

- asset management (a Key Technology Action of VTT)

- safety and security of the built environment (criminality, terrorism, biological weapons and diagnostics related to them, possibilities of wireless data transfer and digital image processing).

1.2.3 International technological breakthroughs

In the following areas, the research is very close to the international top level, and world-class results are expected in:

- Driver Monitoring Techniques (already participating in two European Integrated Projects, and a third is in the planning phase)

- Offshore Vessel Traffic Service (VTS) system (the VTMIS, Vessel Traffic Management and Information Service to be developed will be at the top-most level)

- Self-Diagnosis and Prognosis System of Machines (the international machine diagnostic centre has already started).

It is difficult to identify which areas possess the most potential for international technological breakthroughs. What is a breakthrough? How it is defined? And what are the criteria for it? At the moment the Driver Monitoring Techniques project has raised the most international interest and increasing international activity.

1.2.4 Are the projects scientifically and technologically challenging?

The following research areas are thought to be the most scientifically and technologically challenging:

- Unobtrusive Driver Fatigue Monitoring is an area where a lot of research has been conducted, however applicable systems have not yet been developed.

- In the FI-TOOL project the concept to be developed is quite clear for the researchers, however, the problem involves persuading industry (machine manufacturers) of the value in utilising this kind of system and developing practical applications.

- Risk Assessment of GMO's is a very new area, and generally accepted methods are not available. The most remarkable problem is that there is no practical data related to the risks available. A new methodology has been developed, but it is difficult to get international acceptance for this kind of new approach. A new approach and guidance for risk assessment of GMOs has been developed, published, and accepted into use in Finland.

The Scientific Advisory Board has ranked the projects, and especially the projects SYSTELI (Systems Analysis in Management of Plant Lifetime and Production Safety) and METODI (Human-centred design methodology for human-machine systems) also received a high-level ranking for novelty and ambition (impact).

1.2.5 International level

All the projects in the theme aim to achieve results of international level. This is assured by visiting other international research institutes, attending conferences, and developing contacts with internationally high level researchers. The international contacts are presented later in the chapter on networking, and further details are in the project reports. It is noticeable that the theme projects have increased the amount of international contacts and internationality. At the moment, the most active international networking is in the following projects:

- SYSTELI (thematic networks, researcher exchange to and from VTT)
- LIIKKUDIA (International Machine Diagnostic Centre)
- METODI (researcher exchange from VTT)
- VTS (fixed networking with Russian and Estonia)
- SYKE (two European IPs accepted, one under preparation).

One point which could be developed further is the cross-utilisation of this international contact network in all research projects. A lot of information is also available through the thematic networks, however, the problem is the lack of resources for distributing and utilising all this information.

1.2.6 Impacts of the theme projects

When planning the theme a clarification was made about the areas, in which disturbances (unreliability) and accidents result in the largest losses. This is referred to in the introduction of this report. The aim was to start projects in those areas.

The Scientific Advisory Board has ranked the projects and in this issue the highest ranking was given to FI-TOOL and GMORA. In the FI-TOOL project the area and field to which the results of the project can be exploited is deemed to be very wide, while GMORA is directed at a very new area where not many tools are currently available. A high ranking was also given to the SYSTELI and METODI projects.

Good examples of the impacts can be found from the results of the following research projects:

- The VTS project is developing a VTMIS simulator, which is a combination of different research and training simulators in Finland, Russia, and Estonia. It offers an international platform for maritime safety research and for planning and further developing the harmonised trilateral operation in the VTMIS area.

- In the LIIKKUDIA project, the Machine Diagnostic Centre has been created. It offers a platform for the development of remote diagnostics and prognostics within an international network.

- In SYSTELI, a risk assessment model for performing and maintaining Hazard Analysis and Critical Control Points (HACCP) analyses and a self-checking system in the pulp and paper industry has been developed. It has been presented at international conferences, and has received very positive feedback.

- Driver impairment monitoring system has been seen to offer possibilities for improving traffic safety. Results may have applicability also in monitoring areas other than road traffic.

1.2.7 National and international networking

Safety and reliability can not be developed in the laboratory alone. The research has to be fixed to real operating systems or products. When planning the projects, the case and object areas were selected to represent of high international level. That way the pursued results should also be world-class.

In research, the first phase in networking occurred inside VTT, and this is naturally extended in the direction of Europe. Systems engineering and the HTI area have also started networking towards the USA and Canada. And the Machine Diagnostic Centre has started collaborating also with Canada and Australia. Collaboration with Kyoto University in Japan has also been started.

The current active contact net, based on the all the researchers and the projects of the theme, includes many research institutes, thematic networks of the EU, and associations, etc. One good example of the extent of these networking activities is the ESReDA Seminar (European Safety and Reliability Association) – organised by VTT in Tampere 11–12 May 2004.

European research organisations have organised thematic networks for collecting together expert organisations in each area. The theme has contacts in at least the following European networks:

- SAFERELNET, Thematic Network on Safety and Reliability of Industrial Products, Systems and Structures: http://mar.ist.utl.pt/saferelnet/

- S2S, a Network on Plant and Process Safety: http://www.s-2-s.org/

- RIMAP, Risk Based Inspection and Maintenance Procedures for European Industry: http://research.dnv.com/rimap/

- SAFETYNET, a Network on Process Safety: http://www.safetynet.de/

- HARSNET, a thematic network on Hazard Assessment of Highly Reactive Systems: http://www.harsnet.de/

- PRISM, Process Industries Safety Management: http://www.prism-network.org/

- INID, Research Organisations and Diagnostic Centres dedicated to developing and enhancing research on condition monitoring, diagnostics and prognostics

- HUMANIST.

Especially noteworthy is the fact that SYKE has been increasing networking with automotive industry and other related industry. This occurred mainly as a result of planning three European Integrated Projects.

1.2.8 Synergetic collaboration inside VTT

Collaboration with different research institutes of VTT had already been started while planning the theme. Three seminars were organised and researchers from all of VTT's research institutes participated. All of VTT's research institutes currently participate in the theme projects. Nowadays a commonly accepted opinion among researchers is that the theme has increased the real collaboration between VTT's institutes in the focus areas of the theme.

Practical collaboration has also been made, for example, when Safety and Reliability theme together with the planning team of the Human-Technology Interaction KTA were preparing the VTT Roadmap, Human-Technology Interaction Research and Design. It was published in December 2003.

The focus areas have increased the collaboration between the theme projects. In life-cycle management, the systems engineering and probabilistic approaches developed in SYSTELI can also be utilised in LIIKKUDIA. The data management system developed in FI-TOOL can support the management of monitoring data needed by the tools developed in both LIIKKUDIA and SYSTELI.

Projects related to HTI and safety focus area also form a project cluster. The Core Task Analysis method was developed further in METODI, and is utilised in mining machines. The same approach has been used when developing operating principles in the VTS system. Also the CABIN project will utilise this method.

1.2.9 Implications of the theme to other research at VTT

Until now, the effect of the theme research on other research at VTT has not been extensive. This is partly due to the time span of the themes, which has been presented to be several years. A preliminary plan has been developed about how the results of the theme would be utilised in research institutes.

Some results of the theme have already taken into use. One example is the microbiological method developed in the SYSTELI project to identify harmful bacteria in paper and paper board. It has been taken into use in research projects and industrial services.

The vision of the METODI project is to be the impetus for a major change in Human-Technology Interaction. The developed human centred design methodology will be widely applicable in designing products and production systems.

1.2.10 Mutual synergy between the themes

There has not been very much collaboration between the themes to date. It seems that more mutual synergy could be found and more collaboration could be initiated in the following areas:

- intelligent package (ÄLYPAKKAUS) (system IDs and TAG, systems engineering, safety and reliability of transport systems)

- wireless data transfer (wireless transferring of data needed in condition monitoring and diagnostics).

Collaboration has already started, for example, in the intelligent package project (ÄLYPAKKAUS) application of TAG device in active communicating packing systems.

Methods and tools developed for assuring safety and reliability would perhaps be more widely applicable in the projects of the other themes. The other themes are mainly focused on developing new technologies, whose reliability and safety could be assured with the tools developed in this theme.

1.2.11 Theme from the viewpoint of the customers

The results of the theme can be utilised in many application areas: large-scale systemic risks, occupational accidents, as well as production disturbances; in different kinds of industries: the process industry, metal industry, machine construction, energy production; and in transport infrastructures: marine transport, railway, automotive. New generic methods, tools and techniques for risk management are being developed, tested, and validated in several of those application areas. The applicability of the results is wide and the methods and knowledge can be transferred and utilised also in other application areas such as the food and construction industries.

While planning the theme, the needs of the customers were also taken into account. Four working groups were collected from the industry in order to define the goals of the theme. They represented the following industrial fields:

- working machines
- pulp and paper industry
- chemical industry
- transport and logistics.

These working groups had several meetings for defining the future needs and visions which affect, and which should be considered, when planning the theme and the theme's projects.

Discussions with the customers have continued also after the start of the theme. Meetings have been organised also for different customer groups for the purpose of exchanging information about research results and customer needs. An example of this kind of activity is a meeting related to sea traffic, maritime safety, and safety of transport, which was organised in February 2004 for the Finnish Maritime Administration.

1.3 Contents of the theme

Research carried out in the theme is in accordance with the three focus areas: life-cycle management, Human-Technology Interaction and safety, and new technologies and operating principles. The research itself is conducted in projects. The goals and objects of the focus areas are:

- Increase the profitability of production systems by improving their reliability during their life cycle. The projects are related to the prevention of hazards and accidental disturbances in movable working machines, as well as in paper and energy production.

- Implement Human-Technology Interaction so that the user is taken into account already when planning the system. The case areas include road and marine traffic, and the mining industry.

- Develop technologies and applications for monitoring the system and the operator. The aim is to utilise this information in operation and maintenance, and when assuring safety.

Referring to the status reports of the projects, the major goals have all been obtained. The projects have mainly continued from the start of the theme. Only one project has been suspended – the risk analysis of GMOs. In that case it became obvious that the international top level results could not be obtained with the available resources, and the project could not find industrial partners, customers, and public funding.

The following section discusses the main aspects of the focus areas. The contents of the projects, as well as the results have been discussed in more detailed in the individual project reports.

1.3.1 Methods for life-cycle management

Three projects are running in this focus area:

- LIIKKUDIA – Monitoring and Diagnostics: Lifetime Management of Mobile Machinery

- SYSTELI – Systems Analysis in Management of Plant Lifetime and Production Safety

- FI-TOOL – Management of safety and reliability knowledge during the life cycle of working machines.

In SYSTELI, system technical methods are being developed to support safety and dependability studies. The methods combine historical data and measurements, and the predictions of probability-based failure and condition monitoring models. In FI-TOOL, a data management system embedded into the machines and devices is being developed for the management of safety and dependability knowledge. The system covers the entire life cycle of the devices and production systems. In LIIKKUDIA the self-diagnostics of the work machines is being developed so that the machine will be able to diagnose its own condition and send the diagnosis, measurement data, and maintenance order to a remote supervision centre.

The most significant results expected are the following:

- System analytical models and approaches have been developed and tested for multi-criteria decision making related to safety and reliability (SYSTELI).

- Related to microbiological production safety in pulp and paper industry, a bacteria identification method has been developed including the rapid screening for the presence of bacteria. This results in a shortening of the time needed for obtaining the results from several days to only one day (SYSTELI).

- A knowledge management system at the conceptual level is currently in the testing phase (FI-TOOL).

- One employment invention concerning video monitoring of a production line using wireless technology has been made and accepted (FI-TOOL).

- The Machine Diagnostic Centre has been created at VTT. It offers a platform for the development of remote diagnostics and prognostics within an international network (LIIKKUDIA).

1.3.2 Human-Technology Interaction (HTI) and safety

Three projects are running in this focus area:

- METODI – Development of a human centred design methodology for human-machine systems: Remote operation of mining machines as a case study

- VTS – Offshore VTS (Vessel Traffic Service) for the Gulf of Finland

- CABIN – New interfaces in the cabins of the future in movable machines and vehicles.

In METODI, a methodology for the evaluation of man-machine systems is being developed. The methodology will include the principles and criteria needed for the development of different types of man-machine systems. The new methodology will be developed in the research on the remote use of mining machines. In VTS, a training system utilising several simulators and virtual technology is being developed in order to support the implementation of the vessel traffic management and information service (VTMIS). In CABIN, a new generation of user interfaces of movable machines and vehicles, which utilise the newest information and communication technologies, is being developed.

The most significant results expected are the following:

- Knowledge about available HTI research, as well as the applicability of existing and new methods used at VTT to different HTI problems has increased (METODI).

- A preliminary model, "Human-Technology Interaction design process" for integrating HTI issues into the technical design process of automated mining has been developed (METODI).

- A Formal Safety Assessment (FSA) was conducted and submitted to the International Maritime Organisation, IMO (VTS).

- A Technology Road Map has been developed and the summary of the needs collected from the companies (CABIN).

1.3.3 New technologies and business concepts

Three projects are running or have been running in this focus area:

- SYKE – Unobtrusive Driver Monitoring Technologies

- TRUST – Trusted Software Technologies

- GMORA – Risk Assessment of Genetically Modified Plants.

In SYKE, unobtrusive monitoring methods for driver fatigue detection is being developed. They will be based on the integrated use of EMFi technology and other sensors. In TRUST, a knowledge management system that enhances the ability to utilise specific methods and techniques to design and demonstrate safety and reliability of

software is being developed. In GMO, a framework for the risk assessment of genetically modified plants, that helps the plant developer to manage the risks during the plant's development cycle, was developed.

The most significant results expected are the following:

- First feasibility tests have been carried out on a non-invasive sensor technology (SYKE).

- A common concept concerning the content and the way of realising the subprojects has been created (TRUST).

- Preliminary method for identification of safety critical requirements has been developed (TRUST).

- New hazard identification and risk assessment method for GMOs has been published.

1.4 International viewpoint

The theme brings together VTT's research groups and specialists in the field of safety and reliability. The critical mass that comprises this focused network consists of high-level experts in the fields of safety engineering, risk assessment, industrial mathematics, modelling, simulation, material science, mechanical engineering, software engineering, psychology and biotechnology. This group has a very wide international contact network, which supports the research carried out in the theme projects, and provides a good basis for increasing and cross-linking the international networking.

International networking is promoted and supported by procedures accepted and applied in the theme. Theme leader and researchers have visited several research institutes in Europe, USA and Japan. Results of these travels, contacts, discussions, ideas, proposals, etc. are reported and distributed within the theme. Public results of research projects have been presented at several conferences and seminars.

As a result of international activities, for example, the following activities can be listed:

- Several European research initiatives have been proposed, and research has been started in several projects.

- Several reserchers and senior research scientist of VTT will join to other institutes for some period of time.

- Visiting students from other Research Institutes will join the projects of VTT.

- Preparations and project proposals have been made to start the collaboration and researcher exchange (theme leader) with japanese universities in the area of systems safety.

1.5 Management of the theme

1.5.1 Preparation and starting of the theme

When planning the theme, the following activities were carried out:

- The theme had an internal supporting group of three researchers at VTT.

- A summary was made about the costs caused by disturbances in different kinds of areas and safety problems in different fields.

- Four working groups were collected from industry for defining the customer's needs and requirements for the theme. They represented the following industrial fields: working machines, pulp and paper industry, chemical industry, and transport and logistics. These working groups had several meetings for defining the future needs and visions of each area.

- In the planning phase, five focus areas of research were selected for development.

- In March 2001, a workshop of about 30 researchers from VTT was organised for selecting the focus areas and developing the research ideas.

- In June 2001 another working seminar of about 30 researchers from VTT was organised for developing research proposals further. The aim was to define and clarify the focus areas.

- In August 2001 the third working seminar was organised for developing roadmaps and defining the required projects.

- The theme leader collected the proposals and made the first proposal for the theme projects.

In 2001 the executives of VTT decided about the theme projects for the year 2002. In this connection three focus areas were accepted.

In 2002 and 2003 the evaluation of the proposals was made in Scientific Advisory Board of the theme. Based on this evaluation the theme leader has made a proposal and prioritisation of the projects for the next year. This way the decision making process has been more clear.

1.5.2 Management of the theme

VTT Industrial Systems is responsible for the management of the theme. Since its inception, the **theme leader** has been research professor Veikko Rouhiainen. He has the overall responsibility for co-ordinating the theme, and reporting about its progress to VTT.

The theme has three focus areas, each of which has a **focus-co-ordinator**. The research itself is carried out in projects, each of which has its own **project leader**. The focus areas "life-cycle management" and "HTI and safety" both have their own **steering committee (SC),** which also is the steering committee of the projects related to those focus areas. These SCs are nominated by the research areas carrying out the work in the focus area. The aim of these SCs is to make links and assure contacts to the line organisation of the research institutes of VTT.

Focus-co-ordinators and project leaders have regular **project-leader meetings**, in which common goals, operating principles, etc. are developed and accepted. The aim of the meetings is also to increase the collaboration with different research groups, harmonise operating principles, benchmark procedures, etc.

The theme leader is supported by the **scientific advisory board (SAB**), which has a meeting once a year at the beginning of June. The SAB's role is mainly to give scientific and technological support in decision-making related to the ranking of project proposals, as well as in commenting the project proposal. In this theme, the work of the SAB has been very worthwhile and profitable. The SAB has also helped in international networking. The members of the SAB are from a reserch institute in Netherlands, from a University in Japan and from VTT.

The **steering committee** of the theme is nominated by VTT. It has from three to four meetings a year, as required. Its role is to support the theme leader in fulfilling the technology themes' goals set by VTT. The SC has an important role also in deciding about new initiatives, and starting the preparation of new project proposals. The members of the steering committee are from VTT.

1.5.3 Decision-making process in the theme

The project proposals are made by the researchers, but also commitment from the research institutes is required. This has ensured that there have not been any major problems with the resources when carrying out the research. The original requirement was of commitment from at least three research institutes for each project; however, this was not always possible.

When starting the themes in 2001, the process, as well as the theme concept itself, was not yet very clear. Also different kinds of opinions and views were observed. Since then, and especially when the new operating model, and strategy, as well as the technology strategy of VTT has been presented, the operation of the theme has become easier.

1.5.4 Cross-organisational activities of the theme

Proposals are awaited from all research institutes of VTT; however, they are mainly developed within VTT Industrial Systems. VTT Industrial Systems, as well as VTT Biotechnology and VTT Building and Transport, have the main roles in this theme. These institutes are involved in a remarkable amount of research related to safety and reliability.

On a very positive note, it can be noted that all the research institutes of VTT are participating in this theme. However, some institutes could more actively participate. The low participation rate can be attributed to the fact that safety and reliability are not strategic focus areas of all the institutes, and they obviously will focus their strategic research on their own focus areas.

Specifically to increase the knowledge of the theme within VTT, a scientific seminar was organised in April 2003, and about 35 researchers participated.

In general, the commonly accepted attitude among researchers is that the themes have had a positive contribution to the increase of collaboration within VTT, and the importance and benefits of this collaboration is understood.

1.5.5 Visibility of the theme outside VTT

The theme has prepared its own communication plan. Public information about the theme and research projects is presented on a website, which is to be updated as required. The theme has, however, not yet organised its own information seminar or meeting. This is mainly due to the fact that safety and reliability alone are not usually of

enough interest to the media. However, the theme is active in participating in different kinds of information dissemination activities. In this connection, for example, the following can be mentioned:

- The theme and research projects have been presented at several seminars, articles, etc.

- In August 2003, in connection with the 'Portals go rock' concert, an information seminar was organised for customers together with three of the VTT's knowledge portals.

- In February 2004, the intermediate results of the VTS project were presented, in conjunction with the Finnish Maritime Administration, for an international press group of eight journalists from five countries.

- Several activities are also under preparation, including a seminar for safe technology in Tampere in June 2004, and a Technology 2004 exhibition in Jyväskylä in October 2004.

2. Methods for life-cycle management

2.1 Executive summary

Aino Helle

The focus area 'Methods for life-cycle management' under the Safety and Reliability technology theme comprises of three projects:

- T4LIIKKUDIA – Monitoring and Diagnostics – Lifetime Management of Mobile Machinery

- SYSTELI – Analysis in Management of Plant Lifetime and Production Safety

- FI-TOOL – Management of safety and reliability knowledge during the life cycle of machines.

The research in the three projects is directed to different aspects of life cycle management, with different approaches. While T4LIIKKUDIA focuses on monitoring and diagnostics of mobile machinery and develops methods and means for a machine to diagnose faults and its condition, estimate the remaining life time and to communicate with a remote supervision centre, SYSTELI has a system analytical approach for the management of lifetime and production safety of industrial plants, including microbiological production safety. The third project, FI-TOOL focuses in developing an information management concept covering the whole life cycle of a machine. The projects are both complementary and interrelated, providing data, requirement definitions and tools also for the use of each other. Together they will provide a variety of novel tools and methods for optimisation of the safety and reliability of products, machinery and industrial production plants throughout their life cycle, with simultaneous considerations of cost efficiency.

2.1.1 Background

The increasing complexity of machinery and production systems together with the growing demands on controlling costs, environmental risks and safety increases the importance of focusing research on safety and reliability of products, machines and production systems throughout their life cycle. Monitoring and diagnostic methods are needed for faults in machinery to be detected and predicted early enough to avoid serious damage and to allow for properly timed and focused maintenance actions with the shortest possible production interruptions. Advanced and generic diagnostic

solutions are still lacking, the existing methods being in general relatively restricted and case specific. By systematic analytical approaches and multi-criteria decision making tools, planning of maintenance activities could be enhanced, the safety and reliability be improved and the economic lifetime of products and systems optimised. Information is produced at different points in time in different organisations during the life cycle of a machine. For life cycle management the continuous availability of information is essential, despite the diversity of the organisations producing and utilising the information. Besides good technical knowledge of equipment, production processes and failure modes and mechanisms, life cycle management requires a systematic approach and overall view.

2.1.2 Objectives

The objective of T4LIIKKUDIA is to provide mobile machinery the ability to self-diagnosis and prognosis, as well as to learning and communication. The challenge is to develop a generic self-learning diagnostic and prognostic system. A local online diagnostics system will be capable to specify needs for servicing and spare parts as well as to provide notifications to a remote supervision location.

The objective of SYSTELI is to develop a system analytical framework for the lifetime management of industrial systems, and tools and methods for component lifetime prediction and production safety. These include multi-criteria decision making tools, expert judgement in ageing management and microbiological production safety, as well as probabilistic models for residual lifetime prediction accounting for uncertain multi-source information.

The objective of FI-TOOL is to produce a concept for a comprehensive safety and reliability information management system at the level of individual machine providing information for all persons in need over the entire life cycle of the machine from design to dismantling, utilising unique identification of machines for linking all machine specific information.

2.1.3 Resources

The research in this focus area is widely multidisciplinary and combines resources from four research institutes of VTT. The research institutes involved being VTT Industrial Systems, VTT Information Systems, VTT Biotechnology, VTT Processes.

2.1.4 Main results and impacts

The main results of the projects are presented in the project reports. The focus area and the theme combine the expertise of different disciplines and bring researchers from various research areas and units in contact with each other, both in actual research work and at the meetings and seminars. This has an impact on lowering the threshold of cooperation between the research units. The results from the projects are expected to lead to the start up of several new research projects utilising the cumulated knowledge and networks. The results are particularly applicable to process industry and users of mobile machinery as well as to the machine manufacturers and maintenance service providers though not restricted to only those sectors. Some of the results of the projects showing clear impacts or industrial relevance and interest are shown below.

LIIKKUDIA

- The lubrication and hydraulic systems form a major focus for the development of the diagnostics in mobile machinery. The results achieved this far include a stochastic model for lubricating film thickness, fault simulation and fault analyser, having immediate impact by serving as starting points also in two spin off projects currently in preparation, one being a national project related to mobile machinery and the other one an international project focusing on the effects and properties of dirty lubricants.

- Diagnostic Center has been created at VTT and offers a platform for development of remote diagnostics and prognostics within an international network. A basic idea for developing a first stage learning diagnostic system is based on utilisation of the Diagnostic Center to create cumulative knowledge on faults in machinery.

SYSTELI

- System analytical models and approaches developed are often needed to assess uncertainties or when analyses are partly based on uncertain information. The models improve the understanding of the importance of various factors in life cycle management.

- The research on microbiological production safety has produced results with clear industrial interest and immediate impact. Paper and packaging industry has shown interest in the tool that was developed for risk assessment and Hazard Analysis and Critical Control Points (HACCP) analyses, showing the results in clear charts and including a data bank on risk analysis and problematic micro-

organisms in the pulp and paper industry. Bacteria identification methods have been developed for rapid screening of the presence of bacteria, resulting in that the time needed for obtaining the results has shortened from several days to one day. This is particularly important in case of food packaging materials and bacteria causing food poisoning. Rapid detection of the bacteria reduces loss of production and risks concerning product safety. The new methods are in use in projects and contracts with industry.

- A tool for integration of structural analyses and simulated process parameters is being developed. It will allow e.g. analysis of the effects of different plant operation scenarios on structural reliability of components.

FI-TOOL

- The knowledge management system at conceptual level is under testing phase. The main parts of the concept include TAG – a system for locating and storing product specific information, EXP – a mobile system for utilisation and updating of data in daily operations, TOP inside an organisation and SHED for global connections – as a background information system with data analysis, synthesis and management capabilities.

- TAG and EXP prototype devices have been developed and demonstrated. The TAG acts as an embedded information system of the machine and may allow the retrieval of information on a machine status and behaviour. A prototype user interface on the EXP device allows reading and writing data to the TAG and storing messages from the user. An assembly of TAG and EXP has been constructed to test the communication functions between the two subsystems. Testing is based on scenarios of various operational states and conditions.

- Other application areas for the TAG device are e.g. in active, communicating packaging systems which form the focus of (Älypakkaus)-project.

- One employment invention concerning video monitoring of a production line using wireless technology has been made and accepted.

2.1.5 International and national networking

International networking is at a very good level in the focus area. It is most prominent in SYSTELI, with connections to the European Safety, Reliability and Data Association (ESReDA). An ESReDA seminar was organised by VTT in Finland in May 2004, the

topic being lifetime management of industrial systems. International research exchange will also be realised in SYSTELI as a visiting student will join the project for 6 months and a senior research scientist of VTT will join a research institute in energy field. International networking is active in LIIKKUDIA through the INID network involving 5 European universities and research organisations and the Diagnostic Centre, as well as through an international project currently under preparation involving partners from Japan, USA and Europe. All projects have participated in international conferences and seminars.

Co-operation and networking with Finnish industry and several national research projects is also active in all the projects as well as between the projects.

2.1.6 List of media references

The establishment of the Diagnostic Centre has been referred to in various media.

2.2 Monitoring and diagnostics – Lifetime management of mobile machinery (LIIKKUDIA)

Jyrki Tervo

2.2.1 Introduction

Friction and wear increase the cost of operation of a mobile machine by decreasing the lifetime of components and machinery. Savings can be achieved by increasing the maintenance and design efficiency by correctly diagnosing machinery faults. Reduction of downtime as well as maintenance and replacement costs constitutes the major part of savings. Savings can be achieved by better understanding and diagnosing the phenomena taking place in machinery and by correctly predicting the occurrence the final failure.

Methodologies to diagnose and forecast faulting in mobile machinery are generic in such sense, that similar phenomena are taking place in industrial machinery as well. According to a recent survey among Finnish industry, estimated potential savings are biggest in the sectors of pulp and paper, metal and steel production, metal products production as well as energy production. These sectors comprise 70% of the expenses of mechanical maintenance within the Finnish industry. By applying advanced diagnostic methods the cost can be decreased significantly.

2.2.2 Background of the project

At present, the most available diagnostic methods in general are relatively restricted case specific tools that apply strict rules for reasoning. In some cases the rules have been fuzzified. Some examples have been published that utilise neural network techniques. Stochastic methods and physical models have also been applied in failure modelling. Only some rule based reasoning have been implemented in mobile machinery self-diagnosis.

Since advanced and generic diagnostic solutions do not yet exist, a fundamental research project is needed, i.e. T4Liikkudia. The key issue in machinery self-diagnostics is the intelligent agent capable for learning. In order to be applicable to multi-technical environment of a mobile machine, the solution needs also to be generic.

2.2.3 Objectives

The ultimate goal of the project is to provide a machinery the ability to self-diagnosis and prognosis, as well as to learning and communication.

The new achievement is the necessary means and methods to produce a generic, self-learning diagnostic and prognostic system. This kind of system does not yet exist. In order to fulfil the goal the system needs to be hybrid (uses multiple methods for problem solving), modular (to make it flexible in adding new features and measurements), distributed (to make it flexible in operation), integrated (capable to use data from control system as well) and able to communicate with different user levels. Developed methods and tools will enable a machine itself to diagnose its condition, estimate remaining lifetime and, if needed, to transmit the necessary data and information to a remote supervision centre. The remote supervision centre also acts as a tutor for the system.

Implementation of developed solutions will lead to a self-communicating machine able to specify its own servicing needs. A local online diagnostics system will be capable to specify servicing and spare parts needs, as well as to provide notifications to a remote supervision location. A remote supervision centre provides higher intelligence to the local system. System makes it possible to avoid imminent serious damage by allowing properly timed maintenance measures to be carried out. The way of operation results in the shortest possible production interruptions.

For the year 2004 the aims and goals of the project are as follows:

- Development of advanced signal processing methods by laboratory experimenting and simulation.

- Development of alternative scenarios for learning diagnostic system.

- Initiation of spin-off projects for further development of research results.

2.2.4 Main results

Stochastic model for lubricating film thickness in rolling contact

Film thickness measurements were conducted in laboratory by means of optical interferometer. The multiple linear regression model includes parameters such as rolling speed, sliding ratio, loading, temperature and water content of oil. The model may be used for estimation of film thickness in rolling bearing. Application of the model to practice requires further research. The result will serve as one of the technological start points in the research project for dirty lubricants behaviour (Dirtlub) – see below.

Simulation model for faults in hydraulic machinery

With the model electric faults, control valve jamming and system leaks can be simulated. Faults are examined in position, pressure and flow during different work phase of a cylinder. The simulated target is an existing industrial machine. Results of the simulations are to be used in diagnostics development. The result will serve as one of the technological start point in the diagnostics development project in the Technology program for the Finnish Defence Forces – see below.

Fault analysis demonstrator based on rapid main memory based database system (RapidBase)

Fast fault analyser with possibility for intelligent triggering measuring. Algorithms developed with MatLab are used in the RapidBase as DLL library functions. Fault data is produced by simulation model of the hydraulic machinery. The work is proceeding and testing in laboratory scale is being investigated. The result will serve as one of the technological start point in the diagnostics development project in the Technology program for the Finnish Defence Forces – see below.

Evaluation of signal analysis methods to reduce disturbances in measurement data

Signal analysis tools development for fast discrete phenomena. Methods and means are also studied to disclose measurements disturbing signals – sensors matrix and mathematical tools. The work is proceeding by testing in laboratory scale. The result will serve as one of the technological start point in the diagnostics development project in the Technology program for the Finnish Defence Forces – see below.

Basic investments and ideas on Diagnostic Centre for further utilisation and development

Diagnostic Centre is available for use in remote monitoring and diagnostics applications. A project was initiated to find possibilities to create business with remote diagnostics services. Utilisation of international relationships (INID) is being investigated as well. The result will also serve as one of the technological start point in the diagnostics development project in the Technology program for the Finnish Defence Forces – see below.

Model for utilising Diagnostic Centre for development of 1st stage learning diagnostic system

Basic idea for 1st stage learning diagnostic system is based on Diagnostic Centre, which is used to create cumulative knowledge (i.e. database) on faults in machinery. The result has been published as a poster. The result will serve as one of the technological start point in the diagnostics development project in the Technology program for the Finnish Defence Forces – see below. The fundamental challenge in creating learning diagnostic system is obviously huge. Machine learning (emulation of intelligent behaviour) requires that certain fundamental conditions will be fulfilled. These include teaching and rules generated from experience, model to handle conflicting information, estimation of performance and feedback, analysis of causal errors in diagnosis, ability to find complementary ways for information analysis as well as constant training. Diagnostic Centre can be seen to serve some of these challenges.

2.2.5 Impacts

As an immediate impact of the research new ideas for industry related research projects have been created. Diagnostic Centre offers an international platform for diagnostics and prognostics development. Anticipated further impact will be measured as an increase in industry-related research (international and domestic) and development projects. Since the results are not directly applicable for industrial use, further

development in joint projects with industry is required. The industrial interest (domestic and international) is relatively high, as can be concluded from the interest on spin-off projects. Unfortunately direct participation of industry in Liikkudia project has been lame, which is most likely due to fundamental nature of the research. No patents have been claimed this far.

2.2.6 List of publications

Conferences and Journals

Parikka, R. & Tervo, J. (2003) Condition monitoring of oil in mobile machinery (Condition monitoring 2003).

Tervo, J. (2003) Kunnossapidon kehittyvät mittaukset (Kunnossapito 2003).

Tervo, J. (2003) Presentation at Kunnossapitopäivät 2003 (Maintenance exhibition 2003).

Tervo, J., Vidqvist, V., Parikka, R., Tervo, J., Komonen, K. & Rouhiainen, V. (2003) Enhancing reliability for mobile machinery. KonBin'03, 3rd Internationals Safety and Reliability Conference, May 26–30, 2003, Gdynia, Poland.

Vidqvist, V. (2004) Liikkuvien työkoneiden diagnostiikka. Turvallisen tekniikan seminaari, Tampere 10.6.2004 (CD-ROM). Teknologiateollisuus ry, VTT Tuotteet ja tuotanto, Uudenmaan työsuojelupiiri. Tampere.

Vidqvist, V., Komonen, K. & Tervo, J. (2003) Liikkuvien koneiden käyttöomaisuuden hallinta, diagnostiikka ja prognostiikka (Kunnossapito 2003).

VTT reports

Holmberg, K., Komonen, K., Oedewald, P., Peltonen, M., Reiman, T., Rouhiainen, V., Tervo, J. & Heino, P. (2004) Safety and Reliability – Technology Review. VTT report, BTUO43-031209. 80 p. + appendices.

Vidqvist, J., Alanen, J. & Tervo, J. (2002) Diagnostics of Mobile Machinery: Future Trends. VTT report, Btuo43-021058. 50 p.

Vidqvist, V. & Tervo, J. (2004) Fault Simulation of Hydraulic Cylinder Drive. VTT report BTUO43-041229. 16 p. + app. 11 p.

Working reports

Mäkeläinen, K. (2004). Evaluation of signal analysis methods to reduce disturbances in measurement data. Project report 2004 – not to be published.

Vidqvist, V. Bayesian Methods in Fault Diagnostics and Maintenance of Production Systems. To be published in 2005.

2.3 Systems analysis in management of plant lifetime and production safety (SYSTELI)

Kaisa Simola

2.3.1 Introduction

SYSTELI project aims at developing and promoting system analytical approaches for the management of lifetime and production safety of industrial plants. With the aid of system analytic approaches, maintenance and surveillance activities can be better focused, the safety and reliability can be improved, and economic lifetime can be optimised. With the adoption of probabilistic life assessment methods, the over-conservatism can be reduced and thus further cost savings are possible. Optimally, the costs can be reduced and safety improved simultaneously. The results of the project will partly be applicable in short-term, while the life management framework will be the long-term goal of the project.

2.3.2 Background of the project

There is a need to focus lifetime management activities, and at the same time account for various criteria (e.g. safety & costs) and constraints. It is recognised that more systematic approaches are needed in prioritising systems, structures and components for lifetime management, and for safety-related decision making. An increasing amount of information is available for the decision making, but this information is seldom used efficiently. Methods and tools are needed to select and combine the ageing- and safety-related information so that decisions can be made in a cost-effective way.

The project aims at finding synergistic added value at VTT by combining different expertise, such as systems analysis, microbiology, structural engineering, material sciences & process simulation. Such a wide cross-disciplinary consortium provides a unique forum for research and development in the area of life management and production safety.

2.3.3 Objectives

The objective of the project is to develop system analytical methods for the life management of industrial systems and for production safety. The project consists of both generic methodological development and case studies. These case studies are run to identify the more specific needs that rise from various characteristics of different application areas.

In the project, models and approaches are be developed for:

- multi-criteria decision making in focusing ageing analyses and in the definition of maintenance tasks
- expert judgement in ageing management and microbiological production safety
- probabilistic models for the prediction of the residual lifetime of components and accounting uncertain information from several sources
- measuring and analysis methods for managing product safety.

The outcome will be a system analytical framework for the lifetime management of industrial systems, and tools and methods for component lifetime prediction and production safety.

2.3.4 Main results

The project can be divided in following tasks:

- system analytical models and approaches
- microbiological production safety
- structural ageing management in power generation.

The main results so-far in each of these area are summarised below.

2.3.5 System analytical models and approaches

Good practises and support for multi-criteria decision making have been developed and tested in a case study related to maintenance decisions. The long-term goal is to bring

decision theoretical approaches to practical use, so that they are tailored according to customer needs.

Expert judgement approaches have been developed for management of ageing and microbiological production safety, and for utilisation and combination of maintenance information from several sources for the needs of process industry. Expert judgement is often needed to assess uncertainties, and formal approaches are needed to obtain reliable results.

Principles of stochastic modelling of residual lifetime of components, accounting for uncertain information in the degradation development and inspection results, have been developed. Such models improve the understanding of the importance of various factors in the lifetime assessment, and enable the optimisation of e.g. inspections or replacement.

2.3.6 Microbiological production safety

A risk assessment model for performing and maintaining Hazard Analysis and Critical Control Points (HACCP) -analyses and own-checking systems in the pulp and paper industry has been developed. The tool is based on the principles of risk assessment and HACCP and on the experiences obtained from the pulp and paper industry. The results of the risk analyses are shown in clear charts, enabling the selection of critical control points. Furthermore, a data bank on risk analysis and problematic micro-organisms in the pulp and paper industry is included in the tool.

Methods for detection, identification and population study of micro-organisms have been developed. E.g. a method to detect Bacillus cereus group bacteria from cardboard and paper with real-time PCR has been developed. These bacteria may cause food poisonings and are particularly unwanted in food packaging materials. The developed method can be reliably used for rapid screening of the presence of the bacteria, and the results can be obtained in one day instead of several days demanded e.g. by culturing. Method development for fast detection of other bacterial groups is also under way.

Critical locations for controlling the process air at 15 places in a paper-mill process have been identified. The different sampling methods were studies and the seasonal effect of air quality was identified. Results showed the differences in reliability of various sampling techniques.

Emergence and management of resistant strains is also studied.

2.3.7 Structural ageing management in power generation

Within structural ageing management, software development for combination of process simulation and structural mechanics analysis has been started. The combining of these analysis methods is a challenging task, but there are clear benefits to be expected. The integration of structural analyses and simulated process parameters allows e.g. analysing the impact of different plant operation scenarios on structural reliability of components.

A case study on the integrity of a degraded steam drum has been performed. The goal was to assess and optimise operational procedures and the material behaviour. The case study combines structural analyses and maintenance decision making. This study gives experience what kinds of uncertainties are related to the structural reliability, how they affect the decision making for finding an optimal maintenance policy.

The development of an integral software package for evaluating structural risks in various applications has been initiated. Also a database for input information needed in structural reliability analyses and life management studies is under development.

2.3.8 Impacts (also expected impacts)

The activities and results of the project have so far been presented mainly in international conferences, where very positive feedback has been obtained from the research community. Most of the direct industry contacts have been in the area of microbiological production safety, and the research is followed with great interest. For instance paper and packaging industry has shown clear interest to get the HACCP risk assessment tool in use. Also the bacterial identification methods developed will be used in projects and contracts with industry.

It is expected that the results of the project are of interest widely in the industry. However, e.g. the systems analytical approaches, e.g. practical use of decision making support have to be tested in the case studies to identify specific requirements of different applications. The development of probabilistic modelling principles will certainly still need demonstration in practical applications.

Many of the results are beneficial for VTT by creating better bases for our services, e.g. by developing tools and databases that can be used in future research assignments. The cross-disciplinary work across different research units and fields creates unique synergistic advantage.

2.3.9 List of publications

Journal articles

Maukonen, J., Mättö, J., Wirtanen, G., Raaska, L., Mattila-Sandholm, T. & Saarela, M. (2003) Methodologies for the characterization of microbes in industrial environments: a review. Journal of Industrial Microbiology & Biotechnology 30, pp. 327–356.

Myötyri, E., Pulkkinen, U. & Simola, K. (2003) Application of stochastic filtering for lifetime prediction. Submitted to Reliability Engineering and System Safety 11/2003.

Priha O., Hallamaa K., Saarela M. & Raaska L. Detection of Bacillus cereus group bacteria from cardboard and paper with real-time PCR. Journal of Industrial Microbiology & Biotechnology. (In press.)

VTT publications

Wirtanen, G., Miettinen, H., Pahkala, S., Enbom, S. & Vanne, L. (2002) Clean air solutions in food processing. Espoo: VTT Publications 482. 95 p. ISBN 951-38-6015-9; 951-38-6016-7. http://www.vtt.fi/inf/pdf/publications/2002/P482.pdf

Conference papers

Aho-Mantila, I., Saarinen, K. & Kauppinen, P. (2002) Risk based decision procedures for pressure equipment safety in hydrocarbon applications. ESReDA seminar on Decision Analysis: Methodology and Applications for Safety of Transportation and Process Industries, Delft University, Netherlands, November 18–19, 2002. 11 p.

Cronvall, O., Saarenheimo, A., Simola, K. & Talja, H. (2003) Approaches to Estimate Pipe Failure Rates for Risk-Informed In-Service Applications at Nuclear Power Plants. ESReDA 25th seminar on lifetime management of structures, Paris 17.–18.11.2003.

Kunttu, S. & Kortelainen, H. (2004) Supporting Maintenance Decisions with Expert and Event Data. RAMS Conference, January 2004.

Miettinen, H., Salo, S., Raaska, L. & Wirtanen, G. (2003) Comparison of three air sampling methods in food packaging materials production. In: Wirtanen, G. & Salo, S. (eds.). 34th R3-Nordic contamination control symposium. Espoo: VTT Symposium 229. Pp. 77–82. ISBN 951-38-6284-4; 951-38-6285-2. http://www.vtt.fi/inf/pdf/symposiums/2003/S229.pdf

Raaska L. (2003) Hygienic aspects & HACCP related to the production of packaging materials. Presentation in Food safety in relation to novel packaging technologies. The SAFE consortium workshop 20–21 November, 2003, Brussels.

Raaska, L. (2003) Safety and hygiene management in manufacturing packaging materials. In: Wirtanen, G. & Salo, S. (eds.), 34th R3-Nordic contamination control symposium. Espoo: VTT Symposium 229. Pp. 69–76. ISBN 951-38-6284-4; 951-38-6285-2. http://www.vtt.fi/inf/pdf/symposiums/2003/S229.pdf

Raaska, L., Partanen, L., Suihko, M.-L. & Mattila-Sandholm, T. (2002) Safety and hygiene management in manufacture of packaging materials. Noordwijk Food Safety HACCP Forum 9–10.12.02.

Raaska, L., Wirtanen, G., Pulkkinen, U. & Simola, K. (2002) Systems analysis in life management and production safety – application to microbiological production safety in paper industry. ESReDA seminar on Decision Analysis: Methodology and Applications for Safety of Transportation and Process Industries, Delft University, Netherlands, November 18–19, 2002. 11 p.

Simola, K., Talja, H. & Smeekes, P. (2002) Use of plant specific information in life management. IAEA International Symposium on Nuclear Power Plant Life Management 4.–8.11.2002. 15 p.

In addition there are several work reports written in the project.

2.4 Management of safety and reliability knowledge during the life cycle of machines (FI-TOOL)

Arto Säämänen

2.4.1 Introduction

The important role of safety and dependability in modern industry is obvious. The current trends in industry, such as desire for agility, increasingly networked companies, new patterns of working and co-operation in networking enterprises and need for feedback information to designers have created a need for continuous availability of safety and reliability information during the whole life cycle of machines.

The main objective is to provide tools, methodologies and technologies, supporting safety and dependability management during the entire life cycle of machines. The developed concept will provide completely new means for the manufacturers to manage

and for operators to utilise safety and dependability information. It will also improve quality of maintenance and quality of production as well as agility of factories.

The *Fi-Tool* concept will include a system for locating/storing of product specific information, a mobile system for the utilisation and updating of safety and dependability knowledge in daily operations, and a background information system with data analysis, synthesis and management capabilities.

2.4.2 Background of the project

Management of safety and reliability of machines requires continuous availability of safety and reliability information during the whole life cycle of machines. At the moment this information is not easily accessible because it is produced at different points in time in different organisations during the life cycle of machine (design-production-operation-maintenance-dismantling etc.). Besides, due to the diversity of information producing organisations, the essential safety and reliability data can be spread out in different information systems within the company. The current general tendency, however, is to increase the level of integration of company information systems, e.g. product data management systems and resource management systems, even into a one comprehensive system. Moreover, wireless communication and the use of transponders (RF tags) for various applications are increasing. Therefore, a common technological basis for improving the management of safety and reliability exists.

The challenge is to utilise these techniques in a novel way for knowledge management of safety and reliability information. The challenge of this project is to enable the continuous and timely availability of this data in every day machine operations. As solution, a concept is seen, which includes unique identification of machines and through it an individual machine's life cycle safety and reliability knowledge management.

2.4.3 Objectives

The project aims for better availability and utilisation of safety and reliability information and thereby to enhance the safety and reliability management. Thus, it supports the decision making in daily operations in companies. This kind of comprehensive safety and reliability information management system at the level of individual machine has not been put into practice before.

The project will produce technologies and procedures for providing safety and reliability information for all persons in need over the entire life-cycle of a piece of machinery (from design to dismantling). The development of the technologies and

procedures is done first in a conceptual level and completed by selecting the most relevant issues for further detailing. The ambition of this project is a concept level proposal, which will work as a more comprehensive solution. This ***FI-TOOL concept***, the concept of technologies and procedures, will contain the following main components, which are recognised to be the most credible solution candidates:

- **TAG** –Technology for specifying the machine identity combined with archiving, storing and updating functions for risk and dependability data/knowledge. This ensures data transfer with the machine.

- **TOP** –Technologies, methods and procedures for managing, archiving, storing and updating safety and dependability information as a cumulative knowledge along the life-cycle of machine.

- **EXP** –Technologies, methods and procedures for utilisation and updating of safety and dependability knowledge in daily operations. This can be e.g. a mobile phone, PDA, tablet-PC or laptop.

- **SHED** – global connection and data warehouse for sharing of knowledge between partners.

As there are simultaneous R&D widely going on, the timing of the introduction of the concept and the implementation of project findings is crucial.

The detailing of technologies and procedures forming the concept will be worked-out, tested and customised in case studies to fulfil all partners' needs.

2.4.4 Main results

A concept of safety and dependability information system was developed using conceptual modelling. The initial part of the conceptualisation process involved interviews with four major machine manufacturers in Finland and also discussions with other industrial partners. The concept is now under test and will be further developed based on the results of the subsystem tests.

The concept includes: 1) a system for locating/storing of product specific information (***TAG***), 2) a mobile system for the utilisation and updating of safety and dependability knowledge in daily operations (***EXP***), and 3) a background information system with data analysis, synthesis and management capabilities (***TOP*** inside an organisation, and ***SHED*** for more extensive global connections).

A demo of safety and dependability information system, especially concerning the ***TAG*** and ***EXP*** subsystems, was planned for testing stage purposes. The procedural steps in the construction of the system for locating/storing of product specific information was: 1) the architectural design of the ***TAG*** subsystem, 2) the construction of the selected physical subsystem elements, 3) the coding of programs needed to fulfil the defined subsystem functions. After the construction phase, the subsystem functions are first tested separately, and after that the whole subsystem, connected to a machine, is tested.

A construction of ***TAG*** subsystem as a prototype device was developed for the demonstration purposes. The main function of the TAG is to act as an embedded information system of the machine. Additionally, the TAG may allow the retrieval of information on the machine status and behaviour. Different levels of the TAG subsystem are identified in the conceptualisation process. In its most simple form (Level 1A), the TAG only has to identify the machine, and all the information is stored remotely in the background system. In this case, either barcode or RFID can be used to identify the machine. RFID allows also to store static data (e.g. design data) to the TAG, and sensors can be integrated in the TAG (levels 1B and 1C). By adding a serial link to the machine, e.g. by using CAN-bus, information on the actual status of the machine and its sensors can be retrieved. The level 2 TAG is a separate device, which communicates wirelessly with the EXP device, e.g. using Bluetooth or WLAN. If the machine has its own on-board computing facilities, the TAG device can be integrated in the machine (Level 3) and provide a wireless communication link to the EXP device.

In order to test the technical feasibility of the concept, a prototype with a wireless Bluetooth and with CAN connection, corresponding to the advanced level 2 type has been developed. The TAG prototype contains the following components: an ARM-processor with 136 KB RAM, 1 MB FLASH memory; Bluetooth radio, RS-232 serial connection. CAN-messages are read and written by use of a RS-232 to CAN-bus converter. For control of the Bluetooth radio, an embedded Bluetooth stack has been implemented on the ARM-processor.

An example of an ***EXP*** subsystem as a prototype device was developed to test the functionalities of the TAG subsystem. The Nokia 7650 mobile phone, featuring a Symbian operating system and a Bluetooth connection, was used for that purpose. A simple protocol and data structure has been developed for exchanging information between the TAG and the EXP subsystems. On the TAG device, functions for storing data and for data exchange with the EXP device and with the CAN-bus have been implemented. On the EXP device, a prototype user interface has been developed, which allows reading and writing data to the TAG and storing messages from the user.

Preliminary tests were performed to investigate the technical feasibility of the TAG. More specifically, the identification of a product with the TAG, the access process to the product's specific information, and the availability of the information by using the TAG subsystem were investigated. An expert group of scientists observed and analysed test scenario cases during a test session to find the nature of the information, e.g. context dependencies and changes of content along the life cycle because of machine modifications. The experiment scenario was planned to consist of examples of typical operation and maintenance work tasks.

An assembly of the ***TAG*** and ***EXP*** subsystems was constructed for the test stage purposes. The test was arranged in a laboratory environment. A machine, similar to, e.g. a loader or a harvester having its own control system, was selected as target, of which the product specific information was to be read. The target's control function, which communicates with other equipment on-board over a CAN-bus, was modelled in this test by using the CANALYZER software from Vector Informatik GmbH. The model produced the similar data and information packets transferred over a local CAN-bus. The machine operation was not modelled or present in the test, and only the communication functions were observed.

A scenario based testing and an example of a scenario for operational states and conditions in a fictitious working system was designed. During the scenario, the different functionalities of the TAG were tested through the prototype user interface at the EXP device. The scenario consisted of the following phases: checklist for starting up the machine, reading data from the TAG, and getting information on how to handle an error reported by the machine's CAN-bus.

The limitations and focal points of the study have been set in order to concentrate on the most relevant issues of the concept. The concept includes an information system with data analysis and management capabilities, and a data input and information display system to serve as a user interface (TOP). At the moment special interest is placed on knowledge transfer and knowledge creation aspects between product development and maintenance activities. Although the concept also supports decision making in the daily operations of companies, this topic will be covered later in this project.

Examples of recognised management systems are PDM systems, CMM (Computerised Maintenance Management) systems and safety information management systems. Typically, PDM systems include huge amounts of product related information. In addition to the basic/standard product descriptions and documents included are e.g. information relevant to configuration and maintenance management. Further items, that may be included, are supply chain management information and resource management information. In addition to information on maintenance events, CMM systems may

contain functionalities that allow planning of maintenance tasks and keeping record on spare parts inventory. Safety management systems typically contain information on accidents, injuries, incidents, hazardous chemicals and other documents concerning occupational safety issues. At the moment we explore how existing information management systems and information items found in these systems could be used to create knowledge items relevant to the previously described FI-TOOL safety and dependability concept.

2.4.5 Expected impacts

The project aims to improve the safety and reliability management of machines. It will produce benefits both to the companies manufacturing the machines as well as to the end user of the machines. Machine manufacturers will benefit from the feedback information of the safety and reliability of their machines on the field. The end user will benefit from the easy availability of the specific safety and reliability information of the machine. The ultimate goal of this project, together with other projects in lifetime management focus area, is to help machine users in their actions in optimising the gross profit.

Other application areas for TAG equipment have also been found. The same concept is used at the moment in a active, communicative packaging systems (Älypakkaus)-project. Also application in the area of building services are considered.

At the moment the FI-TOOL knowledge management system exists at the conceptual level. In future the FI-TOOL concept can be tailored to fulfil customers' needs. The project may also promote new service business in the information storage/exchange area. The time period of utilisation of the results will be about 5 years.

Several industrial partners has shown interest on this concept (e.g. Fortum Oil & Gas Oy, Outokumpu Technology, INMET Mining Pyhäsalmi Mine Oy). The negotiations with them are ongoing.

At the moment one employment invention concerning video monitoring of production line using wireless technology has been accepted.

2.4.6 International and national networking

This project will co-operate with EU FP5 CHEM -project (Advanced Decision Support System for Chemical/Petrochemical Manufacturing Processes) in the area of operator support. In the CHEM project a tool to take existing safety and operability related

information into full use in process operation is developed. The type of co-operation is exchange of information and experiences.

Exploitation of maintenance event information to extend the economic life of plants has been studied by the recently completed EU funded Elapse project. The project was co-ordinated by VTT. Information exchange between the Elapse and Fi-Tool projects will take place trough those researchers who have worked for both of the projects.

The project is collaborating with other projects from VTT's Intelligent Products and Services theme (Älyteema). The TAG, the embedded database which has been developed in the FI-TOOL project, and the protocol to communicate over Bluetooth, will also be used in the "Älypakkaus" project, in which an active communication package is developed. In this project, the TAG will be attached to a parcel, and communicate with a server in the truck.

The project is co-operating with other projects (LIIKKUDIA, SYSTELI) going on the "Methods for life-cycle management" focus area. Liikkudia-project will provide essential diagnostic data to the developed information system. Thus, the Systeli-project can utilise the information while improving the life management of industrial systems using system analytical methods. The demands of the both project will be considered.

This project is doing knowledge exchange with KONEMASINA project (Tekes, VTT, national universities and 10 companies) focused on the issues of the human machine system modelling and the user interfaces. These issues are of great interest to both of the projects although having a slight different point of view and thus completing each other.

An extensive survey on the need and actual use of safety and dependability information within the manufactures of mobile working machines has been carried out by the Turvakaari project (funded by Tekes and industrial partners). Information exchange between the Turvakaari and Fi-Tool projects will take place trough those researchers who have worked for both of the projects.

2.4.7 List of publications

Scientific publications & conference papers

Leino, S.-P., Viitaniemi, J. & Keula, S. (2002) Human comfort and safety analysis in virtual prototyping. Case: Off-road vehicle. In: Proceedings of Digital Human Modelling Conference, Munich, Germany, June 18–20, 2002, VDI Berichte 1675, VDI-Gesellschaft Fahrzeugund Verkehrstechnik – Düsseldorf: VDI Verlag and SAE-International.

Leino, S.-P., Viitaniemi, J., Aromaa, S. & Helin, K. (2002) Dynamics Simulation and Comfort Analysis of Human-Vehicle Systems. In: Kelhä, V. (Ed.). VTT Industrial Systems Review – ISR 2002, Espoo. Pp. 37–41.

Permala, A. & Scholliers, J. (2002) New technologies for multi-modal tracking and control. – Proceedings of 9th World Congress on Intelligent Transport Systems. Chicago, Illinois, 14–17 Sept. 2002. Paper 2084. 9 p.

Reunanen, M., Scholliers, J., Säämänen, A., Viitaniemi J. & Välisalo, T. (2004) Improving Safety and Dependability by Enhancing the Availability of Product Specific Information. Psam 7 – Proceedings of The 7th International Conference on Probabilistic Safety Assessment and Management, 2004. June 14–18, 2004, Berlin, Germany. (Accepted.)

Tiusanen, R., Hietikko, M. & Alanen, J. (2002) Procedure and analysis methods for risk assessment of automated working machinery. VTT Industrial Systems Review 2002. Pp. 42–47.

Tiusanen, R., Hietikko, M. & Alanen, J. (2002) Risk analysis of a large-scale mine automation system. 4th International Conference on Machine Automation, ICMA'02.Tampere, 11–13 Sept. 2002. Tampere University of Technology TTKK. Pp. 475–782.

Viitaniemi, J., Säämänen, A. & Reunanen, M. (2004) Safety and Dependability Information Exploitation in Maintenance Planning and Product Development. NordDesign 2004: Product Development in Changing Environment, 18–20 August 2004, Tampere, Finland. (Abstract Accepted.)

Reports

Management of safety and reliability knowledge during the lifetime of working machines – State-of-the-art. (In Finnish: Turvallisuus- ja käyttövarmuustiedon hallinta työkoneen elinkaaren aikana – Nykytilaselvitys.) VTT Industrial Systems. 2003. Fi-Tool project internal report.

Management of safety and reliability knowledge during the lifetime of working machines – System requirements. (In Finnish: Turvallisuus- ja käyttövarmuustiedon hallinta työkoneen elinkaaren aikana – Järjestelmävaatimukset.) VTT Industrial Systems. 2003. Fi-Tool project internal report.

Vidqvist, V. (2003) Distributed Multimedia Systems. VTT Research Report.

Inventions

Kuivanen, R., Säämänen, A. & Viitaniemi, J. (2002) Video monitoring of production line using wireless technology. (In Finnish: Tuotantoprosessin seuranta langattoman teknologian avulla), Employment invention. Taking into possession, date 20.12.2002, Announcement nr. 002149.

Other publications

Presentation at the ICT portal opening, November 2002.

Presentation at Automaatiopäivät 03 exposition, September 2003.

Presentation at Tehdaspalvelu 03 exposition, October 2003.

3. Human-Technology Interaction and safety

3.1 Executive summary

Maaria Nuutinen

In recently published VTT Roadmap report *"Human-Technology Interaction Research and Design"* human-technology interaction is defined as follows: "Human-Technology interaction denotes the activity of a distributed cooperative system that the users and the technology form together with their physical and social environment." (Norros, L., Kaasinen, E., Plomp, J. & Rämä, P. (2003.) Human-Technology Interaction Research and Design. VTT Roadmap. Espoo: VTT Research Notes 2220. P. 9). This report also stresses the multilevel nature of the HTI phenomenon and that it should be studied from many different perspectives. Research activities on the HTI area are currently rich and extensive at VTT: about 70 projects were linked to HTI theme (Norros et al. 2003). As illustrated in the report there are many important HTI research challenges that are considered significant for the development of HTI and information and communication technology.

As a part of the VTT Safety and reliability theme, *the HTI and safety focus area* emphasises the importance of understanding the role of human activity in the construction of safety and reliability of any technical system. In safety critical domains there are particular demands for designing and modifying HTI and assessing its safety effects. The focus area consists of three projects: "Development of a human centred design methodology for human machine systems" (T4METODI), "Offshore VTS for the Gulf of Finland" (T4VTS) and "New interfaces in the cabins of the future in movable machines and vehicles" (T4CABIN).

3.1.1 Objectives

The main aim of the focus area is to increase VTT readiness to fulfil HTI needs on safety critical domains by bringing together results and experiences from the HTI projects (including also projects outside of the safety and reliability theme umbrella), co-operating and sharing knowledge of HTI relevant issues on different domains.

3.1.2 Main results and impacts

The projects are still in progress and the gained results are presented in the project reports. However, there are several general results of the focus area research activity that have been promoted readiness to tackle HTI & safety issues and are therefore worth mentioning here. The fact that different kinds of domains and levels of technology mediated interactions to the environments are well represented in the focus projects creates good possibilities for comparisons highlighting both similarities and unique

characters of the domains and for more general level discussions between specialists. This has created an excellent prerequisite for following development:

- increasing knowledge about available HTI research, human reliability and human centred design methods; similarities and differences of HTI on different domains; the applicability of the existing and new methods to different HTI problems

- understanding of HTI phenomena, what kind of shape the HTI problems can take in practice, how to manage HTI related risks

- increasing cooperation, information sharing and common project preparation over organisational boundaries

- developing and "transferring" competencies. The project teams have members with different educational and occupational backgrounds and experience. The focus area activity has also promoted individual development of expertise (doctoral thesis work)

- increasing knowledge about VTT HTI expertise and international research partners

- increasing knowledge of HTI needs and future trends at industry

- communicating the importance of the user point of view and the behavioural science based ways of doing that. This communication has been directed towards public financier, industry customers and VTT engineers. The communication has also served marketing purposes

- learning from a domain to an other domain in order to avoid "the old mistakes" of the technology driven development. The technology mediated work has a long history (See e.g. Zuboff S. 1988. In the age of the smart machine. New York: Basic Books.) and the HTI safety issues have been studied for a long time on "old" safety critical domains like aviation, nuclear power production and transport industry. Increasing complexity, technology mediatedeness and automating are current new trends on domains like mining and forest industry. For example, development of automated mining, remote control of machines and vessel traffic service can gain lot of the lessons learn from the "older" domains. Specially, about how technology changes human work, how the risk associated with the change can be managed, what kind of methods are available etc. Also the "old" domains can take benefit from new technical innovations of the "new" domains. These can be for example experiences from the use of virtual reality and virtual environments.

3.2 Development of a human centred design methodology for human-machine systems (METODI)

Maaria Nuutinen

3.2.1 Background of the project

There are increasing safety, reliability and economical demands in industry and transport. These demands emphasise the efficiency of Human-Technology Interaction (HTI). The importance of taking human factors into account already in the design phase of the system has been widely noticed. This human-centred design (HCD) can be seen as a key factor in ensuring the safety and reliability of future systems. However, there is no agreement on basic questions like, what is human-centred design, what are criteria for valid methods in different domains and what kind of conception of user should be adopted for the basis of design, neither in behavioural science nor in technical design practice.

HCD is often restricted to user interviews and small-scale experiments that focus on particular features of the product. In resent times the restrictions of this kind approach are noticed, particularly in safety critical domains. Many international research groups are currently searching ecologically oriented approaches to user studies in order to analyse HTI more comprehensively and in its real context. VTT share this aim. As a central actor in the field of the new technical innovations, VTT provides fruitful environment for future oriented, interdisciplinary and internationally competitive research activities in the development of HTI. This project brings together the expertise and the work done in different research units of VTT and their business and research partners.

The emerging research topic "Human-Technology Interaction" (HTI) is an important part of the humane technology development of VTT. The main challenge of the HTI research is to develop concepts and methods for human-centred design. The research project "Development of a human-centred design methodology for human machine systems" (T4METODI) was started 2002 and is in progress. As a part of the Safety and reliability theme, this METODI project focuses on Human-Technology Interaction issues in safety critical domains. In these domains HCD principle should be adopted for the whole life cycle of the system. Safety demands put particular constraints on the methods of human-centred design and emphasise the usability and controlled modifications of the systems and products.

3.2.2 Objectives

The general aim of the project is to develop a human-centred design methodology of human-machine (technology) systems. This methodology pursues to construct a bridge between human activity analysis and engineering design. New and modified methods for integrating HTI design into system's life cycle planning and evaluating HTI safety effects will be created. These will include a test regime for evaluating available or near market in –vehicle information systems, a use-case based risk analysis for automated mobile machine systems, an activity system approach based accident analysis for promoting development of the system and a tentative, core task analysis based validity method for control room modifications. The results of the project will be published on VTT reports, conference papers and scientific articles. The main results and methodological conclusions will also be published in a concluding book.

The development work is conducted in detailed case and pilot studies on different domains, which represent different levels of the Human-Technology Interaction from direct control of a machine (passenger car driving) to the mediated control of machine(s) or process (remote use of mining machine and pulp process) and the divided control of complex socio-technical systems (vessel traffic service).

This project is very challenging and there are many theoretical, methodical and practical questions open. The development of applicable human-centred design methodology requires continual interdisciplinary working and discussion between experts on psychological theories, technological development and innovations and practical problems during the project. This will and had been ensured by interdisciplinary project team, common workshops and cross occupying the work packages.

3.2.3 Main results

The project produces four kind of results: HCD methodology and methods, knowledge of HTI and safety effects, knowledge of practical HTI needs, and co-operation and competence.

<u>HCD methodology and methods</u>

At the beginning of the project the existing HTI research methods and frameworks used at VTT were reviewed and development needs recognised. Also the applicability of common user-centred methods for presenting the requirements of complex system was evaluated.

The methodical work is in good progress. For example, the existing VTT's method called the core task analysis were tested and further developed for design purposes by modelling the core task of remote mining machine operator and vessel traffic service operator. A preliminary model, "Human-Technology Interaction design process" for integrating HTI issues into technical design process of automated mining was defined. This model was guided by the current design practices and planned for an intermediate phase on the way to real human centred design practices. In order to develop a test regime for available or near market in-vehicle information systems the field experiment was conducted in the instrumented car. As result tentative safety indicators of driver behaviour was identified.

In the future the emphasis of the project will be on analysing further the cases, reflecting the developing and developed methods and constructing methodological conclusions. The need of additional cases will be critically assessed.

Knowledge of HTI and safety effects

In addition to methodical results the project produces knowledge about the safety effects of HTI on case domains. This knowledge (as well as methods) has been shared and submitted for critical scientific evaluation in several international conferences. These conferences have also served as networking purposes on scientific research partners.

Knowledge of practical HTI needs

Networking with industrial partners and conducting case studies have created deeper understanding of practical HTI challenges faced on the case domains. The future trends at HTI area were also clarified. In the same process the project has prepared the way for adopting more broadly the human centred point of view in technical design and modification of complex systems at industry. The project participated Human-technology road map work which provided an analysis of the generic societal and technical changes that increase the need for understanding HTI issues and identified main research challenges in this area.

VTT co-operation and competence

The project has already increased the co-operation between HTI researchers at VTT and created understanding of each group's special competencies. This will promote the reaching of the best HTI expertise for future projects. During the project also VTT's competence in general at this area is developing through e.g. conducting case studies, making literature reviews, participating conferences and research exchange. The work done in the project also supports PhD thesis going on.

3.2.4 Expected impacts

The project provides direct benefits for industries participating in the case studies. The better-designed human-technology system degreases cost caused by, for example, human error or delayed implementation.

At VTT the main result of this project is the "bottom-up" impact on the long-term HTI challenge; the development of human-centred design methodology. The project provides knowledge about the restrictions and possibilities of the different human-centred methods for designing the safety-critical human-technology systems. The four kinds of the results produced at the project ensure that VTT will have advanced readiness to fulfil HTI needs on safety critical domain in the future.

3.2.5 List of publications

Scientific publications

Norros, L. (2004) Acting under uncertainty. The core-task analysis in ecological study of work. Espoo: VTT Publications 546. 241 p. ISBN 951–38–6410–3; 951–38–6411–1

Norros, L. & Nuutinen, M. (2002) The concept of the core task and the analysis of working practices. In: Oreham, N., Samurcay, R. & Fischer, M. (eds.). Work Process Knowledge. Routledge, London. Pp. 25–39.

Norros, L. & Nuutinen, M. Contextual validation of a disturbance management system. (Accepted for publication in International Journal of Human-Computer Studies.)

Nuutinen, M. (2003) Change of generation as a challenge of safety critical work. Työ ja ihminen 17:2, pp. 173–189. (In Finnish.)

Nuutinen, M. Contextual assessment of working practices in changing work. (Submitted for publication.)

Nuutinen, M. & Norros, L. Learning from accidents: an ecological approach to accident investigation. Risky Work. (Submitted.)

Nuutinen, M. & Norros, L. Learning from accidents: an ecological approach to maritime accident investigation. (Submitted for publication.)

Savioja, P. (2003) User-centred methods in presenting the requirements of complex systems. (Master's thesis in Finnish.)

Conference papers

Norros, L. (2003) Understanding use in the design of smart objects – reflections on the conception of collaborative design. Smart objects conference, Grenoble, 15–17 May 2003.

Norros, L. (2003) Combining causal and reason-based explanations of actions – Improving learning from accidents. New challenges to understanding system safety, 6–7 October, Fredensborg, Sweden.

Tiusanen, R. & Karjalainen, J. (2003) System level approach for safety risk management of teleoperated working machinery applications. SIAS 2003 (Safety of Industrial Automated Systems).

VTT reports

Norros, L., Kaasinen, E., Plomp, J. & Rämä, P. (2003.) Human-Technology Interaction Research and Design. VTT Roadmap. Espoo: VTT Research Notes 2220. 118 p. + app. 11 p. [1] ISBN 951-38-6196-1; 951-38-6197-X. http://www.vtt.fi/inf/pdf/tiedotteet/2003/T2220.pdf

Nuutinen, M. (draft) Modelling of the core task. The task of the VTS operator and mining machine operator. (In Finnish.)

Nuutinen, M., Reiman, T. & Oedewald, P. (2003) Osaamisen hallinta ydinvoimalaitoksessa operaattoreiden sukupolvenvaihdostilanteessa [Management of operators' competence and change of generation at NPP]. Espoo: VTT Publications 496. 82 p. (In Finnish.). ISBN 951-38-6046-9; 951-38-6047-7. http://www.vtt.fi/inf/pdf/publications/2003/P496.pdf

Rathmayer, R. & Luoma, J. (2002) Traffic researcher's manual. (In Finnish.)

Rathmayer, R. & Rämä, P. (eds.). (2003) Research frameworks of Human-Technology Interaction at VTT. (In Finnish.)

Rathmayer, R. & Rämä, P. VTT's approaches for studying Human-Technology Interaction. (In Finnish.)

[1] Result of VTT Key technology action work

3.3 Offshore VTS for the Gulf of Finland (VTS)

Tapio Nyman

3.3.1 Executive summary

The research project "Offshore VTS for the Gulf of Finland (T4VTS)" was started in 2001 under the VTT large-scale research theme Safety and Reliability. The backbone for this research project was the need for new tools to improve the maritime safety and to protect the Baltic Sea environment against the risks caused by the increasing maritime traffic, particularly against the threat imposed by the increase of marine oil transportation.

The acronym VTMIS (Vessel Traffic Management and Information Services) is often used for the entirety consisting of the various telematic and information systems developed to enhance the safety and effectiveness of the maritime traffic. Also the term Offshore VTS has been used in the same context (VTS = Vessel Traffic Service).

VTMIS was considered to be a primary tool to assist merchant maritime traffic in the Gulf of Finland area. The maritime authorities of Russia, Finland and Estonia decided to establish a VTMIS consisting of a new routing system and a mandatory ship reporting system for this sensitive sea area. This decision was based on the preliminary study conducted by VTT. This in turn launched a heavy need for the new simulator research and training environment where various traffic scenarios could be arranged and studied.

The primary scheme of the new research project consisted of (1) FSA risk analyses (Formal Safety Assessment), (2) designing and building of a new generation VTMIS simulator and (3) creating of the research and training environment to test and develop the methodologies for the human-machine interaction.

At present, the uniform procedures for the operators conducting their work in the future VTMIS-system are under construction, which in turn forms a challenging environment for the R&D work. The new procedures being created here will be based on the IALA (International Association of Lighthouse Authorities) and IMO (International Maritime Organisation) guidelines and regulations. This means that these procedures will have an international significance since they can be applied in similar systems to be established in other sea areas of the world.

For the year 2004, the work is divided into three work packages:

- Implementation of the simulator environment [WP1]
- Development of the Intelligent Marine Risk Indicator (IMRI) [WP2]
- Analysis and modelling of the working procedures of the VTS operators [WP3].

3.3.2 Objectives

The aim of this research project theme is to establish a VTS/VTMIS simulator to Otaniemi in the frames of the designed new VTMIS service for the Gulf of Finland.

The strategic objective is to achieve the internationally accepted status as a classified maritime safety expert among the Baltic Sea states and to promote modern navigation and safety aids world-wide in the frames of the sustainable development.

The technical objective is to connect various simulators and use them linked via the Internet or other telematic means in real-time or in virtual environment. The essential feature of the new system algorithm is the enhancement of simulation research activities for the stakeholders. To the technical objectives of the project can also be added the development of the equipment and user interfaces in the VTS-centres based on the HTI (Human-Technology Interaction) expertise of the project team as well as on the information collected of the work of the VTS operators.

The operative objective of the project is to analyse and develop the working procedures of the VTS/VTMIS operators by simulator exercises, by observations in the existing VTS centres and by operator interviews using a method called core-task-analysis. The experiences obtained in the analysis can be utilised in developing the HTI methodology in the METODI-project. This work also collects material for the training purposes of the VTS/VTMIS-operators.

3.3.3 Main results

In 2003, the work in WP1 (Design of the VTMIS simulator environment) and WP2 (Introducing HLA technology for linking of various simulators) has started according to the project plan for 2003. WP3 (Implementation of the VTMIS simulator) will continue in 2004. The goals of WP4 (Development of an information system to support the VTS/VTMIS operation) will be fulfilled by participating in the work of the Trilateral Committee Technical sub-Committee where the experts from Finland, Russia and Estonia are developing the information system. WP5 (The Intelligent Marine Risk Indicator IMRI) will start in latter half of the year. An application for additional funding for the WP5 has been sent to the EU INTERREG program.

The connections to the Estonian and Russian Maritime Administrations as well as to the St. Petersburg and Tallinn VTS -centres have already been established in early stages of the project. Connections to the Traffic Centre Hoek van Holland, Rotterdam Port Authority, Maritime Simulation Rotterdam b.v., Maritime and Coastguard Agency in

UK, the Channel Navigation Information Service (CNIS) in Dover and the Marine Simulation Centre of the South Tyneside College, were established by visiting the institutes in May 2003. Dover was the first place in the world to have radar based maritime traffic surveillance. The operation started already in 1972 and thus the co-operation with CNIS gives this project valuable information based on years of experience. Information exchange with CNIS has been started. Connections will also be established to the Svendborg International Maritime Academy (SIMAC) in Copenhagen and to the VTS-centres of Kørsör and Gothenburg as well as to the National Maritime Research Institute in Japan following the contacts of the international Scientific advisory board of the Safety and reliability theme.

VTT prepared a Formal Safety Assessment, which was submitted to the International Maritime Organisation, IMO, as a justification for the adoption and enforcement of the new trilateral VTMIS system. The report was also given to the HELCOM countries. In addition the results of the project were presented in the international RINA-conference (RINA = Royal Institute of Naval Architects) "Formal safety assessment". VTT has also been invited to participate in the FSA enhancing discussion arranged during the IMO Maritime Safety Committee meeting.

The basis of the harmonised operational procedures for the operators working in the VTMIS centres have been developed and tested. This work begun already in 2002 when the experts and maritime authorities of Estonia, Finland and Russia gathered to the first Operational Exercise (OE I) arranged in Otaniemi. During this meeting several operational guidelines were developed but also major defects and imperfections in the definition of the system were discovered. The results of the OE I were submitted for consideration and approval of the Trilateral Committee. The Committee recognised that it is necessary to further development the system and in conclusion appointed an Operational sub-Committee and a Technical sub-Committee to promote the development of the VTMIS. The preparation of the Document of Joint Procedures (DJP) was stated on the basis of the results of the OE I and the decisions made by the Committee. The second Operational Exercise OE II) was arranged in April 2003. The results of OE II as amended by the Operational sub-Committee have now been included to the draft DJP and it is submitted for the approval of the Committee in its meeting in August 2003.

The work aimed to link the simulators in Otaniemi i.e. the Finnish Maritime Safety Training Centre (Meriturva), VTT/TUO together with the foreign systems has been started. Simulator co-operation with VTT and Meriturva was deepened to get resources to fulfil both training and research tasks. Here VTT's focus area was selected to promote new technology of the system and to create new operational procedures together with the stakeholders. The preliminary contacts to the international simulator manufacturer

TRANSAS as well as to Navielektro, a subsidiary of the Norwegian Navtec Company delivering equipment to VTS-centres and navigation bridges of ships were established. In addition the contacts to another simulator and VTS-equipment manufacturer HITT NV are planned. Finally, the analysis of the work of the VTS/VTMIS operators was started with observation visits to the Helsinki VTS-centre.

3.3.4 Impacts

World-wide

The VTMIS-simulator, being a combination of different research and training simulators in Finland, Russia and Estonia, offers an international platform for maritime safety research and for planning and further developing the harmonised trilateral operation in the VTMIS-area.

The general framework of the VTS/VTMIS operators' work is outlined in the international regulations and guidelines of IMO and IALA. Thus the working procedures developed in the project for the Gulf of Finland are applicable world-wide for corresponding marine information systems.

National

The simulator will serve as a training facility for the VTS/VTMIS operators of the Finnish Maritime Administration. It will also be a testing platform for the equipment manufacturers delivering equipment and systems to VTS/VTMIS centres.

VTT

VTS/VTMIS-simulator is an effective tool to be used in maritime safety research in the "risk based approach" systems and Human-Technology Interaction (HTI) studies.

3.3.5 List of publications

International conference papers

Nyman, T., Rytkönen, J. & Jolma, K. (2002) FSA analyses as a risk analyses tool for Arctic and Sub-arctic maritime environment. Proceedings of Joint EU-Russia-Canada-US Arctic Workshop. October 25–27, 2001, Brussels. Pp. 510–518.

Rosqvist, T., Nyman, T., Sonninen, S. & Tuominen, R. (2002) The implementation of the VTMIS system for the Gulf of Finland – a FSA study. International Conference on Formal Safety Assessment. The Royal Institution of Naval Architects (RINA). 18.–19.09.2002, London. 8 p. + app.

Rytkönen, J. (2002) Maritime Transportations of the Baltic Sea and the proposed Actions to Improve the Maritime Safety. Nordiska Sjöförsäkrigspoolens årsmöte, Helsingfors, June 29, 2002.

Rytkönen, J., Mylly, M., Chernyaev, R. & Veskimets, A. (2002) Recent Efforts to Improve the Maritime Safety Issues in the Northern Baltic Sea. PIANC 2002, 30th International Navigation Congress. Sydney, Australia. September 2002. Pp. 793–804.

Scientific and technical reports and publications

FORMAL SAFETY ASSESSMENT. The implementation of the VTMIS-system for the Gulf of Finland. IMO/NAV-official documents, accepted by IMO in June meeting.

Hänninen, S. Nyman, T., Rytkönen, T., Rosqvist, T., Sonninen S., Tuominen R., Juva, M., Jalonen, R., Palonen, A. & Riska, K. The implementation of the VTMIS system for the Gulf of Finland. Formal Safety Assessment study. Research Report VAL34-013153 VTT Industrial Systems. 102 p.

Hänninen, S., Sonninen, S., Nyman, T., Rytkönen, J. Rosqvist, T. & Tuominen, R. Sea-Borne traffic in 2000 up to 2015 in the Gulf of Finland. A brief statistical analysis in connection of the VTMIS development for the Gulf of Finland. Presentation held in the Ministry of the Traffic and Communications in 21.03.2002.

Sonninen, S. (2002) The first Operational Exercise on the operational aspects of the Gulf of Finland mandatory Ship Reporting System (SRS). Research Report TUO34-021653. VTT Industrial Systems. Espoo. 27 p. + app. 21 p. (In Finnish)

Sonninen, S. (2003) A travel report of visits to the Traffic Centre Hoek van Holland and Rotterdam Port Authority, Maritime Simulation Rotterdam b.v., the Channel Navigation Information Service centre in Dover and the Marine Simulation Centre at South Tyneside College, Newcastle. Research Report will be delivered in 2003.

Sonninen, S. The second Operational Exercise on the operational aspects of the Gulf of Finland mandatory Ship Reporting System (SRS) including the development of the Document of Joint Procedures (In Finnish). Research Report will be delivered in 2003.

The implementation of the VTMIS system for the Gulf of Finland. Formal Safety Assessment study. Appendix to the report VAL34-013153. 102 p.

List of media references

Nyman, T. (2003) Use of simulators in the planning of the maritime traffic control. Lecture held in the scientific seminar of the Safety and reliability theme. Aulanko 3.4.2003. (In Finnish.)

Research scientist Sanna Sonninen 10.3.2003 in article in Der SPIEGEL -magazine "Alarm auf der Ostsee: Eiswinter zeigt steigende Gefahr einer Ölpest".

Rytkönen, J. (2003) New winds of the sea transportation in the eastern Gulf of Finland – oil transportation strongly growing. Evening seminar on the future of the Gulf of Finland. The Kymeenlaakso environmental protection district, Adult educational centre of the Helsinki University in Kotka. Kotka 20.2.2003. (In Finnish.)
http://www.inf.vtt.fi/pdf/jurelinkit/TUO_Rytkonen2.pdf.

Rytkönen, J. (2003) On the safety of the maritime traffic in the Gulf of Finland. Tekniikka ja Kunta. Vol. 27, No. 3, pp. 14–17. (In Finnish.)
http://www.inf.vtt.fi/pdf/jurelinkit/TUO_Rytkonen.pdf

Rytkönen, J. (2003) Tanker traffic and traffic control and monitoring systems. Oil transportation in the Gulf of Finland -seminar. Kymeenlaakso Polytechnic; Adult educational centre of the Helsinki University. Kotka 9.4.2003. (In Finnish.)

Rytkönen, J., Hänninen, S. & Sonninen, S. VTT recommends the implementation of the VTMIS-system for the Gulf of Finland. Press release for the Minister Kimmo Sasi's press meeting 21.3.2002.

Several articles/stories in Finnish magazines and newspapers, including radio and television.

Sonninen, S. & Rytkönen, J. (2004) Security on the Roads, Sea and in the Air, Press Tour in Finland, 17.–23.2.2004. "Research on vessel traffic information systems at VTT Industrial Systems", Helsinki Sea Traffic Centre, 18.2.2004.

3.4 New interfaces in the cabins of the future in movable machines and vehicles (CABIN)

Timo Määttä

3.4.1 Background of the project

The products of movable working machine industry are ever more versatile and need to be designed more for the process of a customer rather than as tool. The importance of usability and safety of a movable working machine as a part of production is increased. The needs for user and environment friendly products are also rising. The development of technology will give possibilities to resolve the problems in handling the needs. The intelligence of a product will increase. The product will be able to learn about the behaviour of the user and of the environment, and adapt to new situations to work effective and safely. These features are in some part already implemented in the automotive industry. New interface technology is under research and developing activities in the world for cars but less activity is aimed for developing new interface technology for movable working machines.

The project integrates the knowledge of different research institutes in the field of movable working machines and interface technology including human centred design. The project highlights the need for new design concept for interface of machines and vehicles and is aimed to reach into a new level of technology assisted manoeuvrability. It will emphasise the safety and reliability of a movable working machine by developing interfaces taking account the different use situations more analytically than before.

3.4.2 Objectives

The main objective is a new simulation based methodology for operator centred design of cabins in movable working machines and vehicles in terms of safety and reliability.

The partial objectives of the project are:

- A new operator centred and simulation technology based interface design method for movable working machines

- New concept for adaptive interface technology in movable working machines.

3.4.3 Main results

The main results are the Technology Road Map and the information of the needs collected from the companies for the new interface technology of movable working machines and vehicles. According to the roadmap and industrial interviews a new project proposal for the CABIN theme project has been built. The impact of this project will be based on the second stage of the project as it will be started in the year 2004. As for now the background information for the project has been collected.

There have been no major scientific or technological impacts so far because of the late starting period and the activity in creating the industrial and financial consortium.

3.4.4 Expected impacts

The technology roadmap has had positive impacts on the industrial interest for the development of interface technology in movable working machines. Three industrial projects have been established according to the roadmap and the ideas of CABIN project. These projects will be interlinked in predetermined way to the CABIN project in the future (2004). Several actions of interest from industrial companies have been notified.

3.4.5 List of publications

Määttä, T. (2004) Virtual environments in machinery safety analysis. PhD dissertation. Espoo: VTT Publications 516. 170 p. ISBN 951-38-6261-5; 951-38-6262-3. http://www.vtt.fi/inf/pdf/publications/2003/P516.pdf

Naumanen, M. (2003) Technology Road Map for the Movable Working Machines and Vehicles. VTT, Internal Report. 49 p.

4. New technologies and business concepts

4.1 Executive summary

Tapani Mäkinen

The three projects, Risk Assessment of Genetically Modified Plants (GMP), Unobtrusive Driver Monitoring Technologies (SYKE) and Trusted Software Technologies (TRUST) represent very different fields under Safety and Reliability technology theme's new technologies focus area. The objectives of GMP was to develop a framework for the risk assessment of genetically modified plants (GMP) that helps the plant developer manage the risks during plant's development cycle. The objectives of SYKE is to develop unobtrusive sensors and related algorithms for monitoring driver behaviour, especially drowsiness while driving. The task of TRUST is to increase reliability, safety and security of software. The projects are also in different stages of their development and networking. While GMP was a very focused national project and has already been terminated, whereas SYKE joined two large EC funded Integrated Projects (IP) and has started its main activities early this year. TRUST as a conglomeration of six independent projects with specific objectives and structures is presently active in three of its subprojects. The GMP project developed a new hazard identification and risk assessment method for GMPs contained use. These methods will be further developed in later projects. SYKE main activities have started in January 2004 and new sensor applications for monitoring driver impairment is expected to be tested by major European car manufactures in four years time. In TRUST the work is underway and the expected outcome of the project is the methodological framework to support any given organisation in the selection of specific knowledge (methods, techniques and skills) to design and demonstrate safety, reliability and security of software.

4.1.1 Background and objectives of the projects

The three projects, GMP, SYKE and TRUST represent very different fields under Safety and Reliability technology theme's new technologies focus area.

The first mentioned of the projects, GMP dealt with creating the framework for the risk assessment of genetically modified plants (GMP) that helps the plant developer manage the risks during plant's development cycle. The other aim was to improve the ecological risk assessment process. The effects that might occur through the use of genetically modified organisms can actualise directly but also through indirect ecological processes. Not infrequently, the potential effects are difficult to determine since there is no earlier operational experience on the use of organisms. Current tools to assess the GMOs risks are based on regulatory lists and they are not designed concerning risk management aspects.

SYKE project aims at developing driver monitoring technologies to address the pressing safety needs of driver impairment accounting for most road traffic accidents today. The research on driver impairment monitoring has made great progress during the past ten years. However, currently there are no systems on the market that can reliably detect driver fatigue. Such a system can not be foreseen on a mass production car until 5 to 6 years from now. The most potential systems are existing as prototypes, and they are still beset by too many false alarms. It is possible that driver fatigue detection systems will not be introduced alone but as a complementary function of an overall driver impairment monitoring system. For this reason, continuous work on sensor optimisation and refinement of data fusion algorithms is needed. SYKE project will bring new unobtrusive sensor technologies for driver impairment monitoring.

TRUST project aims at developing methods to improve software dependability that has been an important research field at VTT for a number of years. Originally, this field was started in the late seventies when the development of programmable instrumentation and control systems made evident a need for high reliability applications such as safety systems at nuclear power plants. Later, development of software-based systems has brought in also other aspects of software dependability that will be addressed in the project. The objective of the main task of the TRUST is to develop a methodological framework which enhances organisational ability to take in use specific methods and techniques to design and demonstrate reliability, safety and security of software. In addition, by the methodological framework organisation is able to educate software developers about software reliability.

4.1.2 Expected impacts

GMO

- Guidance notes to perform the risk assessment for the use of genetically modified plants in contained environment. The paper is recommended and delivered by the Finnish board of gene technology.

- The results and "know-how" gained during the project has been was employed in later projects as in the current Academy funded research project "Assessment and Regulation of Ecological Effects of GMOs in Boreal Environment". The aim is to produce "standardised" procedures for the industry and regulative authorities.

- The industry is interested in comprehensive risk assessment since they can better manage the risks the new technology might pose. However negative public acceptance of GMOs have frozen the research and commercialisation activities in the Europe.

SYKE

- Increased knowledge of non-invasive sensor technologies
- Improved networking of VTT with other major European players in the field
- Possibility to improved traffic safety by means of advanced driver monitoring technologies
- improved market possibilities for Finnish SME's in sensor development area
- project results may have applicability also in other monitoring areas than road traffic only
- negotiations with automotive industry partners for other cooperation in sensor development.

TRUST

- The methodological framework of the TRUST will be a great support for an organisation in selection of specific knowledge (methods, techniques and skills) to design and demonstrate safety, reliability and security of software.
- the integration of the different expertise related to software development process will become easier, resulting to better design solutions.
- Expected impacts for manufacturers of programmable medical devices:
  - systematic and cost efficiency design process
  - better documentation throughout software engineering process
  - better verification and validation activities during software development
  - better software maintenance and management of modification
  - effective and traceability system requirement phase
  - less inadequate or inappropriate software requirements.
- Dedicated devices and systems with embedded software are used in several more or less critical fields (for example, smart sensors and transmitters in nuclear plants and conventional industry, users of mobiles, medical device community). The results of the subproject will support manufacturers and purchasers of these dedicated devices in their effort of qualifying software safety and reliability.

4.2 Driver vigilance monitoring with minimum obtrusiveness (SYKE)

Tapani Mäkinen

4.2.1 Introduction

SYKE project aims at developing new unobtrusive sensors for driver impairment monitoring in car environment. Also other applications are possible, where an operator's activation level monitoring is needed. SYKE has joined two EC funded Integrated Projects (IP) Advanced Integrated Driver-vehicle Interface (AIDE) and Sleep, Wakefulness and Hypovigilance monitoring (SENSATION). The IP's have been started within the three first months of 2004. The first results will be expected in the course of one and a half years. VTT is responsible in the projects for wearable sensors integrated either in the driver's seat or other inconspicuous places including clothing. The expected outcome of the projects is a sensor system that can be used in reliable monitoring of driver/operator impairment and hypovigilance. SYKE project has already by now improved VTT's networking with major automobile and parts manufacturers in Europe and has also paved way to other projects for VTT in Advance Driver Assistance Systems (ADAS) area.

4.2.2 Background and objectives of the project

Currently, there is a world-wide race going on for a real-time system to monitor and detect driver's impairment and reduced vigilance (hypovigilance) specifically. A number of demos and early phase prototypes are being tried out by major car manufacturers now. However, no breakthrough has been made in the area. The objective of SYKE-project is to develop new unobtrusive sensors, related signal processing and algorithms for driver monitoring systems in cooperation with major car manufacturers and other OEMs. Sensor and software technology at VTT have good possibilities of bringing the driver monitoring systems far beyond the current state-of-art. The innovative part includes finding solutions for making existing systems more robust and error-free, which is essential concerning the integration of the system in vehicle control systems. The innovations come from new approach to 3-D machine vision by means of laser technology, monitoring the overall activity level of a driver and new type of data fusion. Driver monitoring systems will be a part of Advanced Driver Assistance Systems (ADAS) in future vehicles – say, in the next 10 years.

4.2.3 Expected impacts

Since the main part of the project has recently started there are not yet any major impacts. Some feasibility tests have been carried out and they have been reported previously.

- Increased knowledge of non-invasive sensor technologies,
- Improved networking of VTT with other major European players in the field,
- Possibility to improved traffic safety by means of advanced driver monitoring technologies,
- improved market possibilities for Finnish SME's in sensor development area,
- project results may have applicability also in other monitoring areas than road traffic only,
- negotiations with automotive industry partners for other cooperation in sensor development.

4.2.4 List of publications

List of publications

Korpinen, J., Laitinen, J., Mäkinen, T. & Viitanen, J. (2002) Kuljettajan monitorointi – Esikartoitus mahdollisista teknologioista ja tutkimusyhteistyö EU-tasolla. (Driver monitoring – Prestudy on potential technologies and cooperation at EU level).

Mäkinen, T., Rouhiainen, V. & Viitanen, J. (2003) Driver Fatigue Monitoring in Europe. Paper presented at the IPSS in Taipei, 18–20 November 2003.

List of media references

SYKE-project themes have been covered in all main media in Finland including local and national papers, radio and TV. The number of newspaper articles and other media coverage exceeds 20.

4.3 Trusted software technology (TRUST)

Hannu Harju

4.3.1 Introduction

TRUST project consists of one main task and six subprojects (SP's). The subprojects are independent research projects with special objectives, resources and budgets. The objective of the main part is to gather specific results of the subprojects. Some of the subprojects have already begun (SP's 1, 2, 4 and 6); some will begin later on this year and they are not under the scope of this report.

The task of the main part of the TRUST firstly gathers and edits the research results of the subprojects for a so called knowledge body. Secondly, it will compress the knowledge body for sets of fundamental principles. Finally, a collection of fundamental principle sets are utilised in developing a methodological framework which enhances organisational ability to take in use specific knowledge (methods, techniques and skills) to design and demonstrate reliability, safety and security (dependability) of software. In addition, with the support of the methodological framework, software developing organisation is able to educate their developers about software dependability.

Executive summary of the subprojects 1, 2 and 4

In software engineering, the different points of view of experts representing different disciplines and the lack of a common language may prevent the systematic ways of acting and increase software failures which contribute to reduced software dependability and effectiveness of software production. The long term objective of the subproject 1 *"Safety Culture"* is to develop procedures and tools which help in improving communication practices in co-operation between experts working in software design teams, between the different phases of the development process and between the designers and the users. The prerequisites for applying a new approach, a systemic communication analysis method, originally developed for nuclear waste management, to software engineering have been considered and a common concept concerning the content and the way of realising the subproject has been created in co-operation with the representatives of subprojects 2 and 3.

Despite the great amount of development knowledge, experience, and tools available today, a remarkable percentage of software projects fail. Often the reason is that the requirements are not correctly determined and defined at the beginning, or are not managed correctly as the project progresses. The subproject 2 *"Managing Software*

Requirements" concentrates on safety and reliability requirements of critical software in area of medical device industry.

Various parties (licensers, manufacturers and users) of software based systems have recognised the problems raised by the evaluation of software dependability of dedicated devices. In the subproject 4 "*Qualification of Dedicated Systems Software",* these problems are concentrating on the difficulty of assessing existence of critical software errors. The coverage of the large number of distinct behaviours of a discrete system means that the testing is not sufficient for the assessment of reliability of software based systems. However, complexity of functions of system or device, its potential for configuration, and the extent of its interfaces and interactions with the rest of the system can possibly be limited so as to allow a thorough functional coverage by tests.

Possible common cause failure modes of software systems make the assessment even more difficult. An error in single version software of multiple processors is unquestionably an important source of common cause failures. Several partial and complementary approaches exist for the solution to these problems. Isolation of safety and non-safety functions, functional diversity, and independent V&V are one of the most effective solutions.

4.3.2 Background of the project

Software dependability has been an important research field at VTT for many years. Originally, this field was started in the late seventies and early eighties when the development of programmable instrumentation and control systems made it evident that they would have to be introduced also in high reliability applications such as safety systems at nuclear power plants. Later development of software-based systems has brought in also other aspects of software dependability. The list in the appendix describes some finished and on-going projects within VTT Industrial systems, which are related to software dependability.

Problems that need a new way of thinking to be solved are the following:

- Software reliability theory is defective. It is based on random failures and possesses similarities with hardware reliability theory. This prevents development of good design and demonstration practices.

- Software is everywhere. Practices to design and implement vary between application domains challenging reliability design and demonstration.

- There is not time to design and demonstrate reliability in software development projects themselves. Demonstrations are used only in very critical application domains.

- Students and new researchers have difficulties to familiarise themselves with the subject of software dependability.

- There are too many application specific processes and methods for demonstration of software dependability.

- There are too many possibilities to integrate dependability processes and design processes.

SP 1. Safety Culture

Not only technical but also human aspects have an effect on software dependability. In software production human co-operation is fundamental and this challenges the way the persons communicate with each other. The different points of view of experts representing different disciplines and the lack of a common language may prevent the systematic ways of acting and increase software failures. There is, therefore, a need for developing methods which help in improving the communication practices.

In VTT Industrial Systems a new approach has been created for the analysis and development of multidisciplinary expert communication. The approach has originally been developed for the analysis and development of expert communication practices in nuclear waste management, at Posiva Oy, Finland. The basic idea of the approach is that in order to improve communication, the experts' mutual understanding has to be increased and the essential content of the mutual information needs have to be identified.

The developed method is a systemic communication analysis which consists of two types of analysis, a core-knowledge analysis and a cognitive network analysis. The purpose of the former one is to identify what the experts belonging to the focused work chain have to understand of the whole and of the connections between their tasks in order to be able to carry out their tasks and communicate in the best possible way. In the latter analysis the interfaces between the different experts' tasks are defined and the associated information-related dependencies between the tasks are identified. After that, the information needs resulting from these dependencies are defined and the factors which hinder the necessary flow of information are identified. Finally, the criteria for the communication practices which enhance software dependability and the effectiveness of software production are defined. On the basis of the criteria the

practical development procedures are designed for the organisation's process system, training, knowledge management and for the experts' personal communication. It is important that the experts representing different disciplines and contributing to the same work chain make the analysis together, discussing the common aims and related communicational aspects from the different points of view.

SP 2. Managing Software Requirements

Requirements specification is one of the most important portions of software engineering. By a good specification the implementation of safety requirements, schedule and cost-effectiveness of design process can be assured. To developers, managers, and quality assurance personnel of the medical device industry, the complexity of device technology seems to be growing almost exponentially. Running modern medical devices requires thousands of lines of complex software.

This increasing complexity will invoke a fundamental question to be solved: What are the real requirements for such a device? The answering to this question will support of solving how devices claims of safety can be assured and measured. In addition, managers of company can predict the level of effort that will be required to develop and produce the device. Requirements management technique can be used effectively to manage this increasing complexity.

SP 4. Qualification of Dedicated Systems Software

The subproject establishes the concept for demonstrating safety of software of dedicated programmable system. This kind of software often adopts many black box or COTS features. The software might have high reliability and safety features, but the purchaser does not have demonstrated knowledge of the level of the reliability or safety. Software usually is single version software and diversity requirement has to be managed only by functional redundancy.

The embedded software of dedicated system may be relatively large. In addition, safety and reliability requirements are often high. In spite of these facts, purchasers are not willing to pay as much qualification costs of dedicated systems software as for similar software, for example in large control system. This is because size of a dedicated device is small; nothing compared with normal control systems. There is a need for a sophisticated evaluation method of software safety and reliability. Unfortunately, in research literature, there is not any coherent description about the fault tolerance methods for single version software.

SP 6. Software dependability in complex systems

Reliable and continuous electricity supply has become more and more important for the electricity consumers as the use of sensitive equipment and processes rapidly increases. Already short outages and voltage dips result in high costs for many consumers.

Electricity supply is increasingly dependent of devices and systems that include software. At every level from network operation and substation automation down to individual components such as protection relays, software plays a crucial role nowadays.

4.3.3 Objectives

The objective of the main task of the TRUST is to develop a methodological framework which enhances organisational ability to take in use specific methods and techniques to design and demonstrate reliability, safety and security of software. In addition, by the methodological framework organisation is able to educate software developers about software reliability.

SP 1. Safety Culture

- Development of new procedures and tools which help in improving the communication practices between persons working in software design teams, between the different phases of the development process and between the designers and the users.

- Objectives for 2003: Preparation of the subproject in co-operation with the representatives of subprojects 2 and 3 by creating a common concept concerning the content and the way of realising the task.

SP 2. Managing Software Requirements

The objective is to develop instructions and guidelines for requirements management of medical device software development. These instructions will offer the following benefits that would otherwise be missing from the software development process:

- better control of the development project

- common understanding within the development team of what must be built and tested

- better demonstration of software reliability and safety

- reduced project costs and delays by early reduced requirements errors

- easier compliance with regulations.

SP 4. The Qualification of Dedicated Systems Software

The objective of the subproject is to produce principles by which the software safety qualification can be cost-effectively performed for dedicated programmable device.

SP 6. Software Dependability in Complex Systems

This subproject focuses on the impact of software on electricity distribution reliability. Network reliability programs of today do not generally include modern distribution automation in sufficient detail. The aim is to develop methods that consider issues of reliability in a systematic manner when dealing with software development within electricity distribution.

4.3.4 Main results

SP 1. Safety Culture

A common concept concerning the content and the way of realising the subproject has been created, and a plan for the subproject has been made, based on the concept. Sales material for the method has been made.

SP 2. Managing Software Requirements

- Development of software traceability matrix between software requirements and risk management

- Preliminary method for identification of safety critical requirements.

SP 4. The Qualification of Dedicated Systems Software

- Software design faults. This task was considering the problem of software faults, and provides background for constructing the Knowledge Body for qualification of single-version software.

- Means for dependability. The following four means to manage with software faults were presented: avoidance, removal, fault tolerance, and operator actions.

- Design for software fault tolerance for a single-version software. Dependability by using fault tolerance techniques to a single-version of a piece of software is

achieved by introducing special fault detection and recovery features into the software of the system. These include considerations on 1) modularising, 2) error detection, and error recoveries: 3) exception handling and 4) check pointing, 5) process pairs, and 6) data diversity.

- Hardware and software interaction. A significant cause of a failure of computer devices is a transient fault that will manifest in hardware-software interaction. Failure modelling of dedicated devices should contain permanent and transient faults in the hardware, and permanent faults in the software, and effects of hardware transient faults on the software behaviour.

SP 6. Software Dependability in Complex Systems

The work has started with surveying electricity distribution systems from a reliability point of view. The subproject focuses first on substation level; on protection and substation automation. The work will incorporate malfunction of devices including software in reliability assessment of distribution networks.

Features within power system control that are most critical with regard to reliable electricity supply will be defined. The role of different protection schemes and individual relays on the reliability of the system will be assessed by cases.

4.3.5 Expected impacts

Theory, practice and utilisation of software dependability are not so familiar to software community than is, for example, software quality. The methodological framework of the TRUST will be a great support for an organisation in selection of specific knowledge (methods, techniques and skills) to design and demonstrate safety, reliability and security of software.

SP 1. Safety Culture

With the help of the method, the integration of the different expertise related to software development process will become easier, resulting to better design solutions. The experts' awareness of the significance of their own ways of acting to the dependability of the end product will be increased. The mutual understanding between the different parties will be enhanced and the communication will be improved. The software failures will be reduced and the effectiveness of the activity will increase. The developed concept is applicable to all kinds of expert co-operation in software production. Companies have identified the communication problems and are interested in improving expert communication.

SP 2. Managing Software Requirements

Expected impacts for manufacturers of programmable medical devices:

- systematic and cost efficiency design process
- better documentation throughout software engineering process
- better verification and validation activities during software development
- better software maintenance and management of modification
- effective and traceability system requirement phase
- less inadequate or inappropriate software requirements.

SP 4. Qualification of Dedicated Systems Software

Dedicated devices and systems with embedded software are used in several more or less critical fields (for example, smart sensors and transmitters in nuclear plants and conventional industry, users of mobiles, medical device community). The results of the subproject will support manufacturers and purchasers of these dedicated devices in their effort of qualifying software safety and reliability.

4.4 Risk assessment of genetically modified plants (GMORA)

Antti Alavuotunki

4.4.1 Introduction

The aim in the development work was to create the framework for the risk assessment of genetically modified plants (GMP) that helps the plant developer manage the risks during plant's development cycle. The other aim was to improve the ecological risk assessment process.

The project was joined to the theme one year only. The results achieved were the risk assessment method and guidance notes for the GMP's early development stage. The development work has been continued in other projects.

4.4.2 Background of the project

The effects that might occur through the use of genetically modified organisms can actualise directly but also through indirect ecological processes. Often the potential effects are difficult to determine since there is no earlier operational experience on the use of organisms.

Current tools to assess the GMOs risks are based on regulatory lists and they are not designed to concern risk management aspects. This project did apply risk assessment methods and theoretical framework widely used in process industry to the field of plant gene technology.

4.4.3 Objectives

The overall objective was to develop a framework for the risk assessment of genetically modified plants (GMP) that helps the plant developer to manage the risks during plant's development cycle. This included the development of risk assessment tools for different stages of the GMP's development cycle and for the ecological risk assessment.

During the first year the objectives were:

- Development of risk analysis methods for the contained use of genetically modified plants. Development included method testing with case studies.

- Study the plant development process and the needs that it poses for the risk assessments.

4.4.4 Main results

In the project new hazard identification and risk assessment methods for GMP's contained use were developed. These methods has been further developed in later projects.

4.4.5 Expected impacts

Published Guidance notes require performing the risk assessment for the use of genetically modified plants in contained environment. The paper is recommended and delivered by the Finnish board of gene technology.

The results and "know-how" gained during the project has been employed in later projects like in the current Academy funded research project "Assessment and

Regulation of Ecological Effects of GMOs in Boreal Environment". The aim is to produce "standardised" procedures for the industry and regulative authorities.

The industry is interested in comprehensive risk assessment so that it can better manage the risks the new technology might pose. However negative public acceptance of GMOs has frozen the research and commercialisation activities in the Europe.

4.4.6 List of publications

List of publications

Alavuotunki, A., Koivisto, R., Kauppinen, V., Törmäkangas, K. & Wessberg, N. (2002) Prosessiteollisuuden käytännöistä hyötyä geenitekniikalla muunnettujen kasvien riskinarvioinnissa (Practices of Chemical industry benefit risk assessment of genetically modified plants). Kemia-Kemi, Vol. 29, No. 2, pp. 35–37.

Bulletin: http://www.tiedetoimittaja.com/sivut/riskinarviointi.html

Ohje GM-kasvien suljetun käytön riskinarviointiin (Guide for risk assessment of GM-plants in contained environment). Published in the www-pages of the Board for Gene Technology. Available in: http://www.geenitekniikanlautakunta.fi/lomake/kasviriskarv.rtf

List of media references

Raunio, H. Prosessiteollisuuden riskianalyysit soveltuvat biotekniikkaan (Risk analyses of process industry are applicable in biotechnology). Tekniikka ja Talous 17.4.2003. Available in:
http://www.tekniikkatalous.fi/doc.do?f_id=456600 &
http://www.tekniikkatalous.fi/doc.ot?d_id=80664

Published by

Series title, number and
report code of publication

VTT Research Notes 2270
VTT–TIED–2270

Author(s)
Rouhiainen, Veikko (ed.)

Title

Safety and Reliability
Technology Theme, description of the programme

Abstract

"Safety and Reliability" is one of the four strategic Technology Themes of VTT. In this theme, technologies, system models, and measurement, modelling and estimation methods are developed for the Finnish industry's needs. The results are applied to the development of safety and the life-cycle management of socio-technical systems. Under the theme, the know-how encompasses the fields of safety engineering, risk management, system engineering, machine diagnostics and monitoring, psychology, microbiology and management of safety and dependability knowledge.

The research in the theme will be focused on

- methods for life cycle management
- Human-Technology Interaction (HTI) and safety
- new technologies and operating principles.

The evaluation of the Technology Themes was carried out in 2004. For this, each project developed a status report describing the research carried out and results achieved. This report compiles the reports developed for the evaluation in the projects of the Safety and Reliability -Technology Theme.

Keywords
safety, reliability, dependability, risk analysis, diagnostics, monitoring

Activity unit
VTT Industrial Systems, Tekniikankatu 1, P.O. Box 1306, FIN–33101 TAMPERE, Finland

ISBN			Project number
951–38–6513–4 (soft back ed.) 951–38–6514–2 (URL: http://www.vtt.fi/inf/pdf/)			G2SU00035
Date December 2004	Language English	Pages 79 p.	Price B
Name of project Technology Themes of VTT, Safety and Reliability		Commissioned by VTT	
Series title and ISSN VTT Tiedotteita – Research Notes 1235–0605 (soft back edition) 1455–0865 (URL: http://www.vtt.fi/inf/pdf/)		Sold by VTT Information Service P.O. Box 2000, FIN–02044 VTT, Finland Phone internat. +358 20 722 4404 Fax +358 20 722 4374	

Strategic technology themes of VTT combine VTT's research units and competence in technically and technologically challenging way. The aim is to reach international top quality results by networking with best possible partners and synergetic co-operation.

Safety and reliability is one of the four themes. It places greater emphasis on safety and reliability in order to identify and reduce risks and to ensure continuous operations without disruptions.

In the safety and reliability theme, technologies, system models, and measurement, modelling and estimation methods are developed for the Finnish industry's needs. The results are applied to the development of safety and the lifecycle management of socio-technical systems.

The know-how encompassed under the theme includes the fields of safety engineering, risk management, system engineering, machine diagnostics and monitoring, psychology, microbiology and management of safety and dependability knowledge.

Tätä julkaisua myy
VTT TIETOPALVELU
PL 2000
02044 VTT
Puh. 020 722 4404
Faksi 020 722 4374

Denna publikation säljs av
VTT INFORMATIONSTJÄNST
PB 2000
02044 VTT
Tel. 020 722 4404
Fax 020 722 4374

This publication is available from
VTT INFORMATION SERVICE
P.O.Box 2000
FIN–02044 VTT, Finland
Phone internat. + 358 20 722 4404
Fax + 358 20 722 4374

ISBN 951–38–6513–4 (soft back ed.)
ISSN 1235–0605 (soft back ed.)

ISBN 951–38–6514–2 (URL: http://www.vtt.fi/inf/pdf/)
ISSN 1455–0865 (URL: http://www.vtt.fi/inf/pdf/)