422

VTT PUBLICATIONS

Pekka Pyy

Human reliability analysis methods for probabilistic safety assessment

TECHNICAL RESEARCH CENTRE OF FINLAND ESPOO 2000

VTT PUBLICATIONS 422

Human reliability analysis methods for probabilistic safety assessment

Pekka Pyy

VTT Automation

Dissertation for the degree of Doctor of Technology to be presented with due permission for public examination and debate in Auditorium 1381 at Lappeenranta University of Technology, Finland, on the 7th of December, at 12 o'clock noon.

TECHNICAL RESEARCH CENTRE OF FINLAND
ESPOO 2000

ISBN 951–38–5585–6 (soft back ed.)
ISSN 1235–0621 (soft back ed.)

ISBN 951–38–5586–4 (URL: http://www.inf.vtt.fi/pdf/)
ISSN 1455–0849 (URL: http://www.inf.vtt.fi/pdf/)

JULKAISIJA – UTGIVARE – PUBLISHER

Valtion teknillinen tutkimuskeskus (VTT), Vuorimiehentie 5, PL 2000, 02044 VTT
puh. vaihde (09) 4561, faksi 456 4374

Statens tekniska forskningscentral (VTT), Bergsmansvägen 5, PB 2000, 02044 VTT
tel. växel (09) 4561, fax 456 4374

Technical Research Centre of Finland (VTT), Vuorimiehentie 5, P.O.Box 2000, FIN–02044 VTT, Finland
phone internat. + 358 9 4561, fax + 358 9 456 4374

VTT Automaatio, Teollisuusautomaatio, Tekniikantie 12, PL 1301, 02044 VTT
puh. vaihde (09) 4561, faksi (09) 456 6752

VTT Automation, Industriautomation, Teknikvägen 12, PB 1301, 02044 VTT
tel. växel (09) 4561, fax (09) 456 6752

VTT Automation, Industrial Automation, Tekniikantie 12, P.O.Box 1301, FIN–02044 VTT, Finland
phone internat. + 358 9 4561, fax + 358 9 456 6752

Technical editing Leena Ukskoski

Otamedia Oy, Espoo 2000

Pyy, Pekka. Human reliability analysis methods for probabilistic safety assessment. Espoo 2000. Technical Research Centre of Finland, VTT Publications 422. 63 p. + app. 64 p.

Keywords human reliability analysis, HRA, probabilistic safety assessment, human factors, decision making, expert judgement, simulator studies

ABSTRACT

Human reliability analysis (HRA) of a probabilistic safety assessment (PSA) includes identifying human actions from safety point of view, modelling the most important of them in PSA models, and assessing their probabilities. As manifested by many incidents and studies, human actions may have both positive and negative effect on safety and economy. Human reliability analysis is one of the areas of probabilistic safety assessment (PSA) that has direct applications outside the nuclear industry.

The thesis focuses upon developments in human reliability analysis methods and data. The aim is to support PSA by extending the applicability of HRA. The thesis consists of six publications and a summary. The summary includes general considerations and a discussion about human actions in the nuclear power plant (NPP) environment. A condensed discussion about the results of the attached publications is then given, including new development in methods and data. At the end of the summary part, the contribution of the publications to good practice in HRA is presented.

In the publications, studies based on the collection of data on maintenance-related failures, simulator runs and expert judgement are presented in order to extend the human reliability analysis database. Furthermore, methodological frameworks are presented to perform a comprehensive HRA, including shutdown conditions, to study reliability of decision making, and to study the effects of wrong human actions. In the last publication, an interdisciplinary approach to analysing human decision making is presented. The publications also include practical applications of the presented methodological frameworks.

PREFACE

This work has been motivated by both theoretical and practical studies on human reliability assessment carried out at VTT (Technical Research Centre of Finland) Automation through the years 1994–2000. The studies have mostly been a part of the research projects LURI (Reliability and Risk Analyses) and METRI (Methods for Risk Assessment) of which the author has been the project leader. The projects belong to the research programmes RETU 1995–1998 (Reactor Safety Research Programme) and FINNUS 1999–2002 (Finnish Nuclear Safety Research Programme). Furthermore, participation in both development and application of methods, in a co-operation with the Finnish power companies Teollisuuden Voima (TVO) and FORTUM, has significantly contributed to this thesis.

The work has been supervised by Professor Heikki Kalli from the Lappeenranta University of Technology. I am grateful to him for his support and advice, which has helped me greatly in finalising the project. Many valuable comments were also received from the reviewers of this work, Docent Jussi Vaurio from FORTUM and Dr. Tech. Lasse Reiman from STUK. Their comments were especially helpful in enabling me to consider the thesis in the light of other developments and the current status in the area.

Prof. Urho Pulkkinen from VTT Automation has been a great help and support during the preparation of the thesis. Without his constructive criticism the result would have definitely been inferior. Therefore, I wish to express my deepest gratitude. There are many other people who have helped me with their comments in the course of this work, and I am aware that it was an extra duty for them. Therefore, colleagues and friends, I wish to thank you all for your help.

I am much obliged to the financial support received from the Imatran Voima Foundation and from VTT Automation for making it possible to finalise the thesis. Finally, I wish to express my warm gratitude to my wife Eva and to my children Christa and Petra for their understanding – and I am aware of the fact that they have needed a great deal of it during some hectic phases of the endeavour. Now it is done dear PirTU and other people – and the life goes on!

LIST OF PUBLICATIONS

The publication numbering corresponds to the order in which they are discussed in the text.

[I] Pyy, P. 2000. An analysis of human maintenance failures of a nuclear power plant. To appear as a revised version in: *Reliability Engineering and System Safety*. Published in *Lappeenranta University of Technology, Department of Energy Technology*, EN A-50 (2000). 12 p. + app. 1 p.

The paper discusses maintenance-related human actions that have contributed to faults in a nuclear power plant, based on a database that has been collected in another study. The author's share, which is reported in this paper, was to reanalyse the data and to make statistical inferences about the roles of different kinds of faults caused by human actions.

[II] Pyy, P. & Himanen, R. 1996. A praxis oriented approach for plant specific human reliability analysis – Finnish experience from Olkiluoto NPP. In: Cacciabue, P. C. & Papazoglou, I. A. (eds.). *Proceedings of Probalitistic Safety Assessment and Management'96. ESREL'96 – PSAM III Conference*. Vol. 2. Crete, Greece, June 24–26, 1996. Great britain: Springer Verlag. Pp. 882–887.

The paper presents a method for including the influence of human actions in a probabilistic safety analysis of a nuclear power plant. It includes both a theoretical framework and an application. The author developed most of the methodology, participated in its application and wrote a major part of the paper.

[III] Pyy, P. & Jacobsson, P. 1998. Human reliability assessment by using an expert judgement methodology. In: Lydersen, S., Hansen, G. K. & Sandtorv, H. A. (eds.). *Safety and Reliability, Proceedings of ESREL '98 European Conference*, Trondheim, Norway, 16–19 June, 1998. Rotterdam: Balkema Publishers. Pp. 775–782.

The paper discusses an application of expert judgement methodology developed earlier by VTT Automation for the HRA of a shutdown situation. The author's role in the paper was to apply the methodology, carry out the direct combining of judgements, define the variables for expert judgement, and to participate in the expert judgement procedure as a normative expert. The author was responsible for writing the paper.

[IV] Pyy, P. 2000. An approach for assessing human decision reliability. In: *Reliability Engineering and System Safety*, Volume 68, Issue 1, pp. 17–28.

This paper discusses a methodology for analysing operator crew decision making and its role in a safety significant disturbance. The paper shows an application and discusses the traits of the methodology. The author developed the method and carried out the application.

[V] Pyy, P. 1999. A framework for analysing human commission errors – FACE. In: Schuëller, G. I. & Kafka, P. *Safety and Reliability, Proceedings of ESREL '99 European Conference*, Garching, Germany, 13–15 September, 1999. Rotterdam: Balkema Publishers. Pp. 669–674.

The paper presents an HRA methodology developed especially to analyse wrong human actions and, more generally, the aggravating effects of human actions. The method is applicable to all kinds of failures in human actions. The author developed the methodology.

[VI] Holmberg. J., Hukki, J., Norros, L., Pulkkinen, U. & Pyy, P. 1999. An integrated approach to human reliability analysis – decision analytic dynamic reliability model. *Reliability Engineering and System Safety, Vol.* 65, pp. 239–250.

The paper presents a methodology for performing an interdisciplinary analysis of human reliability with an application. The author's particular role was to develop an integrated approach as a part of the team, to model contextual factors and their contribution to human reliability, to develop models, and to lead the analysis team. The author actively participated in writing the paper.

LIST OF ABBREVIATIONS

BWR – boiling water reactor

CO – commission opportunity (opportunity for a wrong human action and/or for a wrong system function due to human action)

EoC – error of commission (wrong human action)

EoO – error of omission (missing human action)

HCR – human cognitive reliability

HEP – human error probability

HFE – human failure event

HRA – human reliability analysis

IE – initiating event

LOCA – loss of coolant accident

NPP – nuclear power plant

OAT – operator action tree

PWR – pressurised water reactor

PSA – probabilistic safety assessment (level 1 PSA studies accident sequences leading to severe core damage, level 2 PSA studies phenomena leading to containment failure and level 3 PSA studies risk to the public)

PSF – performance shaping factor, factors affecting probability of human actions (also PICs, performance and probability influencing factors, is used in Paper [V])

SHARP – systematic human action reliability procedure

SLIM – success likelihood index method

TRC – time reliability correlation

THERP – technique for human error rate prediction

DEFINITIONS

Critical failure, a failure that is assessed to result in unacceptable consequences such as unavailability or wrong function leading to personal or property damage – modified from ESReDA (1999) and IEC (1990).

Diagnosis, identification and interpretation of the state of equipment or process so that a decision may be made (modified from ASME, 2000). A diagnosis may be general (defining the condition of equipment or of a system) or detailed (defining the cause for the condition).

Human (primary) action, an action through which man is in direct interface with a process or with equipment. Secondary human actions, such as planning, procedure writing, training, etc. assist and prepare primary actions. When secondary actions are discussed, this is always indicated separately.

Human error, failure of a human action due to internal human failure mechanisms (for consequences, see *Critical failure*). Used in literature, e.g. ASME (2000), to loosely describe any sub-optimal human performance.

Human failure (event), failure of a defined human action in an HRA model (modified from ASME, 2000). There may be many reasons for failure (compare to human error). A human failure affects components (faults) and processes (disturbances). If the effect is significant (critical), a recovery or repair has to take place.

Fault, the state of an item as characterised by its inability to perform a required function, excluding inability during preventive maintenance or other planned actions, or due to lack of external resources – ESReDA (1999), IEC (1990).

Failure, the termination of the ability of an entity to perform a required function – ESReDA (1999), IEC (1990). Note: 1) after a failure, the entity is faulty and 2) failure is an event as distinct from a fault, which is a state.

Recovery, the change of state of equipment (from fault) or process (from disturbance) so that safety or availability are again secured. Both technical equipment and human actions may be recovered. Recovery can be handled by the operating personnel as distinction from repair, which deviates from the definition of ASME (2000).

Repair, as distinct from recovery, the part of corrective maintenance in which manual actions are performed on an item – modified from ESReDA (1999), IEC (1990). Normally repair includes fixing a fault, whereas recovery can be carried out by simply restoring a function. Repair is carried out by specialised maintenance organisations.

CONTENTS

Appendices of this publication are not included in the PDF version. Please order the printed version to get the complete publication (http://otatrip.hut.fi/vtt/jure/index.html)

1. INTRODUCTION

Human actions are an essential part of the operation and maintenance of a nuclear power plant (NPP), both in normal and abnormal conditions. Generally, man can ensure a safe and economic operation by proactive means, but in disturbances a reactive performance may also be required. Thus, human actions affect both the probability of risk significant events and their consequences; and these are studied in a probabilistic safety assessment, PSA. Hirschberg (1990) has reported the contribution of human actions to PSA results to be as high as 88%. On the other hand, the role of human action may be insignificant in new passive reactors (e.g. Schmalz, 1999). The differences are partly due to different designs, but also due to differences in methods, assumptions, definitions and analysis practices.

The accidents at TMI in 1979, Chernobyl in 1986 and Tokai Mura in 1999, in which man played a significant role, have brought additional information about the importance of human reliability. In the process industries, human actions are also found to be significant contributors to accidents (Bello & Colombari, 1980 and Drogaris, 1993). Among the accidents where human actions have played a major role in the process industries and transport, have been the Flixborough explosion (1974), the Teneriffe airport accident (1977) and the capsizing of the Herald of Free Enterprise (1987).

Swain & Guttmann (1983) define human reliability as follows: human reliability means the probability that a person (1) correctly performs an action required by the system in a required time and (2) that he does not perform any extraneous activity that can degrade the system. There are other qualitative definitions, for instance in Hacker (1998), related to the human ability to adapt to changing conditions in disturbances. The HRA discussed in this thesis aims to support PSA, and, consequently, the probabilistic definition is more appropriate. In some cases, HRA may be extended to include an analysis of correct and scheduled human actions that have negative availability influence. This is due to the importance of modelling co-ordinated maintenance actions, such as maintenance umbrella packages in outages, in the PSA model in a structured way.

Any method by which human reliability is assessed may be called a human reliability analysis (Swain, 1990). The analysis typically includes the following phases: (1) identification of human actions, (2) modelling of important actions and (3) assessment of probabilities of human actions. The identification and modelling of important human actions from the PSA point of view takes place most often as part of systems analysis and accident sequence modelling, as demonstrated, for example, in IAEA (1992).

HRA concentrates on human actions that are important to reactor safety. They are:

1) Actions causing system disturbances, i.e. PSA initiating events (IEs)
2) Actions causing latent failures in safety-related systems, e.g., imperfect maintenance
3) Actions taking place during the management of disturbances, i.e. balancing actions after an IE.

Human actions can have both positive and negative impacts on safety. Factors such as ergonomics and organisation often appear as performance shaping factor (PSF) influences embedded in the HRA models. The modelling phase is followed by probability quantification. It often forms an integral part of the HRA.

The concept human error probability (HEP) is often used in a HRA context. Assessing HEPs is difficult, and is related to two concepts: human error and probability. The theory of probability is discussed, for instance, by Savage (1972). Human error is widely discussed in psychology literature, e.g. by Reason (1990), Woods et al. (1988) and Hollnagel & Marsden (1996). In this thesis, instead of using the term human error, the concept of a human failure event (HFE) is applied (e.g. see Hirschberg & Dang, 1998 and ASME, 2000). The reason is that the word ‘error’ is too restrictive and, in some cases, may be regarded as referring to internal human error mechanisms (e.g. Hollnagel 1998, Bieder et al. 1998). In reality, human actions modelled in PSA have a mission under the conditions of contextual factors: a certain history, tools, resources and environment. HFE corresponds better to the definition used in this thesis for human reliability and the basic events in a PSA model (ASME, 2000).

The thesis consists of five summary sections, 1–5, and the six published papers, which are enclosed as Appendices I–VI. The general objective of this thesis is to present new HRA methods and uses of data for PSA studies.

The development of different main streams of HRA is discussed in Section 2, and the approaches in the papers in this thesis are compared to them. Types of different human actions that take place at NPPs are presented in the same section. Papers [I] and [II] are closely related to Section 2. Paper [I] discusses how plant-specific maintenance data are and should be used to discover new information about faults induced by human actions. Paper [II] illustrates the development of a comprehensive HRA methodology and its application to a full scope PSA study, including a shutdown analysis.

Advances made in human reliability methods and data are discussed in Section 3. Papers [III]–[V] are closely related to Section 3. Paper [III] illustrates a developed expert judgement methodology and its use in producing relevant information for a HRA of shutdown conditions. Paper [IV] presents a method for explicitly including decision making in a HRA, and, thus, to improve the validity of analyses of diagnosis and decision making in disturbances. These papers also illustrate developments in using simulator data and expert judgement in HRAs. Paper [V] describes a methodology for identifying and quantifying wrong human actions and wrong system functions due to human actions in the PSA framework.

Section 3 ends with a discussion on interdisciplinary analyses of human reliability. Paper [VI] presents a detailed methodological framework for performing such an HRA, together with an application. Finally, in Sections 4 and 5 the conclusions of the papers are presented in a condensed form and concluding remarks are made summarising the most important findings of the thesis.

2. HUMAN RELIABILITY ANALYSIS AND HUMAN ACTIONS IN NUCLEAR POWER PLANTS

2.1 Development of HRA

Human reliability analysis is a fairly new interdisciplinary research area. The Second World War led to a considerable acceleration in the technical development of military equipment, which resulted in control problems. The consequence of this development was a need to study ergonomics, reliability, operability and maintainability. The first probabilistic human reliability study was carried out in 1952 for a weapon system feasibility in Sandia National Laboratories, USA (Swain, 1990). The probability of each unsuccessful action was assumed to be 0.01 or 0.02, depending on whether the action had to be performed on the ground or in the air.

Military HRA was transferred to civil applications for man machine system design in the 1960s. An example of HRA advances from that time is the study "*An Index of Electronic Equipment Operability*" by American Institutes for Research (AIR). In the study, human performance was decomposed into isolated sub-actions and the total human failure probability was obtained by combining the individual probabilities. The failure probabilities of the sub-actions formed the AIR Data Store, described, for example, in Topmiller et al. (1982). The first version of THERP, *Technique for Human Error Rate Prediction*, was presented in the early 1960s (Swain, 1963). It combines dependencies, recoveries and situational factors with the decomposition approach and is still widely used in HRA. Modern human factor studies also began in the 1960s including drill training, operating procedures, ergonomics and design guidelines for power plant control rooms.

Development of the HRA was related to an increased use of probabilistic safety and availability analysis methods. The first probabilistic study for NPP siting was presented in the 1960s (Farmer, 1967). In the mid 1970s, a large probabilistic safety assessment, including a THERP-based human reliability analysis, WASH-1400, was published (NRC, 1975). Many different HRA approaches started to evolve after WASH-1400. Time reliability correlations were developed to determine the time-dependent probabilities of post-initiating event actions such as diagnosis (Hall et al. 1982, Hannaman et al. 1984, Swain & Guttmann 1983). At the same time, models to calculate the dependence of HEPs on combinations of various performance shaping factors (PSFs) were developed, as presented e.g. by Embrey et al. (1984), Philips et al. (1987), Bello & Colombari (1980) and Williams (1988).

The HRA models presented above represent holistic approaches, i.e. the details of human behaviour mechanisms are not modelled. In parallel, detailed approaches were developed to explain human internal information flow and thinking processes. The most widely used is evidently the step-ladder model and the related skill, rule, knowledge (SRK) concept by Rasmussen (e.g. 1979). The model was not originally intended for probabilistic usage, but other authors like Hannaman et al. (1984) adopted its principles to HRA.

2.2 Approaches and trends in HRA

HRA methods can be classified according to 1) detail level of modelling, 2) treatment of diagnosis/decision making and cognitive mechanisms, 3) treatment of time dependence, 4) treatment of contextual factors, and 5) the data used. Figure 1 depicts how some most generally used HRA methods and Papers [I]–[VI] of this thesis relate to the classes. Different HRA methods have been presented more extensively, e.g. in references Fullwood & Hall (1988), Humphreys (1988), Hirschberg & Dang (1998) and Hollnagel (1998).

The detail level of modelling may be used to classify HRA methods into holistic, such as expert judgement approaches discussed in Comer et al. (1984) and in Paper [III], and into decomposition ones, presented, for instance, by Swain (1987) and Cooper et al. (1996). The former aims at assessing human actions as a whole, whereas the latter aims at dividing the actions into small sub-actions. Between the extremes, there are interim levels of detail, such as the OAT division into detection, diagnosis and manual actions (e.g. Hall et al., 1982). The reason for different decomposition levels is sometimes related to data and sometimes to risk management. Data may be either available on human actions as a whole or about different decomposed sub-actions. Risk management also has connections to the modelling level since by more decomposed and refined modelling it is easier to find possibilities of reducing hazards. However, it may be impossible to collect data and include all dependencies if the model detail level is too high. There is also evidence that too decomposed modelling may lead to optimistic probabilistic results due, for example, to the fact that not all the dependencies were taken into account (Poucet, 1988).

There is a distinct difference between the HRA methods that are developed to assess the effect of human actions on systems reliability and those developed to explain human internal failure mechanisms, i.e. cognitive models. Black box models of human behaviour are often used for the former purpose. An example of one of them is Paper [III] that directly expresses the operator crew failure probability as a function of time. Other important lines of modelling are confusion matrices, discussed, for instance, in Potash et al. (1981), Oconee (1984) and Illman et al. (1986), and decision models discussed in Paper [IV]. These models aim to present different identification and decision alternatives and their effect on plant safety rather than to model detailed behavioural mechanisms. As a contrast, Cacciabue (1992) and Hollnagel (1998) discuss cognitive models. Moreover, Cacciabue (1998), Dang (1996) and Hollnagel (1995), among others, present man machine system simulation models. Cognitive models do not directly belong to the scope of this thesis, but to some extent human goals and alternatives are discussed in the probabilistic modelling of decision making in Papers [IV] and [VI]. Holistic and black box modelling approaches are inherently coupled, whereas cognitive models are one main stream of decomposed HRA modelling approaches.

Time dependence is one point of view that may be used to classify probabilistic HRA models. Time independent models are well suited to human actions before an initiating event (IE), since the available time is not normally among the most important contributors to the success of maintenance and testing actions. The THERP HRA tree (Swain & Guttmann, 1983), and models for human actions before an initiating event, discussed in Papers [II] and [V], are examples of time independent models. TRC (time reliability correlation) type models are best suited to actions after an IE, especially when the available time is short. TRC models were mostly developed in the 1980s. Some examples are OAT (Hall et al., 1982), Swain's ASEP-TRC (Swain & Guttmann 1983, Swain 1987), ORE (Moieni et al., 1989), HCR (Hannaman et al., 1984) and models in Papers [III] and [VI]. Another possibility apart from TRC for modelling time dependence is to treat time as one PSF among others, as presented, for example, in SLIM-MAUD (Embrey et al., 1984) and Paper [V].

Performance shaping factors (PSFs) represent the effect of contextual factors on the probability of human failure. The number and type of PSFs in various methods vary significantly, as, for example, Hollnagel (1998) and Kim & Jung (1999) discuss. Examples of PSFs are working conditions, stress level, feedback from process/MMI, availability and quality of procedures, time, training and experience. All generally used HRA methods take into account the effect of, at least, some PSFs. At the extremes, HCR model (Hannaman et al., 1984) only uses a few PSFs whereas the approaches in Papers [V] and [VI] intend to cover all potential influence sources. PSFs are modelled in HRA either implicitly, e.g. holistic expert judgement modelling in Paper [III], or explicitly, e.g. in SLIM (Embrey et al., 1984), ATHEANA (Cooper et al., 1996) and Paper [VI].

The applicability of PSFs is also related to HRA data. Data are required to estimate the HRA model parameters. Either generic human reliability data are used directly in estimation, and updated to represent the plant conditions by using PSFs, or plant specific data is directly utilised. For example, the data set of Swain & Guttmann (1983) may be referred as generic due to its multiple sources. Plant-specific data may be based on simulator experience, on expert judgement or on operating experience. Operating experience data is often very sparse. This is due to the delicate nature of HFEs, difficulty in classifying data generally and the fact that the collection effort has been rather small. Papers [I] and [II] discuss plant-specific maintenance data collection and application. Expert judgement and simulator runs are an important HRA data source. Papers [IV] and [VI] show how simulator tests may be used to estimate TRC parameters. Expert judgement may be utilised in directly assessing HFE probabilities, as discussed, e.g. in Paper [III], or in assessing PSFs and their contribution, as shown, for example, in Paper [V].

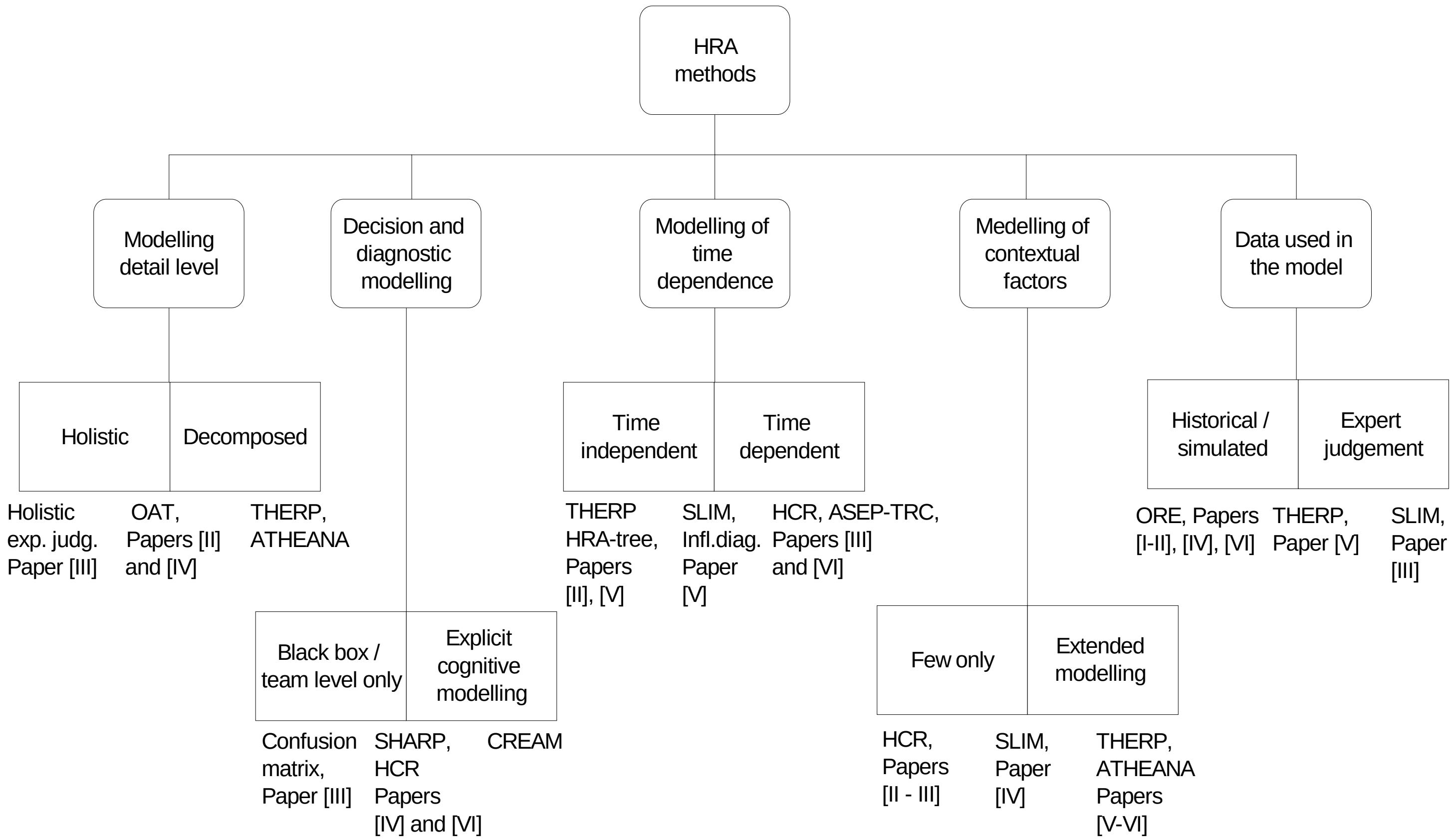

Figure 1. Classification of HRA methods. References are made to some of the most generally used methods and to Papers [I]–[VI].

Lately, the concept of second generation HRA has appeared in international HRA discussions (Hollnagel, 1996 and 1998, Ramey-Smith, 1998 and Bley et al., 1998). Methods like ATHEANA (Cooper et al., 1996), MERMOS (Bieder et al., 1998), CAHR (Sträter, 1996) and CREAM (Hollnagel, 1998) have been developed to improve weak points in earlier methods. There is not a common definition of the meaning of second generation HRA, but all the methods mentioned seek to extend the applicability of HRA. One line of development is the use of so called cognitive methods, represented by CREAM. They have been criticised, e.g. by Dougherty (1997), since they try to model causal mechanisms of phenomena that include a considerable amount of randomness. Another line, represented by MERMOS and ATHEANA, is to model the contextual factors in an extensive way. This approach may be completed by taking into account different forms of evidence about the reliability performance of man-machine systems. It may be called a systems and data-oriented approach, and is systematically followed in the papers in this thesis.

2.3 Human actions in PSA

The spectrum of human actions at an operating NPP is wide. Man takes care of the operation, maintenance, modifications and testing in various parts of the installation. These are primary activities, where man is in direct touch with the process and equipment, whereas there also are planning, design, supervision and other secondary support activities. Furthermore, human activities may be classified according to their position in PSA models and to the plant operating mode in which they take place, as discussed in the following sections.

HRA has the role of performing the transformation of human actions into PSA model events. The generic principle is that only important human actions are explicitly included in a PSA in order to decrease the modelling complexity. Examples of such actions are necessary post-IE operator actions, and unplanned system unavailability induced by testing or maintenance. Effects of other human actions are implicitly taken into account, e.g. as part of component failure data and initiating event frequencies. Post-IE operating actions, such as the human back-up start of a pump in a situation where the automatic signal has failed, and accident management affect PSA results in a positive way. Generally, other modelled human actions have a negative impact on safety.

2.3.1 Maintenance and operating activities

Operating activities are carried out by plant operating organisation. They include supervision, control and adjustment, and balancing disturbances. Many operating activities take place in the main control room. However, there are a great number of operating activities that are carried out outside the control room. Examples of these are tests, manual controls, system separations and restorations, and recoveries of failed automated systems in switch gear units or instrument cubicles. The safety significance of activities outside the control room has been recognised, e.g. by Swain & Guttmann (1983) and Fullwood & Hall (1988), and their role has lately been emphasised, e.g. by IAEA (1998).

Maintenance activities include preventive maintenance, i.e. scheduled tasks, and corrective maintenance, i.e. repairing faults. Tests and inspections are an important part of preventive activities, carried out either by the operating or the maintenance organisation. Maintenance activities take place in the repair shop and all over the installation. Maintenance related human activities are discussed extensively in Paper [I].

Paper [II] discusses the human activities that are included in a PSA and presents systematic principles to calculate unavailability due to scheduled activities and HFEs. Actions included are scheduled maintenance tasks and tests, repair of non-critical faults, deficiencies in equipment restoration, maintenance and test induced dependent faults, human activities as initiating events, and various balancing operating actions during disturbances. Recently, accident management has also been included in level 2 PSA studies, as discussed, for instance, in Jae & Apostolakis (1992), Kim & Jung (1999) and Pyy (1999).

2.3.2 Primary and secondary human activities

Human actions that have a potential to affect the process stability or availability of technical systems may be called primary or front line actions. Maintenance, operating acts and tests are primary activities, and they may be explicitly modelled in PSA. Examples of secondary activities include training, quality control, quality assurance, work planning, supervision, inspections, analysis and preparing various plant documents. The effect of secondary activities, often called organisational influences, may be taken into account in HRA by using performance shaping factors (PSFs), as discussed in Papers [II] and [V]. In some cases, the influence of secondary actions may be important. For example, deficiencies in training may increase the probability of human failure in critical situations.

Human operating activities may also be classified according to their role in system actuation. If there are no automated signals, human actuation is necessary, for example, to start a pump. In the case of existing automatic signals, human action can be regarded as a backup. Due to the rather high reliability of automated protection signals, human back-up actions have normally a smaller significance in PSA than the purely manual ones. The role of human actions is dependent on the design of the installation.

A special class of primary activities is recovery. Human balancing actions after an IE can be broadly interpreted as a recovery of a process disturbance. Man can also recover his own or others' failures and, in some cases, even system faults. Recovery is possible given that time, resources, tools and required knowledge are available. Only HFEs that are not recovered in the available time are significant from the PSA point of view, as discussed in the papers in this thesis.

2.3.3 Human action position in a PSA model

The Loviisa NPP HRA (Illmann et al., 1986), and IAEA guidelines for a level 1 PSA (IAEA, 1992) classify human performance into activities before a PSA initiating event (IE), activities as an IE, and post IE actions. This division is well suited to PSA modelling framework, and it is utilised as a starting point in developments discussed in Paper [II]. The paper describes an HRA approach, where the objective was to allow the involvement of several plant personnel groups by using transparent modelling, verbal descriptions of human actions and links to plant practices as the basis for probabilistic parameters.

As discussed in Paper [II], actions before an initiating event include typically scheduled maintenance, tests, deviations in equipment restoration and human induced dependencies. The unavailability due to repair of non-critical faults should be explicitly included in the PSA model if it turns out to be important. The unavailability due to critical faults is generally included in the fault data.

Paper [II] also describes how the human activities causing initiating events are mostly taken into account as contributing to IE frequency. Frequency of rare IEs, for which there is little or no operating experience, may be assessed based on 1) a thorough qualitative analysis, 2) decomposed structural modelling, e.g. a fault tree and 3) a systematic HRA quantification.

The post-IE human activities in Paper [II] include various actions that balance the plant state or mitigate the course of an accident. Post-IE actions have been the main development area of HRA, and they are discussed extensively in Section 3 of this summary.

2.3.4 Human actions in different NPP operating modes

Paper [II] shows how human actions affect NPP safety in all plant operating modes. During power operation, supervisory operating activities and testing play a major role. The role of control activities becomes more important when an installation is being shut down or started up. A major part of maintenance, testing and modification actions takes place during outages. Restoration and operability verification of equipment is important after these activities, to ensure safe and economic operation.

PSA treatment of human actions in shutdown operating modes can basically follow the same principles as for power operation. However, shutdown is characterised by different contextual factors to power operation, as Pyy & Himanen (1993), Sträter & Zander (1998), Hirschberg & Dang (1998) Kattainen & Vaurio (1999) and IAEA (2000) describe. Generally, very few emergency operating procedures are available, automated actuation signals may be unavailable, and opportunities to rehearse the situation with a simulator are limited. Time windows for human action are often quite long, but there are exceptions like large leaks at the bottoms of boiling water reactors (BWRs). Restoration of inoperable systems may be easier than during power operation, due to good accessibility, if no early radiation level increase occurs. However, the system states and organisational set-ups in outages differ significantly from those in power operation. In addition, there are factors such as the high number of external subcontractors and the long working hours of the plant staff that may affect safety, both positively and negatively. These facts have to be taken into account in HRA for shutdown modes.

3. ADVANCES IN HRA METHODS AND DATA

3.1 Human reliability methods

Many HRA approaches created in the 1980s, such as HCR, OAT and SLIM, concentrate on human actions in the control room environment. The second generation approaches, listed in Section 2.2, have not greatly extended this emphasis domain. IAEA (1998) and Hirschberg & Dang (1998) list several key improvement areas in HRA. The items listed by IAEA are decision making, actions outside the control room, shutdown conditions, co-ordination and communication, and actions outside the procedures. Moreover, an important topic is the applicability of time reliability correlation to post initiating event HRA. These issues are discussed under different headlines in Sections 3.1.1–3.1.4.

3.1.1 Methods for evaluation of decision-making situations

Decision making is usually not explicitly included in human reliability analysis, since it is assumed that operators can cope with a disturbance by directly applying procedures after a diagnosis (Hall et al., 1982, Swain & Guttmann, 1983, Hannaman & Spurgin, 1984 and Embrey et al., 1984). This approach may be too simplistic, as, for example, Parry et al. (1996), Hukki & Norros (1998), Svenson (1998) and Dougherty (1998) discuss. Reiman (1994) concludes that operators strive to make a diagnosis and they feel stressed if they are not able to do so. In such cases, symptom-based emergency operating procedures (EOPs) should be used to guide operators.

Diagnosis is, in this thesis, interpreted as the identification and interpretation of a condition of the target system, process or equipment and it does not include decisions (see Figure 3). There are also situations where no diagnosis is possible and no good EOPs are available. In such cases people have to make decisions when uncertain, e.g. about possible measures to be taken and the ways information could be gathered. Thus, decision making deserves a position, especially in the HRA studies of post IE conditions and emergency situations. Decision making and decision theory have been widely studied in many scientific disciplines in the literature. For example, von Neumann & Morgenstern (1944), Keeney & Raiffa (1976) and French (1986) present maximum expected utility theory as forming the basis of a rational decision theory. Kahnemann & Tversky (1979) and von Winterfeldt & Edwards (1986), among others, have expanded the theory to descriptive psychological applications. Naturalistic decision research direction, discussed, for instance, by Orasanu & Connolly (1993) and Klein (1998), emphasises that decision making in real situations may not follow normative theories and that reality is very different from laboratory conditions.

Decision making is an important part of operator actions especially during severe disturbances and accidents. Paper [IV] presents a methodology to include it in HRA. The objective of the paper is to show that decision analytic methods are relevant to HRA. By combining human reliability modelling with knowledge about control room operations, and by utilising normative and descriptive decision theory, a comprehensive view on important factors affecting operator team decision making may be generated. The modelling approach presented in Paper [IV] is an extension of the prevailing HRA paradigm restricted to diagnosis and procedures only. A generic modelling approach is presented together with an application to a severe PWR disturbance case with two different decision situations.

In the first one, the decision is dominated by one criterion and, in the second one, there are multiple objectives. The paper suggests different probabilistic assessment for these two situations. In simple cases where 1) all the decision alternatives are more or less equally good with regard to the main goal of the activity, 2) they produce a similar process response, and 3) competing with time is important, a time reliability correlation is a feasible modelling method. Simulator tests described in Paper [IV] confirmed that the operators swap between decision alternatives until one of them works satisfactorily. This result has a direct implication in the HRA studies. Based on the goal to maintain or to restore a safety function, human reliability should be assessed on a safety function level rather than separately for each system. Time reliability correlation models are discussed further in Section 3.1.3 of this thesis.

In real multi-criteria decision situations, decision theory based HRA models should be applied. A time reliability correlation is not a valid model for such cases, and, in fact, a fast human action may be even seen as premature. Paper [IV] also shows that the values of critical process parameters do not directly affect the decision-making behaviour in such situations. Rather, the operator crews' orientations to the situation, and the way they weight different evidence become important. Finally, Paper [IV] presents a probabilistic quantification approach to the HRA of decision situations, discussed briefly in Section 3.2.2.

Table 1. Comparison of alternative operating methods in the form of a decision table edited from Paper [VI].

System: **Criteria:**	**Auxiliary feedwater system (AFWS)**	**Condensate system**	**Demineralized water and boron systems**	**Core spray system**	**AFWS from a spurious signal**
Safety					
Overpressure protection	Possibility of severe overpressure	Possibility of overpressure up to 28 bar	No overpressure risk	No overpressure risk	Possibility of severe overpressure
Economy					
Time schedule (one pump used)	40 min to +6.4 m level	Very fast, less than 5 minutes to +6.4 m (min)	Slow, from +6.4 m to 8.2 m over 2 h	Very fast, less than 10 minutes to +6.4 m (min)	X min
Purity of water	Acceptable	Acceptable	Acceptable	Not acceptable (from wet well)	Acceptable
Technical feasibility					
Availability	4 pumps	4 pumps, not available if urgent maintenance	2 pump lines	4 pumps	Not accounted
Pumping capacity	(4 x) 22.5 kg/s	(4 x) 250 kg/s max.	(2 x) 2.5 kg/s	(4 x) 125 kg /s	(n x) 22.5 kg/s
Operational culture					
Procedures, operating orders	Legitimate at the beginning	Legitimate at the beginning	Legitimate at the end	Not legitimate due to the water source	Not legitimate
Routines	Alternative to condensate system	Used, if available	Slow, not preferred	Not used	The pump has to be stopped

The time required to pump up to the +8.2 m level is dependent on the pumping method used. Large capacity pumps may be throttled for a smaller flow rate.

A similar decision theory approach to that in Paper [IV] has been used in Paper [VI] to characterise decisions in normal operating action as a part of reactor cool-down before a yearly refuelling outage. A decision table presenting the alternatives and the criteria put in practice by the operators is depicted in

Table 1. With the main goal being to fill the reactor tank, the operators will have to initiate pumping and choose one of the four pumping alternatives with their different features. The fifth alternative represents a spurious pump start, which is not a valid alternative from the operating environment point of view, but may happen. During filling, the operators must assess the water level, change the pumping method and, finally, stop pumping. The unwanted event in this action sequence is the overfilling of the reactor tank followed by a cold pressurisation. The integrated approach used to analyse the operators' decision making and to perform a HRA for the case is discussed further in Section 3.3.

3.1.2 Methods for analysis of commission opportunities

Many HRA studies concentrate on omissions of procedure-based human actions (EoOs). The need to complete PSAs with the analysis of wrong human actions, often called errors of commission (EoCs), has been identified, e.g. by Swain & Guttmann (1983), Vuorio & Vaurio (1987), IAEA (1992), Barriere et al. (1995), Parry et al. (1996), Dougherty (1990, 1998) and Hirschberg & Dang (1998). The reason for this need is that EoCs may lead to many different system responses and sometimes even aggravate a disturbance.

EoCs are defined in various ways in the literature. Swain & Guttmann (1983) define the error of commission as a wrong human output i.e. selection error, error of sequence, time error (too early, too late) or qualitative error (too little, too much). For example, Potash et al. (1981) and Illman et al. (1986) discuss confusion in identifying a disturbance resulting in wrong actions, and present a matrix approach to modelling them in HRAs. Reason (1990) uses the concepts of a) slips and lapses, i.e. unintentional acts, b) mistakes, i.e. mismatch between intention and the actual consequences and c) violations, where deviating from safe practices is intentional.

Furthermore, Parry (1995) discusses premature actions and separates them from alternate actions, of which there are many possibilities. Both Gertman et al. (1992) and Macwan & Mosleh (1994) distinguish between intentional and unintentional EoCs. The former are more related to diagnosis and decision making, whereas the latter are more related to task execution. ATHEANA classification in Barriere et al. (1995) makes a link to PSA by stating that an error of commission (EOC) is ‘an overt, unsafe action that, when taken, leads to a change in plant configuration with the consequence of a degraded plant state’. Julius et al. (1995) draw attention to the fact that many EoCs both lead to a failure in performing the primary function and, in addition, make unavailable safety related equipment or otherwise exacerbate the situation.

Dougherty (1998) and Hollnagel (1998) note that classifying human failure events as EoCs and EoOs may be useless if no deeper contextual analysis follows. For example, a wrong human action can lead to either an active or a passive system response, as discovered in Paper [I] when discussing maintenance-related human failure events. Active consequences are PSA initiating events or other spurious system functions that are normally monitored by plant personnel. Passive system response means component inoperability that is often latent. In the data used in Paper [I], most HFEs could be classified as EoCs, but in about 70 % the consequence to the technical systems was equipment unavailability. Similarly, some EoOs led to wrong system responses (see Figure 3). The findings of Paper [I] emphasise the importance of plant-specific HRA that looks at man machine systems as a whole.

The approach of Paper [V] can be utilised to study all kinds of HFEs, since it is not wise to make any firm distinction at the beginning of an HRA analysis. This is shown in Figure 3 which depicts a generic decision-tree model for classifying human failure events. The model has been developed in this thesis and is an extension of models reported in Hall et al. (1982), Vaurio & Vuorio (1991) and Reiman (1994).

Figure 3 takes into account situations where decisions are made without certainty as, for instance, in accident management. Moreover, the effect of HFEs on the process or equipment cannot normally be judged based on the human failure type (EoO or EoC) only. Even normal human actions can sometimes trigger unwanted consequences if other latent failures are present in the man machine system. Examples of such situations are errors in procedures that lead to a human failure although the operators follow the procedures correctly; and faulty calibration instruments that lead to multiple wrongly calibrated measurements.

* In all cases, identification or decisions may be corrected given that the target system and time allow (recovery)

** No double failures included, e.g. no wrong identification and additional delayed manual actions

Figure 3. Decision tree for classifying human failure events. Unsuccessful recovery is implicitly included in the classes.

Paper [V] discusses human failure events leading to wrong and, in some cases, aggravating equipment functions. In the paper, the concept of commission opportunity (CO) is introduced. It is a systems engineering oriented classification of EoCs, i.e. an identified opportunity for both 1) wrong human actions and 2) other human failure events that may lead to unanticipated or spurious system response. The motivation behind this broad definition is to include all the possible relevant events in the analysis.

The goal of Paper [V] was to develop an approach that could be used to analyse COs. The framework consists of five generic phases that are: target selection, CO identification, screening, modelling, and probability assessment. Defining the context and factors influencing human performance are an important part of the approach. For the identification phase, checkpoints and guiding questions have been developed to help an analyst. Two probabilistic quantification methods are presented in Paper [V].

Next, an application is presented to complete Paper [V]. The framework has been tested in Loviisa NPP in a scenario where a spurious protection signal 'high pressure in containment' is triggered. The signal leads to a risk of the external pressure vessel spraying through the start of the containment spray, and it may also result in a small LOCA after all the consequences of the signal have been triggered in a staggered order. The operators need to identify the wrong signal and make decisions about the counteractions in the context of non-optimal procedures and a limited amount of training.

A team consisting of an HRA specialist, a training instructor and an operations specialist participated in the application of the method. The identification and modelling effort was extensive. As tools, tables manifesting factors affecting identification, decision making and opportunities for wrong manual actions were used to structure the work. Opportunities for wrong identification and decision alternatives were identified, but the conclusion was that, in particular, COs in manual actions manifest themselves quickly and can be recovered. Training, procedural guidance, experience, man machine interface, available time and decision making / safety culture came up as the most important contextual factors also having an effect on probability quantification.

A logistic regression was fitted to the data for the case of failure in identification/decision making concerning a spurious signal. Logistic regression is a commonly used statistical method that may be used to link probability of failure to explanatory factors (e.g. McCullagh & Nelder, 1989, ESReDA, 1995). The parameters in the model were estimated by using expert judgement and the principles presented in Paper [V]. The obtained model for p_{uhf} is shown in equation (1):

$$p_{uhf} = \frac{e^{2.67-0.057*C_1-0.44*C_3-0.61*C_4-0.30*C_5-0.46*C_6}}{1+e^{2.67-0.057*C_1-0.44*C_3-0.61*C_4-0.30*C_5-0.46*C_6}}, \tag{1}$$

where C_1=available time, C_3=training amount, C_4=procedural guidance, C_5=man machine interface, and C_6= decision making/safety culture.

Experience (C_2) was set to a constant in this case since the average is known for plant crews. The parameter time took positive real values and the other parameters were class variables $C_i \in [0,1,2,3,4]$ set so that 0 corresponds the worst level and 4 the best. Altogether 30 combinations of the variables were used to fit the regression model, together with known lower and upper limits for the probability [0,1]. For the current plant conditions, the logistic model fitted gave quite a high result for the human failure probability (p_{uhf}=0.18), but the value obtained for actions leading to aggravated plant conditions through starting more spray pumps was quite small (p_{apc}= 2E-3). This result is satisfactory against the background that the context is rather confusing for the operators. The fit was sufficient (R^2=0.73). Also, there was good agreement between the individual expert judgements.

The participants' insights were that the applied framework was very useful and important factors affecting the operators could be discovered. The most important factors affecting the probability were the available time and procedural guidance, which is understandable against short time windows and the non-existence of procedures for spurious protection signals. The results are applicable to training and procedure development. Although the application was somewhat time consuming this aspect is easy to develop.

3.1.3 Time reliability correlation methods

Time reliability correlations (TRCs) are often used to model human reliability in cases where the mission for human operators is to balance the situation after an IE has taken place. Carrying out the actions in time is important and, thus, the available time for human action is the most important variable in the TRC models presented in Section 2.2. On the other hand, for example, Sträter & Reer (1999) have expressed doubt about the importance of time dependency. Bley (1988) emphasises that time is the key factor of success for post IE human actions in the control room. Also, in most cases other PSFs are taken into account (e.g. Hannaman et al., 1984). The same reference also shows how the cognitive level of human actions may be taken into account, e.g. by using Rasmussen's (1979) skill, rule and knowledge (SRK) classes. Vaurio & Vuorio (1991) show how the cognitive level may be defined by using a measurable parameter, the amount of training. Mostly, simulator runs are utilised as data for the TRC models, but also real events (e.g. Baumont, 2000) and expert judgement (e.g. Paper VI) and their combinations are used.

For example, Hall et all. (1982) and Hollnagel (1998) suggest decomposing human actions in post IE HRA modelling into phases, such as identification, interpretation, decision making and manual actions. This decomposition helps in understanding and modelling human performance problems, as was shown in Figure 3. However, Vestrucci (1989) discusses how modelling decisions about the timing of these phases and their SRK classification may have significant impact on HFE probabilities. Moreover, collecting probabilistic data for them separately is often impossible. Human actions, including potential recovery of failures, have to be carried out before irreversible consequences take place. These facts have led to holistic TRC analyses discussed in Papers [III], [IV] and [VI]. In these papers the calculation of human failure probability took place by Monte Carlo simulation, after estimating the distribution parameters of the time required for human action and of the available time. Other PSFs affecting human performance, were taken into account in the distributions in an implicit way. This was done by applying expert judgement, in Papers [III] and [VI], and by using simulator data, in Paper [IV].

Papers [II] and [V] show how the generic time reliability correlation of Swain (Swain & Guttmann 1983, Swain 1987) may be updated to represent plant-specific conditions in human actions after an IE. The model is based on the idea that the probability of a failed action depends on the available time t and on a number of factors $K_1, \ldots, K_n$ as follows in (2):

$$p_{plant}(t; K_1, \ldots, K_n) = \min\{p_{gen}(t) \prod_{i=1}^{n} K_i; 1\}, \qquad (2)$$

where $p_{\text{gen}}(t)$ is called the generic time-dependent human error probability and $K_1, \ldots, K_n$ are performance shaping factors (PSF) comparable to $C_1, \ldots, C_n$ in *(1)*.

The assessment of human failure probabilities has the following phases: 1) estimation of available time t, 2) obtaining the failure probability p_{gen} from the generic time-reliability curve $p_{\text{gen}}(t)$ in Swain & Guttmann (1983), 3) estimation of PSFs $K_1, \ldots, K_n$, 4) deriving the action specific failure probability with equation (2). The five used classes in Paper [II] have proved to give meaningful estimates. Text descriptions about the principles followed are important and should always accompany an analysis. A procedure to use expert judgement for estimating PSFs has been described in Holmberg & Pyy (2000). Papers [II] and [V] discuss the procedure used in estimating the available time.

The model is transparent and useful for taking into account the effect of PSFs in cases where no experience or simulator data are available. Multiplicative models for updating generic estimates in order to produce plant specific estimates have been suggested, e.g. in Procaccia (1995). The structure of the model allows coping with the anchoring bias common in expert judgement. This means, for example, adjusting the base rate too little although the evidence would suggest something else.

On the other hand, in cases where many of the factors K_{i} obtain either high or low values, an analyst also has to assess a) whether the factors are independent and b) if their effect is actually that strong on the probability, i.e. their weight. The weight is normally implicitly taken into account in the PSF value, but using power functions of PSFs (K_{i}^{j}) is possible. It also is possible to set limits to the maximal effect of the PSFs in order to limit their influence. The results produced by the model may be compared to known simulator run results for other events, and a calibration of the PSF influence carried out, accordingly. Furthermore, it should be noted that the tables of Swain & Guttmann (1983) and the decision trees in Spurgin et al. (1999) may be expressed in the form of a multiplicative probability model.

It is worth noticing that the available time affects human performance in two ways. Firstly, perception about long time windows may cause sloppiness, manifested by, for example, some maintenance-related failures in Paper [I], and ideas about a potentially short time window may be a mental burden, as noticed in the simulator runs used as data for Paper [IV]. Secondly, due to physical processes, the success of the mission is impossible after a certain time point regardless of whether the personnel are aware of the situation or not. In many cases, operators are also capable of changing the time window by their actions, as discussed in Paper [IV].

Estimating TRCs generally requires maximum likelihood principles, which are standard statistical methods discussed in several textbooks, e.g. in Procaccia (1995). The TRC fitted for the first decision-making situation in Paper [IV] produces similar results to the HCR (Hannaman et al., 1984) rule-based curve. The results also are comparable to Swain's nominal TRCs for times up to 60 minutes.

Paper [VI] highlights the effect of event history on human reliability, i.e. all the observed events such as faults and indications may have an effect. Methods for modelling instantaneous failure intensities and history processes in PSA have been discussed, e.g. by Holmberg (1997).

3.1.4 Methods for HRA of shutdown conditions and of actions outside the control room

Human reliability is very important in shutdown conditions and during low power operation. Extensive qualitative and quantitative HRAs have been carried out to study these situations in the Nordic countries. For example, Papers [II] and [III] discuss how coolant leakages caused by human failure dominate the core-damage frequency of BWR plants during refuelling outages. This result shows that other initiating events may be more significant than the loss of residual heat removal in a shutdown PSA.

Paper [II] shows how the same HRA methodology may be applied to all NPP operating modes. HRA has revealed how human co-ordination errors, work order confusion and deficient restoration of equipment may initiate undesired event sequences, e.g. loss of residual heat removal, criticality events, crane accidents and leakages. Human actions also cause both scheduled and non-scheduled system unavailability, which may be important in PSA. Finally, Paper [II] shows how shutdown risk may be significantly reduced by changing working practices. Such changes would be cost effective.

Paper [III] discusses an inadvertent opening of an isolation valve and the follow-up balancing actions undertaken to hinder a rapid core uncovery of a BWR with external circulation loops. Many different factors affecting the leakage probability and the timing of recovery actions were identified. Due to the identified uncertainties, it is advisable to avoid situations where the irradiated fuel both in the reactor and in the pools may become uncovered due to a shutdown LOCA.

Moreover, Paper [VI] discusses the analysis of both decision making and of observation of unanticipated events during reactor tank water filling at the end of a shutdown procedure of a BWR plant. The analysis was related to the cold overpressure risk study. The conclusion of the paper is that the risk is very low, but the process feedback in shutdown conditions could generally be better.

Finally, Papers [II] and [III] also discuss human actions outside the main control room in shutdown conditions. Actions outside the control room, such as starting a pump from its switchgear unit, may also be important in disturbances beginning from power operation, discussed in Paper [IV]. Recovery from outside the control room may help to master a disturbance, but it also requires additional resources and communication, which may have adverse effects on other actions. This has to be taken into account in HRA.

3.2 Human reliability data

Plant specific NPP human reliability data generally consists of expert judgement, simulator runs and, in a few cases, of real life experience. Plant and context specific data collection for HRA is important since human behaviour is very context dependent, as discussed, for instance, by Hukki & Norros (1997, 1998).

3.2.1 Plant maintenance data

In human reliability research, the main focus has not been on maintenance despite the fact that maintenance and testing have contributed to the course of events by disabling equipment in, for example, the Chernobyl and Three Mile Island accidents. Maintenance actions contributing to faults have been studied, e.g. by Samanta & Mitra (1981), Wreathall et al. (1990), Reiman (1994), Morris et al. (1998) and Laakso et al. (1998). In particular, dependent failures affecting several trains of a safety-related system may have a significant contribution to the reactor core damage risk (Hirschberg 1990, Reiman 1994). Also Swain & Guttmann (1983), Samanta et al. (1985) and Vaurio (1999) discuss human-originated dependent faults from a probabilistic point of view.

Paper [I] draws statistical conclusions about the properties of faults caused by maintenance-related human actions. A large database from one nuclear power plant (Laakso et al., 1998) was utilised, which is unique. The most important results of Paper [I] are presented in the following paragraph.

Instrumentation and electrical components were frequently affected by maintenance actions in the database of Paper [I]. This is due to the vulnerability, complexity and large quantity of such equipment. Thus, in HRA more emphasis has to be put on studying instrumentation, control and electrical components in safety critical systems. Paper [I] also compares the amounts of maintenance-related faults during outages and during power operation. A major number of the faults were initiated in outages, which is reasonable because of the large number of shutdown maintenance activities. However, about 50 % of them remained undetected until the power operation. In that respect, single and dependent human errors show almost similar behaviour.

A large number of maintenance-originated faults took place in safety-related systems. The abundance of scheduled maintenance and testing activities with more stringent fault reporting practices in safety-related systems are mentioned as potential explanations for this in Paper [I]. The number of human originated faults in the maintenance data is notable. However, the number of dependent faults remained rather low. The safety significance of single human-induced faults was small, but some dependent faults were found to be significant. Modification related activities were a significant cause of dependent faults.

Statistical information on human actions may be generated, based on maintenance history. This provides an exception to the rarity of quantitative HRA data. Plant maintenance data is one of the few sources of real historical information on effects of human performance on technical systems, and it should be applied more often to that purpose. This is the teaching of Paper [I] together with the fact that the analysis requires a considerable amount of work and knowledge.

3.2.2 Simulator data

Full-scale training simulators have become an important source of HRA information. They can be utilised to identify important human actions and the deviations from these actions, to validate models of human performance and to collect quantitative data. For example, Norros & Sammatti (1986) discuss identifying deviations from procedures in operator performance during simulator exercises, and notice that many of them are somewhat insignificant from the safety point of view. Simulator runs have also been used to make inferences about the influence of certain performance-shaping factors, such as displays (Norros & Nuutinen, 1999), alarms (O'Hara et al., 1998) and manning levels (Hallbert et al., 1996). Furthermore, simulator data has been used to estimate the parameters of time reliability correlation, e.g., in Moieni et al. (1989) and Vuorio & Vaurio (1987).

Reiman (1994) and Hirschberg & Dang (1998), for example, discuss factors that differ from real plant conditions when disturbances are simulated. They are, 1) operator crew's anticipation of abnormal events, 2) concentration of the whole crew in the control room during the disturbance and 3) the difficulty of including the reality outside the control room, including the emergency organisation, in the simulator runs. Also, the participating operator's mental load is lower in simulator exercises.

Most of the above mentioned factors could be taken into account when analysing the international study reported in Paper [IV]. In the study, data was collected both for qualitative and quantitative purposes. The qualitative interviews and video recordings included operators’ reasoning about the factors and the decision goals they considered important in various phases of the disturbance. This data was applied to the qualitative decision models that were used to validate the content of quantitative models.

The quantitative data included recorded behaviour of process parameters and control actions by the operators. The data were used to estimate the parameters of the time reliability correlation for the first decision situation, and the parameters of the probabilistic decision model for the second one (see Section 3.1.1). However, the amount of simulator runs was very limited. Thus, expert judgement was elicited to complete the data. The experts’ probability estimates about operators’ choices formed the a priori expectations. Evidence from the simulator runs was then used to obtain a posteriori estimates by Bayesian updating methods.

The methodology for post IE human action reliability assessment described in Paper [II] also makes use of simulator data for assessing HFE probabilities for actions that have been repeated in training. Swain’s generic TRC correlation formed the a priori estimates, which were updated by using simulator data. Another approach was applied in Paper [II] for cases, where no simulator information is available, and it is described in the following section.

3.2.3 Expert judgement

Methods to elicit and to combine expert judgements have been reported, e.g. in Comer et al. (1984), NRC (1990) and Cooke (1991). Furthermore, Bradley (1953) discusses the paired comparisons used in Paper [IV]. The group consensus techniques to combine judgements, such as Delphi and nominal group technique are discussed, for instance, in Dalkey (1969) and Delbecq et al. (1975). Mathematical aggregation may take place, e.g. through straight averaging, through expert determined weights (e.g. DeGroot, 1974) or by Bayesian methods (e.g. Mosleh & Apostolakis, 1984, Kaplan (1992) and Pulkkinen, 1994). For example, Tversky & Kahneman (1974), Svenson (1989), NRC (1990) and Otway & von Winterfeldt (1992) discuss potential biases in expert judgement and ways to avoid them. A comprehensive collection of aggregation methods is presented in Clemen & Winkler (1999). Finally, Comer et al. (1984) and Reiman (1994) present applications of expert judgement to HRA.

Structured expert judgement may be used to determine important parameters, such as PSFs, in HRA models, and to evaluate their influence. Paper [II] presents an application of expert judgement to a human reliability analysis of a BWR in cases where no simulator training data on post IE human actions exist (see 3.1.3). The method is based on 1) Swain's time reliability correlation as the source of generic estimate for human error probability and 2) on multiplying it by using five plant-specific co-factors: procedures, training, feedback from process, mental load and decision burden. Paper [II] emphasises that the factors have to be based on a thorough qualitative analysis to avoid biases. The method has proved to be useful, and it has also been applied to a PSA study in another NPP discussed in (Holmberg & Pyy, 2000).

Paper [V] shows an application of the multiplicative model, discussed in the previous paragraph, to evaluating probabilities of commission opportunities (see Section 3.1.2). The interpretation of the co-factors in the paper is that they partly directly affect the probability of success, as in the availability of the right tools, and that they partly affect mental burden. Paper [V] also presents a logistic regression quantification method based on the same co-factors as in the multiplicative model, discussed further in Section 3.1.3. Plant or simulator data may be used to calibrate the logistic model and expert judgement completes the data points. The calculation of the correlation parameters takes place by using maximum likelihood principles. Paper [III] presents the HRA study of a leakage during the refuelling outage of a BWR reactor. Human actions are the main possible causes of the leakage. The case was used to develop further the expert judgement methodology of Pulkkinen & Holmberg (1997). The methodology is based on 1) discussions between substance matter experts and normative experts in three phases, 2) direct elicitation of unknown variables, and 3) applying a Bayesian combination of judgements and 4) completing sensitivity analyses. The emphasis is on experts' reasoning and communication in order to avoid biases and the use of heuristics such as rules of thumb and principles that are not founded on theory and reality.

In the application, three variables were chosen for expert judgement. They were the frequency of the leakage, the available time, and the time taken to balance the situation. The substance-matter experts came from the power company and the normative experts from VTT. The substance-matter experts represented a wide variety of expertise ranging from psychology and reliability analysis to operational and maintenance knowledge. All the experts had a good knowledge of the outage situation and related analyses, and they received training on probability assessment.

Three fractiles (5%-, 50%- and 95%-) of the distributions of the variables were calculated. Besides the Bayesian combination, a direct combination of distributions took place, as shown in Figure 5 for one variable. Also the effect of individual experts on the results was studied in the sensitivity study.

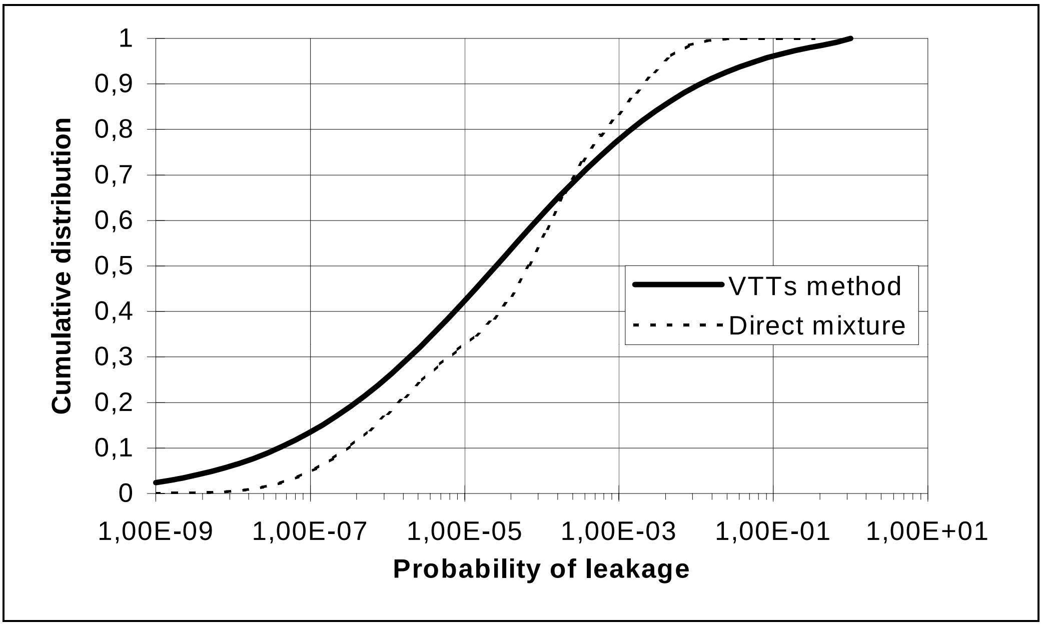

Figure 5. Comparison of combined distributions, variable 3 (θ)), probability of a leakage (per year), in Paper [III].

A direct combination of distributions tends to lead to tighter uncertainty bounds and to some lower expected values than the Bayesian method, as shown in Figure 5. This is mostly due to the fact that the version of the Bayesian model used in the exercise takes into account the potential overconfidence of experts. Although VTT's method produces large uncertainty bounds, the uncertainties related to the leakage proved to be large independent of the method used, which also was the understanding of the power company. Paper [III] showed that expert judgement forms a good complement to other data collection methods, but substance-matter experts may have problems when probability variables are produced.

A way to avoid these problems is to choose observable parameters of the probability model that are better known to the substance matter experts. Paper [VI] presents an application to a BWR shutdown cold overpressure study. The probability of not noticing a spurious start of an auxiliary feed-water pump during the filling of the reactor with water was the variable of interest. Instead of eliciting fractiles of the time distribution directly, the experts were asked to specify the time within which the 2^{nd}, 6^{th} and 11^{th} crew out of a total of 12 plant crews would observe the spurious start of the pump. This was done in order to help them to associate their estimates with plant conditions they knew well. These time points were interpreted as 5%, 50% and 95% fractiles.

The experts participating in the analyses were operators, a simulator instructor and the author. A simulator run was used to refresh the memory of the experts on the exact conditions that occur when water filling. The results in Paper [VI] showed that observing the spurious start is easy, and that it takes place fast.

3.3 Interdisciplinary analysis of human reliability

A balanced human reliability analysis requires knowledge on plant maintenance, operations, design, process physics, reliability engineering and human behaviour, among other requirements. Due to the nature of HRA, it has been difficult to develop methods that are widely accepted by all disciplines. Recently, attempts have been made in several related areas to develop more plausible approaches. Examples of these are cognitive simulation models, discussed briefly in section 2.2, and approaches to integrating PSA and dynamic process simulation, discussed by Cacciabue (1998) and Hortal & Izquierdo (1996). Furthermore, Andersson & Pyy (1998) discuss structured frameworks to allow different disciplines to participate in human reliability analyses. Other approaches of interdisciplinary HRA can be found, e.g. in Barriere et al. (1995) and in Mosneron-Dupin et al. (1997).

The objective of an interdisciplinary HRA, promoted in the papers in this thesis, is to provide a balanced view on important features of human reliability by improved co-operation between different disciplines. Sometimes, this is not trivial due to the very different research approaches, nomenclature and traditions.

There are basically three structured approaches to attain improved and more balanced information exchange in HRA. In the decision analytic approach, discussed in Paper [IV], experts in different disciplines look at a problem from different viewpoints and present their analyses to a decision maker, who weights different pieces of evidence together. In the expert judgement approach, discussed in Paper [III], the task for all disciplines is to assess the values of the same variables of interest. There, experts in probability calculus elicit the data from substance-matter experts, e.g. behavioural scientists and process experts. The third structured method, discussed in Paper [VI], is to create a working group of different disciplines to work on the same problem in a controlled manner. The idea of this approach is to ensure proper interdisciplinary communication, so that the results of an integrated analysis will be more than just the sum of separate analyses. This third approach can be regarded as a real interdisciplinary HRA, which is illustrated in Figure 7, consisting of systems analysis, the behavioural sciences, physical analyses, and the power plant context. In some cases, also, participation of other disciplines, such as structural integrity experts, may be required.

The objective of Paper [VI] was to apply the principles of the interdisciplinary HRA and, especially, to focus upon integrating probabilistic and psychological approaches. An improved communication between disciplines was achieved through adopting reference models that adequately reflected essential features of the phenomenon being studied, and through carrying out an interactive analysis process. The analysis had two major phases: 1) the description of the context and 2) both psychological and probabilistic modelling.

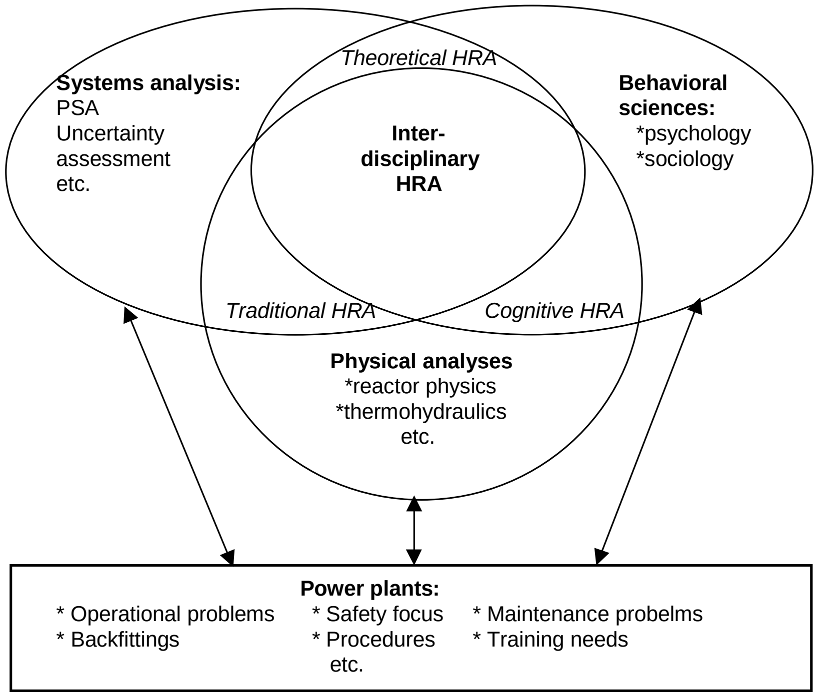

Figure 7. A presentation of the structure of an interdisciplinary HRA modified from Andersson & Pyy (1998).

As discussed in Section 3.1.1, the object of the analysis was the operating procedure for reactor tank filling, including a significant amount of decision making. In the description of the context, the main process events, information sources, human actions, decision points and boundary conditions were visualised by using natural language, and the common reference models were drafted. In the probabilistic analysis, the modelling phase consisted of the construction of a probability model. It was, in Paper [VI], specified as an influence diagram with a marked point-process framework (e.g. Holmberg, 1997). The main probabilistic model included several sub-models.

The description of the context served as a reference, both in the psychological analysis of the adequacy of process control and in the analysis of human actions. The psychological analysis focused on the empirical data of the operators' performance collected in the simulator exercise and, thus, it brings the actors' point of view to the human reliability analysis. This is important in order to evaluate what are the most important PSFs in the analysed case.

In the analysed case, decision analytic thinking was an integrating factor between the probabilistic and psychological analyses. The proposed integrated analysis approach is in itself rather general and applicable to many kinds of situations. Thus, in future, structured interdisciplinary approaches may turn out to be a feasible tool for more realistic HRA. They complement approaches such as the one described in Paper [II] that are tailored more for everyday PSA work.

4. CONCLUSIONS OF THE PAPERS

Table 2 summarises the findings of the papers attached to this thesis.

Table 2. Conclusions based on Papers [I]–[VI].

Paper [I]	Plant maintenance history is a good human reliability related plant-specific data source and should be used more extensively in future. Errors of omission do not lead automatically to unavailability of a system, and errors of commission to wrong system functions, correspondingly – the consequences of human actions are almost completely context dependent, which emphasises the need for target-specific analyses. Instrumentation, control and electrical components are especially prone to human failures, partly due to their vulnerability and partly due to the complexity of the equipment. Thus, more emphasis has to be put on studying I & C and electrical components in HRA. A large number of human failures takes place in safety-related systems, which may be due to the large number of scheduled activities in safety systems, and to the fact that the fault reporting criteria may be less stringent in non-safety related systems. Plant modifications appear as a very important source of dependent human failures, and many of them remain latent until the plant start-up – these facts should lead to a more thorough planning, co-ordination, functional testing and other operability verification actions before starting the operation.
Paper [II]	HRA has to allow the involvement of several personnel groups; this is the reason why the role of transparent modelling and verbal descriptions as the basis for probability parameters is vital. An HRA methodology has to be capable of dealing with very different human actions and environments. Apart from the control room actions in disturbances starting from power operation, for instance, maintenance action induced dependencies and human actions in shutdown conditions are important from the risk point of view. Maintenance and testing related mechanisms leading to dependent failures are, e.g. procedure or work order deficiencies; task characteristics themselves; resource arrangements; calibration equipment or crew composition. Other PSFs such as spatial or temporal coupling may influence the probability estimates but not be the mechanism itself. Risk decreasing actions based on HRA, such as changes in working practices, may be very cost-effective.

Paper [III]	Expert judgement provides important information for human reliability analysis, especially if expert interaction is allowed. However, normative experts have to moderate the discussion in order to restrict biases and to steer the experts to seek for evidence. Different combination principles of expert judgements may lead to significant differences in results. This is an example of modelling uncertainties encountered frequently in HRA. Direct expert judgement of probabilities has to be considered with care since people have difficulties with the concept of probability. In particular, experts have difficulties in defining the fractiles of an uncertainty distribution of probability. Rather, judgements about observable variables that the experts can relate to their experiences should be elicited. Shutdown LOCA risk can be quite high and human actions are in a major position both as sources of risk and in balancing the situation. This fact is also acknowledged by the power companies, and actions have been taken to reduce the risks.
Paper [IV]	Decision making during accidents and disturbances may be modelled by applying methods based on human reliability modelling and the use of decision theory, which is an extension to the current HRA paradigm. The use of probabilistic modelling has to be supported by a qualitative analysis that validates the modelling principles used. Time reliability correlation models may be used to model simple diagnosis / decision situations, whereas in real multi-criteria cases decision behaviour is related to the operator crews' attitudes to the situation and their values. Modelling such cases requires real multi-criteria models. Due to the fact that human reliability data from, for example, simulator runs is sparse, structured expert information may be used to complement it.
Paper [V] and summary of its application in Section 3.1.2	HRA methods should be generic frameworks rather than developed for specific events such as 'errors of commission' only. The presented framework moves consistently from identification of important factors to the probabilistic quantification. The practical application produced many practical working tools, such as table formats, that helped a great deal in documenting and steering the analysis. The work was found to be useful in training and instruction planning by the representatives of a power company. In the case of wrong protection signals, the probability of human failure may be considerable. However, the probabilities of aggravating human actions may still be small.

Paper [VI]	An integrated (interdisciplinary) HRA approach means communication between disciplines with the help of a framework, within which the points of view of each discipline can be taken into account. Models understood by different disciplines (reference models) help in such a task. By taking the operator's view into account, it is possible to achieve a deeper comprehension of the situation, which produces new information about factors affecting probabilities of human actions. The proposed integrated approach is in itself rather general and applicable to many different cases. The approach takes into account the dynamic nature of the man-machine interaction and presents a detailed probabilistic framework for its analysis. The probability of cold overpressure for Nordic BWR reactors is very small. In that respect, the analysis presented in this paper confirms the results of the analyses carried out by the power companies.

Moreover, there are a number of good practices that should be applied to HRA. Generic requirements have been set in the literature for PSA, e.g. in (NRC 1990, Cooke, 1991). The analysis should be reproducible, accountable, subject to empirical control, neutral and fair. Reproducibility means that all the calculations and analyses have to repeatable. Accountability means that the values given can be traced to their source. Empirical control means that the results could, in principle, be falsified by empirical data. Neutrality means independence of the decisions made as a consequence of the analysis, e.g. participating experts should not feel tempted to manipulate the uses of methods and judgements because their own values are involved. Finally, fairness requires that all events and experts are treated equally during the analysis, which does not pre-empt using some screening rules and weighting procedures.

A credible HRA should deal more with observable parameters and PSFs than with ambiguous factors, such as the level of cognitive activity. Human reliability assessment calls for a robust framework under which one may create application-specific refined models that are valid for particular circumstances. In the following, more detailed features of good HRA practices are presented together with references to Papers [I]–[VI].

1. A quantitative HRA method has to be technically valid for the situation to be analysed, and compatible from the identification to quantification. Papers [II]–[VI] emphasise this by showing how the principles and results of the qualitative analysis are used in the quantitative analysis.

2. Human actions are very sensitive to the associated surroundings, and HRA methods have to take into account essential contextual factors. This should take place either explicitly, e.g. by using PSFs / PICs, or implicitly in holistic expert judgement. In the latter case, a qualitative description has to follow, as suggested in Papers [III] and [VI]. Explicit contextual factors and their influence on probabilities are shown in Papers [II] and [IV]–[V].

3. HRA has to look for plant-specific experience data, as Paper [I] emphasises. However, due to the scarcity of this data a method has to be capable of taking into account different kinds of data types, such as simulator information and expert judgement. Methods and uses related to simulator data are presented in Papers [II], [IV] and [VI]. Expert judgement information is used in Papers [II]–[VI] as one of the data sources.

4. The method has to be mathematically acceptable, i.e. the calculus principles have to be sound and presentable in the probabilistic framework. The calculus also should be as transparent as possible, although some mathematical models require, by definition, more knowledge than others. Papers [II]–[VI] emphasise these principles.

5. HRA methodology should be flexible for different PSA modelling levels. This principle, together with (2) and (3), sets requirements for user competence so that the results remain realistic at all levels if the analysis is made more detailed, which also is related to the costs of the analysis. Papers [V]–[VI] present very detailed modelling principles, whereas Papers [II]–[VI] also present rather generic modelling approaches, applicable to a coarse assessment.

5. CONCLUDING REMARKS

Human reliability analysis and reliability analyses of technical systems can be based on the same reliability engineering principles, since the aim is to model events in logical PSA models. Also in areas other than HRA, such as in modelling physical phenomena and structural integrity in PSA, there are discussions about causal versus probabilistic modelling of phenomena. The major differences in the probabilistic analysis of human performance when compared to other parts of PSA are that 1) man can introduce unforeseen dependencies into a technical system and 2) man is capable of decision making and proactive behaviour instead of only adapting to an event.

The most important methodological developments manifested in the thesis concentrate on the HRA of decision making, and modelling commission opportunities. However, it is vital not to analyse them separately but to put them into perspective in the whole spectrum of potentially significant events in human reliability analysis. Those events include human functions from perception to manual actions, the whole life cycle of an installation from design to decommissioning, the events from normal operation to severe accidents and the yearly cycle with all the operating modes including shutdown.

Human reliability analysis consists of many different types of information and knowledge. As shown earlier, using approaches allowing disciplines to communicate in a structured manner, such as expert judgement and decision analysis, should be promoted. At the same time, HRA methodology should be kept transparent and understandable to the many interest groups in order to increase its credibility in risk management. In this respect, it is also vital to strengthen the collection of factual data.

Despite the fact that everybody has had experience of human behaviour, probabilistic human reliability data is generally sparse. Thus, all available data should be used in HRA. There should also be a wider utilisation of plant-specific information. Maintenance databases and training simulators are examples of potential data sources, and they should be utilised more extensively. However, an analyst also has to understand the limitations of and potential biases in these sources. Expert judgement may include insight factors that cannot be obtained by tests etc. It forms a good and necessary complement to other information, especially in the case of rare events. However, expert reasoning should be well documented, the data should not be used outside the context for which it was elicited, and the results should be subject to empirical control whenever possible.

Despite the amount of development presented, both in the methodology and the data, there are still areas to be studied. The dependencies, 1) between the human actions and 2) in technical systems due to human actions, may require more thorough studies, although they may also be treated by choosing a higher modelling level. Extension of human reliability analyses into accident management emphasises the role of decision making in an environment, and for which there cannot be strict procedures. Finally, it is important to continue collecting more information about human failure mechanisms and contexts.

Human reliability analysis is one of the areas of probabilistic safety assessment that has direct applications outside the nuclear industry. Although this thesis consists of applications to NPPs, maintenance outages, for example, take place in all industries and time is a crucial factor in the cockpit of an aeroplane. A proper human reliability analysis studies man machine systems as a whole. Similarly, both the positive and negative aspects of human behaviour are taken into account instead of focusing on errors only. Understanding this increases both the use and acceptability of HRA.

REFERENCES

Andersson, K. & Pyy, P. 1998. Integrated Sequence Analysis. NKS/RAK-1(97)R11. Risö, Informationservice. 52 p.

ASME. 2000. Standard for Probabilistic Risk Assessment for Nuclear Power Plant Applications. Draft version Rev. 12, 30.5. 2000. American Society for Mechanical Engineers. 154 p.

Barriere, M. T., Wreathall, J., Cooper, S. E., Bley, D. E., Luckas, W. & Ramey-Smith, A. M. 1995. Multidisciplinary Framework for Human Reliability Analysis with an Application to Errors of Commission and Dependencies. NUREG/CR-6265. U.S. Nuclear Regulatory Commission, August 1995. 86 p. + app. 97 p.

Baumont, G. 2000. The Recuperare Model and Method – A method integrating human reliability for analysing safety significant events. IPSN, Safety assessment department report 371E, Fontenay-aux-Roses, France. February 2000. 44 p. + app. 5 p.

Bello, G. C. & Colombari, V. 1980. The human factors in risk analyses of process plants: the control room operator model 'TESEO'. Reliability Engineering (1), pp. 3–14.

Bieder, C., Le Bot, P., Desmares, E., Cara, F. & Bonnet, J. L. 1998. MERMOS: EdF's new advanced HRA method. In: Mosleh, A. & Bari, R. (eds.). Proceedings of an international conference on probabilistic safety assessment and management. New York, September 1998. Springer Verlag. Pp. 129–134.

Bley, D. 1988. Light water reactor sequence timing: its significance to probabilistic safety assessment modeling. Reliability Engineering and System Safety 22, pp. 27–60.

Bley, D., Wreathall, J. & Coope, S. 1998. Things not modeled in nuclear plant PSA. In: Mosleh, A. & Bari, R. (eds.). Proceedings of an international conference on probabilistic safety assessment and management, New York, September 1998. Springer Verlag. Pp. 1695–1696.

Bradley, R. 1953. Some Statistical Methods in Taste Testing and Quality Evaluation. Biometrics, Vol.9, pp. 22–38.

Cacciabue, P. C. 1992. Cognitive Modelling: A Fundamental Issue for Human Reliability Assessment Methodology. Reliability Engineering and System Safety 38, pp. 91–97.

Cacciabue, P. C. 1998. Modelling and simulation of human behaviour in system control. Springer Verlag, London. 357 p.

Clemen, R. T. & Winkler, R. L. 1999. Combining Probability Distributions form Experts in Risk Analysis. Risk Analysis, Vol. 19, No. 2, pp. 187–203.

Comer, M. K., Seaver, D. A., Stillwell, W. G. & Gaddy, C. D. 1984. Generating human reliability estimates using expert judgment. NUREG/CR-3688.U.S. Nuclear Regulatory Commission, Washington DC. 47 p. + app.

Cooke, R. M. 1991. Experts in Uncertainty. Opinion and Subjective Probability in Science. Oxford University Press, New York.. 321 p.

Cooper, S. E., Ramey-Smith, A. M, Wreathall, J., Parry, G. W., Bley, D. C., Luckas, W. J., Taylor, J. H. & Barriere, M. T. 1996. A Technique for Human Error Analysis (ATHEANA) – Technical Basis and Methodology Description. NUREG/CR-6350. U.S. Nuclear Regulatory Commission, May 1996. 86 p. + app. 24 p.

Dalkey, N. 1969. An experimental study of group opinion: The Delphi method. Futures (1), pp. 408–426.

Dang, V. 1996. Modeling cognition for accident sequence analysis: development of a dynamic operator-plant simulation. PhD Thesis, MIT, Cambridge, USA.

DeGroot, M. 1974. Reaching a consensus. Journal of American Statistical Association, Vol. 69, pp. 118–121.

Delbecq, A. L., Ven, A. H. van den & Gustafson, D. H. 1975. Group Techniques for Program Planning. A Guide to Nominal Group and Delphi Processes. Scott Foresmann & Company, Glennview.

Dougherty, E. 1990. Human Reliability Analysis – where shouldst thou turn? Reliability Engineering and System Safety 29, pp. 283–299.

Dougherty, E. 1997. Is human reliability a stochastic process? Reliability Engineering and System Safety 55), pp. 209–215.

Dougherty, E. 1998. Human errors of commission revisited: an evaluation of the ATHEANA approach. Reliability Engineering and System Safety 60, pp. 71–82.

Drogaris, G. 1993. Major Accident Reporting System – Lessons learnt from Accidents Notified. CEC, JRC ISEI, EUR 15060 EN. Elsevier Science Publishers, The Netherlands. 240 p.

Embrey, D. E., Humphreys, P. C., Rosa, E. A., Kirwan, B. & Rea, K. 1984. SLIM-MAUD: An approach to assessing human error probabilities using structured expert judgment. NUREG/CR-3518. 29 p.

ESReDA. 1999. Handbook on Quality of Reliability Data. ESReDA Statistical Series no 4. Det Norske Veritas, HØvik, Norway. 179 p.

Farmer, F. R. 1967. Siting criteria – a new approach. Proceedings of IAEA symposium on the containment and siting of nuclear power reactors, Vienna, 3–7 April, 1967. Paper IAEA SM-89/34. Pp. 303–329.

French, S. 1986. Decision Theory: An Introduction to the Mathematics of Rationality. Ellis Horwood Ltd. 448 p.

Fullwood, R. R. & Hall, R. E. 1988. Probabilistic Risk Assessment in Nuclear Power Applications. Pergamon Press. Pp. 198–214.

Gertman, D. I., Blackman, H. S., Haney, L. J., Seidler, K. S. & Hahn. H. A. 1992. INTENT: A method for estimating human error probabilities for decision based errors**.** Reliability Engineering and System Safety, 35, pp. 127–136.

Hacker, W. 1998. Allgemeine Arbeitspsychologie – Psychische Regulation von Arbeitstätigkeiten. Verlag Hans Huber, Bern. 875 p.

Hall, R. E., Fragola, J. R. & Wreathall, J. W. 1982. Post Event Human Decision Errors: Operator Action Tree / Time Reliability Correlation. NUREG/CR-3010, United States Nuclear Regulatory Commission. 48 p.

Hallbert, B., Sebok, A., Morisseau, D. & Persensky, J. 1996. Results of the Study of Control Room Crew Staffing for Advanced Passive Reactor Plants. Proceedings of Enlarged Halden Project Meeting (EHPG), Loen, Norway, May 1996.

Hannamann, G. & Spurgin, A. 1984. Systematic Human Action Reliability Procedure (SHARP). NUS Corporation. EPRI NP-3583. 126 p.

Hannamann, G., Spurgin, A. & Lukic, Y. 1984. Human Cognitive Reliability Analysis for PRA Analysis. NUS Corporation. NUS-4531.

Hirschberg, S. (ed.). 1990. Dependencies, Human interactions and Uncertainties. Final report of NKS/RAS-470 project. ABB Atom. 244 p.

Hirschberg, S. & Dang, V. (eds.). 1998. Critical Operator Actions – Human Reliability Modeling and Data Issues. February 1998, OECD, Nuclear Energy Agency, Nuclear Safety, NEA/CSNI/R(98)1. 247 p.

Hollnagel, E. 1995. Summary of approaches to dynamic analysis of man-machine interaction. NKS/RAK-1(95)R1, May 1995. 18 p.

Hollnagel, E. 1996. Reliability Analysis and Operator Modelling. Reliability Engineering and System Safety 52, pp. 327–337.

Hollnagel, E. 1998. CREAM – Cognitive Reliability and Error Analysis Method. Elsevier Applied Science Publishers. 340 p.

Hollnagel, E. & Marsden, P. 1996. Further development of the phenotype-genotype classification scheme for the analysis of human erroneous actions. European Commission, Joint Research centre, EUR 16463 EN. 88 p.

Holmberg, J. 1997. Probabilistic safety assessment and optimal control of hazardous technological systems – a merked point process approach. Doctoral Thesis. VTT Publications 305, Technical Research Centre of Finland, Espoo. 32 p. + app. 77 p.

Holmberg, J. & Pyy, P. 2000. An Expert Judgement Based Method for Human Reliability Analysis – Application to Forsmark 1 and 2 Probabilistic Safety Assessment. 6 p. A paper to be presented in PSAM 5, International Conference on Probabilistic Safety Assessment and Management, November 27 – December 1, 2000, Osaka, Japan.

Hortal, J. & Izquierdo, J. M. 1996. Application of the integrated safety assessment methodology to the protection of electric systems. Reliability Engineering & System Safety, 52, pp. 315–326.

Hukki, K. & Norros, L. 1997. A systemic approach to the modelling of decision making in the control of complex dynamic processes. Proceedings of the 13th Triennal Congress of the International Ergonomic Association, Tampere, Finland. Volume 3. Pp. 43–45.

Hukki, K. & Norros, L. 1998. Subject-centered and systemic conceptualisation as a tool of simulator training. Le Travail Humain, Tome 61, No 4, pp. 313–331.

Humphreys, P. (ed.) 1988. Human Reliability Assessor's Guide. RTS 88/95Q. Safety and Reliability Directorate, United Kingdom. 271 p.

IAEA 1992. Procedures for Conducting Probabilistic Safety Assessment of Nuclear Power Plants (Level 1). IAEA Safety Series. No. 50-P-4. 175 p.

IAEA 1998. Collection and classification of human reliability data for use in probabilistic safety assessments – final report of a co-ordinated research programme 1995–1998. International Atomic Energy Agency, Vienna, IAEA-TECDOC-1048. 22 p.

IAEA. 2000. Probabilistic safety assessments of nuclear power plants for low power and shutdown modes. International Atomic Energy Agency, Vienna, IAEA-TECDOC-1144. 60 p.

IEC. 1990. International electrotechnical vocabulary, chapter 191: ”Dependability and quality of service”. International Electrotechnical Commission, IEC50(191).

Illman, L., Isaksson, J., Makkonen, L., Vaurio, J. K. & Vuorio, U. 1986. Human Reliability Analysis in Loviisa Probabilistic Safety Analysis. SRE Scandinavia Symposium, Espoo, Finland, October 1986. 12 p.

Jae, M. & Apostolakis, G. 1992. The use of influence diagrams for evaluating severe accident management strategies. Nuclear Technology 99, pp. 142–157.

Julius, J., Jorgenson, E., Parry, G. W. & Mosleh, A. M. 1995. A procedure for the analysis of errors of commission in a probabilistic safety assessment of a nuclear power plant at full power. Reliability Engineering and System Safety 50, pp. 189–201.

Kahnemann, D. & Tversky, A. 1979. Prospect Theory. An analysis of decision under risk. Econometrica 47, pp. 263–291.

Kaplan, S. 1992. ‘Expert information’ versus ‘expert opinions’. Another approach to the problem of eliciting/combining/using expert knowledge in PRA. Reliability Engineering and System Safety 35, pp. 61–72.

Kattainen, M. & Vaurio, J. 1999. Human reliability assessment in Loviisa NPP refuelling outage. In: Modarres, M. (ed.). Proceedings of PSA ’99, International Topical Meeting on Probabilistic Safety Assessment. American Nuclear Society, LA Grange Park, Illinois, USA. Pp. 1354–1361.

Keeney, R. & Raiffa, H. 1976. Decisions with Multiple Objectives: Preferences and Value Trade-Offs. John Wiley & Sons. 577 p.

Kim, J. & Jung, W. 1999. Proposal of performance influencing factors for the assessment of human error under accident management situations. In: Modarres, M. (ed.). Proceedings of PSA ’99, International Topical Meeting on Probabilistic Safety Assessment. American Nuclear Society, LA Grange Park, Illinois USA. Pp. 1119–1124.

Klein, G. 1998. Sources of Power: how people make decisions. The MIT Press. 330 p.

Laakso, K., Pyy, P. & Reiman, L. 1998. Human errors related to maintenance and modifications. Finnish Radiation protection Authority, STUK-YTO-TR 139. 42 p.

Macwan, A. & Mosleh, A. 1994. A Methodology for Modelling Operator Errors of Commission in Probabilistic Risk Assessment. Reliability, Engineering and Systems Safety, 45, pp. 139–157.

McCullagh, P. & Nelder, J.A. 1989. Generalized linear models. Chapman & Hall. Second edition. 506 p.

Moieni, P., Parry G. & Spurgin, A. 1989. A human reliability analysis approach using measurements for individual plant examination. NUS-5191, EPRI, USA. 61 p. + app. 12 p.

Morris, I. E., Walker, T. G., Findlay, C. S. & Cochrane, E. A. 1998. Control of maintenance errors. Safety and reliability, Proceedings of ESREL'98 Conference, Trondheim, Norway. Balkema Publishers, Rotterdam, Netherlands. Pp. 281–285.

Mosleh, A. & Apostolakis, G. 1984. Models for the Use of Expert Opinions. In: Waller, R. A. & Covello, V. T. (eds.). Low-Probability, High-Consequence Risk Analysis, Plenum Press, NY. Pp. 107-124.

Mosneron-Dupin, F., Reer, B., Heslinga, G., Sträter, O., Gerdes, V., Saliou, G. & Ullwer, W. 1997. Reliability Engineering and System Safety 58, pp. 249–274.

Neumann, J. von & Morgenstern, O. 1944. Theory of Games and Economic Behaviour. Princeton N.J., Princeton University Press. 641 p.

Norros, L. & Nuutinen, M. 1999. Contextual analysis of the nuclear power plant operators' utilisation of a disturbance management system. In: Hoc, J.M. et al. Proceedings of CSPAPC'99 Conference, Villeneuve d'Asq, France. Presses Universitaires de Valenciennes. Pp. 87–92.

Norros, L. & Sammatti, P. 1986. Nuclear power plant operator errors during simulator training. Espoo: Technical Research Centre of Finland, VTT Tutkimuksia – Forskningsrapporter – Research Reports 446. 66 p. + app. 27 p.

NRC. 1975. Reactor safety study: An assessment of accident risks in US commercial nuclear power plants. U.S. Nuclear Regulatory Commission, Washington D.C., USA. WASH-1400-MR, NUREG-75/014.

NRC. 1990. Accident Risks: An assessment for five US nuclear power plants, Final summary report, 3 volumes. U.S. Nuclear Regulatory Commission, Washington D.C., USA. NUREG-1150.

Oconee. 1984. A Probabilistic Risk Assessment of Oconee Unit 3. Nuclear Safety Analysis Center, Palo Alto, California, USA. NSAC/60.

O'Hara, J., Brown, W., Hallbert, B., Skraaning, G., Persensky, J. & Wachtel, J. 1998. An Experimental Evaluation of Alarm Processing and Display Characteristics. Enlarged Halden Programme Group meeting. HPR-350/13.

Orasanu, J. & Connolly, T. 1993. The reinvention of decision making. In: Klein, G., Orasanu, J., Calderwood, R. & Zsambok, C.E. Decision making in action: Models and Methods. Ablex Publishing Corporation, Norwood, New Jersey. pp. 3–21.

Otway, H. & Winterfeldt, O. von 1992. Expert judgement in risk analysis and management: Process, context and pitfalls. Risk Analysis 12(1).

Parry, G. 1995. Suggestions for an improved HRA method for use in Probabilistic Safety Assessment. Reliability Engineering and System Safety 49, pp. 1–12.

Parry, G. W., Bley, D. E., Cooper, S. E., Wreathall, J., Luckas, W. J., Taylor, J. H., Thompson, C. M. & Ramey-Smith, A. M. 1996. A process for application of ATHEANA – A new HRA method. In: Probabilistic Safety Assessment PSA '96, September 21 – October 3, 1996, Park City, Utah, USA. ANS, La Grange Park, USA, pp. 671–677.

Philips, L. D., Humphreys, P.& Embrey, D. E. 1987. A socio-technical approach to assessing human reliability. Technical report 83-4. London School of Economics and Political Science, London.

Potash, L. M., Stewart, M., Dietz, P. E., Lewis, C. M. & Dougherty, E. M. Jr. 1981. Experience in integrating the operator contributions in the PSA in actual operating plants. Proceedings of the ANS/ENS Topical Meeting on Probabilistic Risk Assessment, New York. Pp. 1054–1063.

Poucet, A. 1988. Survey of Methods Used to Assess Human reliability in the Human Factors reliability Benchmark Exercise. Reliability Engineering & System Safety, 22, pp. 257–268.

Procaccia, H. (ed.). 1995. Guidebook on the Effective Use of Safety and Reliability Data. SFER Publisher, Paris. ESReDA Series on Statistics, No, 2. Pp. 103–123, 149–153 and 171–177.

Pulkkinen, U. 1994. Statistical Models for Expert Judgement and Wear Prediction. VTT Publications 181. Espoo: Technical Research Centre of Finland. 65 p.+ app. 80 p.

Pulkkinen, U. & Holmberg, J. 1997. A method for using expert judgement in PSA. Finnish Centre for Radiation and Nuclear Safety, Helsinki. Report STUK-YTO-TR 129. 32 p.

Pyy, P. 1999. Human reliability in severe accident management. In: Modarres, M. (ed.). Proceedings of PSA '99, International Topical Meeting on Probabilistic Safety Assessment. American Nuclear Society, LA Grange Park, Illinois USA. Pp. 957–963.

Pyy, P. & Himanen, R. 1993. Shutdown Risk Analysis – Lessons And Views. In: Vestrucci, P, & Cox, T. (eds.). Fourth SRA European Conference, Rome, October 1993. 6 p.

Ramey-Smith, A. 1998. A discussion of new generation HRA techniques, Introductory remarks. In: Mosleh, A. & Bari R. (eds.). Proceedings of an international conference on probabilistic safety assessment and management, New York, September 1998. Springer Verlag. Pp. 1695–1696.

Rasmussen, J. 1979. On the Structure of Knowledge – A Morphology of Mental Models in A Man-Machine Context. Risö National Laboratories, Risö-M-2192, Roskilde, Denmark. 49 p.

Reason, J. 1990. Human error. Cambridge University Press. 302 p.

Reiman, L. 1994. Expert judgment in analysis of human and organizational behaviour at nuclear power plants. STUK-A118, Helsinki. 226 p.

Samanta, P. & Mitra, S. P. 1981. Modeling of multiple sequential failures during testing, maintenance and calibration. U.S. Nuclear Regulatory Commission, NUREG/CR-2211. 69 p.

Samanta, P. K., O'Brien, J. M. & Morrison, H. W. 1985. Multiple-sequential failure model: Evaluation of and procedures for human error dependency. NUREG/CR-3637. 115 p.

Savage, L. 1972. The Foundations of Statistics. Dover Publications. 310 p.

Schmaltz, H. 1999. Reliability based decision making in SWR 1000 development. In: Schuëller, G. & Kafka, P. Safety and Reliability, Proceedings of ESREL '99 Conference, Garching, Germany, September 1999. Balkema Publishers, Rotterdam. Pp. 229–234.

Spurgin, A., Bareith, A., Kouzmina, I., Baumont, G. & Smoutnev, V. 1999. Developments in the decision tree methodology. In: Modarres, M. (ed.). Proceedings of PSA '99, International Topical Meeting on Probabilistic Safety Assessment. American Nuclear Society, LA Grange Park, Illinois USA. Pp. 861–868.

Sträter, O. 1996. Assessment of cognitive errors and organisational aspects based on evaluation of plant experience. In: Proceedings of the International Topical Meeting on PSA 1996, UTAH, USA. Pp. 245–252.

Sträter, O. & Zander, R. M. 1998. Approaches to more realistic risk assessment of shutdown states. In: Balfanz, H. P. (ed.). Proceedings of Reliability Data Collection Workshop, Budapest, Hungary, April 1998. OECD, Nuclear Energy Agency, Nuclear Safety, NEA/CSNI/R(98)10. Pp. 236–246.

Sträter, O. & Reer, B. 1999. A comparison of the applications of the CAHR method to the evaluation of PWR and BWR events and some implications for the methodological development of HRA. In: Modarres, M. (ed.). Proceedings of PSA'99 – International Topical Meeting on Probabilistic Safety Assessment. American Nuclear Society, La Grange Park, Illinois, USA. Pp. 869–875.

Svenson, O. 1989. On expert judgments in safety analyzes in the process industry. Reliability Engineering and System Safety 25, pp. 219–256.

Svenson, O. 1998. A decision theoretic approach to an accident sequence: when feedwater and auxiliary feedwater fail in a nuclear power plant. Reliability Engineering and System Safety 25, pp. 243–252.

Swain, A. 1963. A method for performing a human factors reliability analysis. Monograph SCR-685, Sandia National Laboratories, Albuquerque, NM, USA.

Swain, A. D. 1987. Accident Sequence Evaluation Program Human Reliability Analysis Procedure. NUREG/CR-4772. 104 p. + app. 18 p.

Swain, A. D. 1990. Human reliability Analysis: Need, Status, Trends and Limitations. Reliability Engineering and Systems Safety 29, pp. 301–313.

Swain, A. D. & Guttmann, H. E. 1983. Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications. NUREG/CR-1278, Sandia National Laboratories, USA. 554 p.

Topmiller, D. A., Eckel, J. S. & Kozinsky, E. J. 1982. Human reliability data bank for nuclear power plant operations, Vol.1; A review of existing human reliability data banks. NUREG/CR-2744, US NRC, Washington, DC.

Torgerson, W. S. 1958. Theory and methods of scaling. John Wiley & Sons.

Tversky, A. & Kahneman, D. 1974. Judgment under uncertainty: Heuristics and Biases. Science 185, pp. 1124–1131.

Vaurio, J. K. 1999. Modelling and quantification of testing, maintenance and calibration errors in system analysis and risk assessment. I: Schuëller, G. & Kafka, P. Safety and Reliability, Proceedings of ESREL ’99 Conference, Garching, Germany, September 1999. Balkema Publishers, Rotterdam. Pp. 663–668.

Vaurio, J. K. & Vuorio, U. 1991. Human reliability assessment of Loviisa 1 PSA. In: Apostolakis, G. (ed.). Proceedings of PSAM, Probabilistic Safety Assessment and Management, Feb 4–7, 1991, Beverly Hills, California, USA. Vol. 2. Elsevier Applied Science Publishers. Pp. 841–846.

Vuorio, U. & Vaurio, J. K. 1987. Advanced human reliability analysis methodology and applications. Proc. PSA’87, International Conference on Probabilistic Safety Assessment and Risk Management, Zürich, Aug.30 – Sept 4, 1987. Verlag TUV Rheinland, Köln. Pp. 104–109.

Vestrucci, P. 1989. Assessing crew response probability for a sequence of actions with an overall time constraint. Risk Analysis 9(1), pp. 37–41.

Williams, J. C. 1988. A data-based method for assessing and reducing human error to improve operational performance. In: Hagen, E. W. (ed). Proceedings of IEEE Fourth Conference on Human Factors in Power Plants, Monterey, California, June 5–9, 1988. Pp. 436–450.

Winterfeldt, D. von & Edwards, W. 1986. Decision Analysis and Behavioral Research. Cambridge University Press, Cambridge, England.

Woods, D., Roth, E. & Pople, H. 1988. Modeling human intention formation for human reliability assessment. Reliability Engineering and System Safety 22, pp. 169–200.

Wreathall, J., Fragola, J., Appignani, P., Burlile, G. & Shen, Y. 1990. The development and evaluation of programmatic performance indicators associated with nuclear power plants. NUREG/CR-5436. Vol. 1. United States Nuclear regulatory Commission, May 1990.

Appendices of this publication are not included in the PDF version. Please order the printed version to get the complete publication (http://otatrip.hut.fi/vtt/jure/index.html)

Published by

Vuorimiehentie 5, P.O.Box 2000, FIN-02044 VTT, Finland
Phone internat. +358 9 4561
Fax +358 9 456 4374

Series title, number and report code of publication

VTT Publications 422
VTT–PUBS–422

Author(s)
Pyy, Pekka

Title

Human reliability analysis methods for probabilistic safety assessment

Abstract

Human reliability analysis (HRA) of a probabilistic safety assessment (PSA) includes identifying human actions from safety point of view, modelling the most important of them in PSA models, and assessing their probabilities. As manifested by many incidents and studies, human actions may have both positive and negative effect on safety and economy. Human reliability analysis is one of the areas of probabilistic safety assessment (PSA) that has direct applications outside the nuclear industry.

The thesis focuses upon developments in human reliability analysis methods and data. The aim is to support PSA by extending the applicability of HRA. The thesis consists of six publications and a summary. The summary includes general considerations and a discussion about human actions in the nuclear power plant (NPP) environment. A condensed discussion about the results of the attached publications is then given, including new development in methods and data. At the end of the summary part, the contribution of the publications to good practice in HRA is presented.

In the publications, studies based on the collection of data on maintenance-related failures, simulator runs and expert judgement are presented in order to extend the human reliability analysis database. Furthermore, methodological frameworks are presented to perform a comprehensive HRA, including shutdown conditions, to study reliability of decision making, and to study the effects of wrong human actions. In the last publication, an interdisciplinary approach to analysing human decision making is presented. The publications also include practical applications of the presented methodological frameworks.

Keywords
human reliability analysis, HRA, probabilistic safety assessment, human factors, decision making, expert judgement, simulator studies

Activity unit
VTT Automation, Industrial Automation, Tekniikantie 12, P.O.Box 1301, FIN–02044 VTT, Finland

ISBN
951–38–5585–6 (soft back ed.)
951–38–5586–4 (URL: http://www.inf.vtt.fi/pdf/)

Project number

Date	Language	Pages	Price
November 2000	English	63 p. + app. 64 p.	C

Name of project

Commissioned by

Series title and ISSN
VTT Publications
1235–0621 (soft back ed.)
1455–0849 (URL: http://www.inf.vtt.fi/pdf/)

Sold by
VTT Information Service
P.O.Box 2000, FIN–02044 VTT, Finland
Phone internat. +358 9 456 4404
Fax +358 9 456 4374