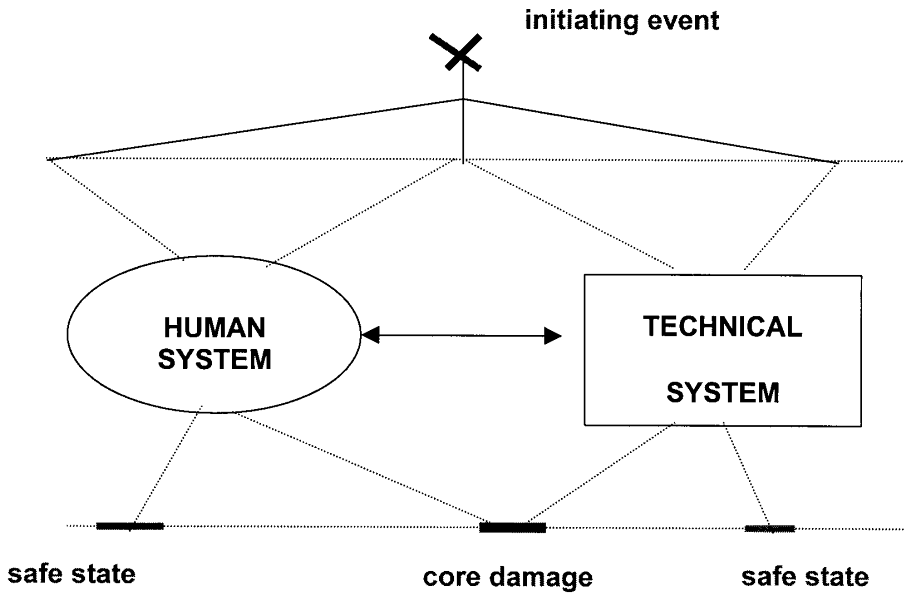
NKS/RAK-1(97)R11
ISBN 87-7893-047-2

Integrated Sequence Analysis

Kjell Andersson[1] and Pekka Pyy[2]

February 1998



[1] Karinta-Konsult HB
[2] Technical Research Centre of Finland (VTT)

Informationsservice, Risø, 1998

NKS/RAK-1(97)R11
ISBN 87-7893-047-2

Rapporten er udgivet af:
NKS-sekretariatet
Bygning 100
Postboks 49
DK-4000 Roskilde

Tlf. +45 4677 4045
Fax +45 4677 4046
E-mail annette.lemmens@risoe.dk
http://www.nks.org

NKS/RAK-1

SUBPROJECT 3

INTEGRATED SEQUENCE ANALYSIS

FINAL REPORT

Kjell Andersson[1] and Pekka Pyy[2]

February 1998

---

[1] **Karinta-Konsult HB**
[2] **Technical Research Centre of Finland (VTT)**

SUMMARY

The NKS/RAK subproject 3 ‘integrated sequence analysis’ (ISA) was formulated with the overall objective to develop and to test integrated methodologies in order to evaluate event sequences with significant human action contribution. The term ‘methodology’ denotes not only technical tools but also methods for integration of different scientific disciplines.

In this report, we first discuss the background of ISA and the surveys made to map methods in different application fields, such as man machine system simulation software, human reliability analysis (HRA) and expert judgement. Specific event sequences were, after the surveys, selected for application and testing of a number of ISA methods. The event sequences discussed in the report were cold overpressure of BWR, shutdown LOCA of BWR, steam generator tube rupture of a PWR and BWR disturbed signal view in the control room after an external event. Different teams analysed these sequences by using different ISA and HRA methods.

Two kinds of results were obtained from the ISA project: sequence specific and more general findings. The sequence specific results are discussed together with each sequence description. The general lessons are discussed under a separate chapter by using comparisons of different case studies. These lessons include areas ranging from plant safety management (design, procedures, instrumentation, operations, maintenance and safety practices) to methodological findings (ISA methodology, PSA, HRA, physical analyses, behavioural analyses and uncertainty assessment). Finally follows a discussion about the project and conclusions are presented.

An interdisciplinary study of complex phenomena is a natural way to produce valuable and innovative results. This project came up with structured ways to perform ISA and managed to apply them in practice. The project also highlighted some areas where more work is needed. In the HRA work, development is required for the use of simulators and expert judgement as data sources. On the modelling side, development is required in more dynamic methods and software tools. In safety studies, more emphasis should be put to instrumentation, shutdown conditions and cases including widely distributed human actions.

FOREWORD

The NKS/RAK-1 project forms a part of a four-year nuclear research program (1994-1997) in the Nordic countries, the NKS Programme. The NKS is a Nordic Committee for Safety Research with members from authorities, research organisations and enterprises in the nuclear field, which formulates and implements co-operative research programs with participation from the five Nordic countries. The programs are financed partly by NKS and partly by national bodies. To date, a total of five four year research program cycles have been completed in areas such as human factors and human reliability, nuclear safety analysis, materials research, probabilistic safety assessment (PSA), severe accident management. Each research program has addressed current nuclear safety issues, prepared topical state-of-the-art reviews, and developed strategies to promote proactive plant safety management.

This report summarises results from one of the topic areas (Integrated Sequence Analysis) in NKS/RAK-1. The entire study is summarised in the main report (Andersson, 1998).

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1. Scope and objectives

The general objective of the NKS/RAK-1 project was to explore strategies for reactor safety. On a more concrete level the project aims were to investigate and evaluate the safety work, to increase realism and reliability of safety analysis and to increase the safety of nuclear installations in selected research areas.

RAK-1 consisted of five sub-projects. The sub-projects were: review of safety work in nuclear installations, analysis of LOCA frequencies, integrated sequence analysis, maintenance strategies and safety importance of plant modernisation. The sub-projects with their research themes are presented in Table1.

Table 1. Subprojects of NKS/RAK-1

SUBPROJECT	**THEME**	**RESEARCH PROBLEM**
RAK-1.1	Survey of safety work in nuclear installations	How can we assess the suitability and effectiveness of the safety work ?
RAK-1.2	LOCA frequencies	Can we go improve WASH-1400 values and which are the LOCA risk dominating mechanisms?
RAK-1.3	Integrated sequence analysis	How should complex event sequences be analysed with new approaches integrating different disciplines?
RAK-1.4	Maintenance strategies	How can one optimise maintenance and testing?
RAK-1.5	Plant modernisation	How can we reasonably meet up with modern safety standards?

The NKS/RAK-1.3 project was formulated with the overall objective to develop and test integrated methodologies to evaluate event sequences. The term ‘methodology’ denotes not only technical tools but also methods for integration of different scientific disciplines. Integrated sequence analysis (ISA) is here defined as event analysis with active participation from different disciplines such as reliability engineering and PSA (probabilistic safety analysis), thermohydraulics and reactor physics (mostly deterministic analysis), material studies (deterministic) and psychology (mostly descriptive).

ISA is not restricted to PSA world, although the application studies discussed in this report also present probabilistic results. The acronym HRA (human reliability analysis) is used in the following to denote both probabilistic and non-probabilistic methods to study human behaviour in system contexts, where high reliability of actions is essential. We believe that more integrated and more dynamic methods are needed to analyse event sequences relevant for HRA.

The report is organised so that Chapter 2 explains the background of the ISA project. Chapter 3 presents the surveys made at the first part of the project providing an overview of methods used and methods being developed within and outside the Nordic countries. Specific event sequences were, thereafter, selected for application and testing of a limited number of methods. These application studies are presented in Chapter 4. In Chapters 5 and 6 we discuss the teachings of these case studies and more generally ISA methodology. Finally, in Chapter 7 we make conclusions about ISA.

2. Background

Today the PSA methodology has been developed to a stage where it is systematically used to evaluate reactor safety and to guide safety-improving measures. The structure of the PSA event trees and the associated success criteria are supported by deterministic analyses. Methods have been developed for human reliability analysis. They are used to support PSA with the factors that influence human reliability (performance shaping factors) and data on probabilities for human error. Human failure probabilities are often important parameters in PSA.

However, the probability estimates for human failure events often vary considerably (e.g. Hirschberg et al. 1990, Poucet 1990) and their basis is in many cases vague. The completeness problem of PSA is also well recognised, especially with respect to human error. The causes of human failure are often very complex and require consideration of man, technology, and organisation as a whole. Another problem with PSA, and the supporting HRA, is its limited capacity to describe the dynamic evolution of events. The event evolution between an initiating event and a number of possible end states can be very difficult to analyse due to complex interactions between the technical process system and the human / organisational system, as show in Figure 1.

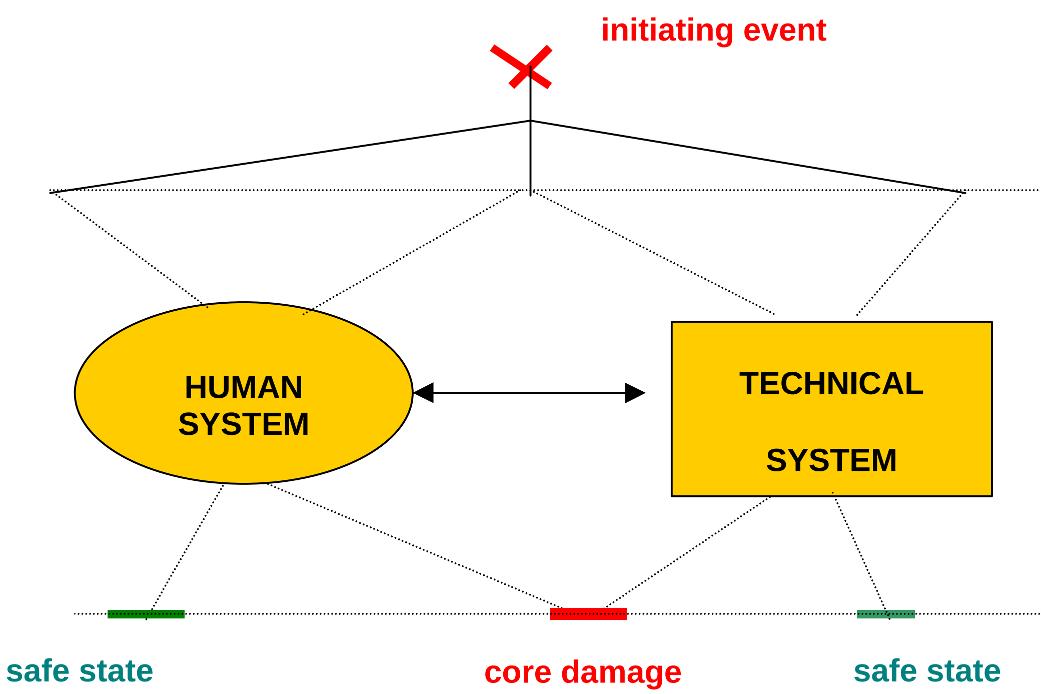


Figure 1: Event sequences are complex interactions between the human and the technical system.

It is recognised that further development is needed to develop existing methodologies for safety analysis into more fully integrated approaches to the interaction between human and technological systems.

Recently, development has taken place in several HRA related areas. For example, more advanced cognitive models are being developed (e.g. Hollnagel 1998, Dang 1996), simulators are used to improve the database for human failure (IPSN 1990, Pyy&Himanen 1996), and innovative approaches for integration and dynamics are being developed (see e.g. Izquierdo & Sanchez-Perea 1994).

NKS/RAK-1.3 project was conducted with the overall objective to develop and test integrated methodologies to evaluate event sequences. In the following Chapters, we extend the discussion of the potential problems and shortcomings of HRA to the whole field of integrated analysis. ISA should touch upon the analysis of complex systems and event sequences as whole with contribution from many different scientific disciplines.

3. Methodological Surveys

Three methodological surveys were carried out at the outset of the ISA project to map the existing methods and needs for development. The first one of them concentrated upon man-machine system simulation. The second survey presented recent developments in HRA approaches that did not explicitly use man machine system simulation. Furthermore, during the project, a survey was performed on available methods for expert judgement elicitation and combination.

3.1 Survey on man machine system simulation methods

The first methodological survey (Hollnagel, 1995), carried out at the outset of the ISA project, concentrated upon man-machine system simulation. The objectives of the study were to present principles for dynamic event analysis (joint system simulation), to survey and characterise the main existing systems, and to recommend concepts and techniques in relation to the aims of the NKS/RAK-1 project.

The report (Hollnagel, 1995) saw dynamic simulation as appropriate since human actions may change the configuration of the system, humans respond to the current situation and humans do not only react, but also do things proactively in anticipation of future events. The study included details (e.g. process and operator model) of seven man-machine system simulation tools: CAMEO, CSE, COSIMO, MIDAS, OASYS, SRG and SYBORG.

To summarise the survey, the seven systems are characterised in Table 2 by using three criteria and by their initial purpose. The three last columns of Table 2 describe the criteria: degree of relevance to PSA/HRA, how flexible the system is to be adapted in another application, and how mature its development is.

Table 2. Summary of surveyed joint system simulations (Hollnagel, 1995).

Name	Purpose	PSA / HRA relevance	Flexibility	Maturity
CAMEO	Analysis of human error mechanisms	Medium	Low	Low
CSE	Operator modeling for PSA, focusing on commissions.	High	Low	High
COSIMO	Simulation of operator cognition and management of complexity	Medium	Low	Medium
MIDAS	Predictive model for MMI design, emphasis on ergonomics	Medium	Medium	High
OASYS	MMI design support tool covering whole life-cycle	Low	Low (?)	Low (?)
SRG	General tool to support joint system simulation	Medium	High	High
SYBORG	Analysis of team communication and performance	Low	Low	Low

As Table 2 shows, none of the systems are in a completely ready state to be used for dynamic sequence analysis. Some of the systems are relevant for PSA, and one has been built with PSA/HRA in mind; others have an acceptable degree of flexibility, although this is no indication of the amount of effort it actually will take to reconfigure them; and some are fully developed systems that are safely beyond the prototype stage. Unfortunately, there is not one of them that possess all the virtues at the same time.

The methodological study concluded that joint system simulation for integrated sequence analysis offers some obvious advantages. Primarily, it is an effective way to overcome the fundamental limitation of static, manual analyses. A joint system simulation does not require the elaboration of an explicit event tree, but uses instead a specification of initial conditions and likely events, described, for example by their triggering conditions. This means that the ensuing analysis is not limited by the possibilities that have been included in the event tree, although it is limited by other things, cf. below. A joint system simulation can be used not only for sequence analysis, but will also have applications for design evaluation, training, etc. It may also serve as a vehicle for a so-called second generation, i.e. further developed, HRA with proper consideration of human performance and probability calculus.

A problem with man machine system simulation is that the quality of the output from a joint man machine system simulation depends on the quality of the constituent models. Developing a joint system simulation, where the human and the system functions are simulated in a coupled manner, requires a substantial amount of work and financial resources in specifying the knowledge needed by the two models and the interface between them. Finally, one must realize that the developments of techniques for joint system simulation still are at an early stage.

As a consequence of the survey (Hollnagel, 1995), the following recommendations were made. First, integrated sequence analyzes should be dynamic rather than static. Second, the use of joint system simulations is preferable to the use of dynamic event trees i.e. event trees with ramifications taking into account the current system state. The reason is that a dynamic event tree does not clearly separate process events and operator events, since they both are represented as nodes in the event tree. Third, scenarios, i.e. event sequences with changing information context in time, should be considered as an alternative to event trees. A scenario description is also more meaningful for considering man machine interface (MMI) than an event tree is. Cognitive models generally relate to a context rather than to an event sequence.

Fourth, efforts should be spent on defining the principles of modelling rather than of running and controlling the joint system simulation. The problems are in developing the models and in defining interfaces, for example the knowledge or assumptions that must be represented in the system. Finally, it is necessary to develop robust principles for operator cognitive modelling. Even if it turns out to be impossible to implement an actual operator model, the detailed description of the principles may enable a simple off-line simulation.

In the context of man machine system simulation, it is also necessary to mention the Computerised Accident Management Support, CAMS, developed by OECD Halden Reactor Project (Fantoni et al, 1995). The system is a prototype of a software package to support operators and organisations in decision making during serious accidents in a nuclear power plant. CAMS is planned to consist of several modules working together as an entity: data acquisition, plant database, signal validation, tracking simulator, predictive simulator, strategy generator, critical function monitor, man-machine interface, state identification, probabilistic safety assessment and system manager. Thus, CAMS could be used to complete man machine system simulation by bringing in several other options.

3.2 Survey on latest developments in HRA methods

3.2.1 State of art in HRA

The conventional HRA analysis includes the following phases: (1) identification of human interactions, (2) modelling of interactions as tasks and (3) an assessment of error probabilities in the performance of tasks (Hannaman & Spurgin, 1984). HRA begins with a task analysis of important human interactions. This part is usually connected to fault and event tree analyzes so that human interactions are inputs or model components to fault and event tree models. Other factors such as design and organisation appear as secondary influences embedded in the models, if at all. The modelling phase is followed by the probability assessment in an integrated manner.

The existing human reliability models may be divided into timing focused ones, time independent ones and their combinations (hybrid models). Examples of timing focused models are Swains TRC (Swain & Guttman, 1983), Operator Action Tree (OAT, Hall et.al., 1982) and Human Cognitive Reliability Model (HCR, Hannaman et al., 1984). HCR explicitly models how performance shaping factors (PSFs) affect the reliability. Another well-structured model that explicitly shows what PSFs mean is Embrey's Success Likelihood Index Method, SLIM-MAUD (Embrey et al., 1984). The model is based on multi-attribute value function decomposition.

All these models were developed for post initiating event (IE) HRA purposes. Especially, an effort has been directed towards the human diagnosis reliability assessment.

The HRA development work for manual activities and maintenance has been small when compared to post IE diagnostic reliability assessment. A.D. Swain presented a framework analogous to fault trees to decompose and model pre-IE human actions including error recovery (Swain & Guttman, 1983). Similarly, models have been created for maintenance action dependence (Samanta et al., 1985) and simulation (Siegel, 1984).

Due to lack of data, expert judgement, simulations and laboratory tests are relied on in probability assessments. However, for example expert judgement may be used in many ways — it may appear as direct probability assessment of failure probability or experts may be asked to give assessments about HRA model parameters.

Cognitive models have been created to cope with the psychologists' requirements concerning HRA validity (See e.g. Cacciabue 1992 and Hollnagel 1996). The ATHEANA method (Parry et al. 1996) highlights situational factors that may considerably impair human performance by discussing so-called error forcing contexts. INTENT (Gertman et al. 1992) provides a suggestion on how to assess probabilities of decision (intentional) errors and HITLINE (Macwan & Mosleh, 1994) is a probabilistic joint system simulation model, including errors of commission.

3.2.2 HRA methodological survey

The purpose of the second methodological survey of NKS/RAK-1.3 (Kahlbom & Holmgren, 1995) was to compile recently developed HRA methods and to propose some of these methodologies for use in the sequence analysis task. Mainly, non-dynamic HRA methodologies were included in the work.

The survey considered information in books, journals, and several databases and found more than 200 references. However, most of the new methods were basically dynamic or cognitive models. For the rest, enhancements concerning the treatment of psychological and cognitive behaviour in already well established methodologies were many. Those methods discussed in the study are the Enhancement of SLIM-MAUD (Zamali et.al., 1992), INTENT (Gertman, 1992), COGENT (Gertman, 1993), HIET (Drouin, 1989), HITLINE (Macwan & Mosleh, 1994) and HRMS (Kirwan & James, 1989).

The methodological HRA method survey (Kahlbom & Holmgren, 1995) concluded by giving recommendations of usability of the methods in RAK-1.3. COGENT (Gertman, 1993) and HIET-EOP **(**Drouin et. al, 1989) were identified as being the best candidates among the surveyed methods in the continued work. COGENT was found to be well fitted for treatment of the cognitive aspects of human error. HIET, on the other hand was found to be better for situations which to a large extent are emergency operating procedure (EOP) driven. These methods were also applied in the analysis of different sequences, as discussed in Chapter 4.

3.3 Survey on existing expert judgment methods

The survey on existing expert judgement methods was carried out as a part of one of the case studies of the RAK-1.3. Human reliability and PSA can be seen as one of the areas, where expert judgement will always be required. In the literature, several methods and their variants to elicit and to combine expert judgements have been reported (e.g. Cooke 1991, Mosleh & Apostolakis 1984, Comer et al. 1984, Reiman 1994). Generally, all these references emphasise the importance of selection of experts, definition of the problem and proper combination of judgements (topic resolution).

The most well known expert judgement elicitation techniques are called direct elicitation and indirect elicitation. There is a host of more sophisticated and complex methods, too. They make use of betting rates, lottery tickets etc. (see e.g. van Steen & Oortman Gerlings 1989). Certain methods use scoring rules (see e.g. Cooke 1991) to determine the quality of an expert, leading to rewarding weighting factors for the judgements when they are combined. Apart from the techniques itself, also the context in which the elicitation takes place is important.

In direct elicitation, the experts are directly asked to judge values of unknown variables. This is done either in the form of point estimation or interval elicitation. In interval estimation, fractiles of the uncertainty distribution of an unknown variable are asked. Graphical tools may be used to demonstrate the given distribution and the effects of possible changes.

Paired comparisons is a form of indirect elicitation. In a paired comparison method, the experts only have to compare two cases with regard to one feature at a time. They then select the superior one with regard to that feature e.g. ‘ A is longer than B, B is longer than C, etc.’. This comparison then goes on until all the cases have been compared, which results in [n(n-1)]/2 comparisons if n is the number of cases.

The judgements of different experts are presumed independent and are, in the most generally used model of Thurstone (Torgerson 1958), combined by using the preference proportions to derive relative distances between two cases interpreted as normal distribution deviates. Other ways to use paired comparisons are e.g. the Bradley-Terry model (Bradley 1953) and Pulkkinen’s Bayesian method (Pulkkinen 1994). The advantage of paired comparisons is their simple form and straightforward calculation of the aggregated group estimate. The coherency of the individual assessments may be studied e.g. by Kendall’s coefficient of correlation. However, the easiness of elicitation is compensated by the loss of information and by assumptions concerning underlying distributions leading to vague transformations from relative into absolute scales.

Ranking and rating are other forms of indirect elicitation. In ranking, the cases are rank ordered with regard to the degree to which they satisfy an evaluated feature. If the question ‘how much longer or how more probable’ is asked, a method may be called interval rating. Saaty’s analytical hierarchy is one example of giving directly relative distances in paired comparisons (Saaty, 1980).

Combination of different judgements takes place either by using group consensus techniques or by using mathematical aggregation models. A very general way is to use both of them in sequence.

The best-known group consensus techniques are the Delphi method, the Nominal Group Technique (NGT) and the (Total) Consensus Method. In Delphi technique (e.g. Dalkey 1969), the group members remain anonymous and only receive other’s judgements as feedback. In the Nominal Group Technique (Delbecq et al. 1975), the experts interact in a limited manner. The topics to be evaluated and expert judgements are discussed in the group, and the discussion is steered by a leader in order to overcome social biases. In the total consensus method, the group has to arrive at one estimate at the end of its work. The possibilities to discuss and share information increase from Delphi to Consensus methods. The trade-off is that group influences begin to influence more and - in the worst case - even lead to distorted judgements. Delphi and NGT require an add-on mathematical combination of the individual judgements, because at the end, there normally remain deviating values.

The most common and simplest mathematical aggregation methods are arithmetical or geometric averaging of the estimates. Another possibility is to use scoring rules, discussed above, to weight different experts. In one of the techniques, the experts’ themselves score their and others weights, i.e. the proportional amount of expertise with regard to each topic to be evaluated (DeGroot, 1974). One form of these scoring rules may be based on the information and calibration of experts (Cooke, 1991). Here, information refers to the distribution the experts produce for a certain case - the narrower the distribution the more information is given. Calibration may, in this context, refer to the distance between the true and the assessed mean value - the longer the distance the poorer the calibration. There are other definitions, too.

In some cases, the aggregated distribution is equivalent to that obtained by a simple additive error model discussed by Mosleh and Apostolakis (1984). Bayesian methods for combining judgements rely on Bayes theorem and on the principle of exchangeability - if we have expert judgements given the assessed variable, we are able to compute the value of the variable given the different judgements.

The elicitation process is important in order to avoid biases. Biases are distorting factors affecting, unfortunately, both experts and common men. They may be caused by social pressures in the elicitation situation, over-reliance on own knowledge and using simple heuristics to determine the judgements. Examples of such heuristics are anchoring, i.e. adjusting stubbornly the first value only little although new evidence would say something else, and availability, i.e. experienced phenomena get larger value than they deserve (Tversky & Kahneman, 1974). Other bias types are known as base rate fallacy and overconfidence dealing with problems in probability assessment. Otway and von Winterfeldt (1992) discuss also motivational and structural biases - the first one results from assessor's dependence on the topic to be evaluated and the second to framing. For example, the probabilistic results look very different on a lognormal scale than on the linear scale. Svenson (1989) has given an overview of possible biases in ratings elicited for different HRA methods, among them HCR and SLIM.

Due to potential biases, several requirements have been set in the literature to ensure proper use of expert judgement, e.g. in (NUREG-1150, Cooke, 1991). First, only experts that have demonstrated their expertise should be selected. Then the analysis should be reproducible, accountable, subject to empirical control, neutral and fair. Here, reproducibility means that all the calculations and analyzes have to allow to be traced back to their origin and repeated. Accountability means that the values given can be traced to their source (expert). Empirical control means that the results should, in principle, allow them to be falsified (by empirical tests etc.). Neutrality means that experts should not be able to play with their judgements but instead to be encouraged to give their true assessments. Fairness requires that all experts are treated equally during the analysis, although some scoring rules and weighting procedures might classify them afterwards. Finally, the results should be internally consistent. All these requirements are also prerequisites of a sound scientific method.

4. Case studies

Four case studies were selected in RAK-1.3 sub-project for ISA in order to demonstrate evolutionary approaches to integrated sequence analysis. Originally, the idea was to use these case studies throughout the whole NKS/RAK-1, but this proved to be impractical, later on. All the case studies aimed at improved human reliability analysis.

4.1 Presentation of the case studies

Two of the case studies, large human initiated LOCA and cold overpressure events of a BWR were directly linked with shutdown PSA studies (SPSA). The third case study is a PWR steam generator tube rupture (SGTR), which involves balancing actions on both primary and secondary side of the installation. In addition, there is a risk of early radioactive release through an atmospheric relief valve on the secondary side. The fourth case study deals with a confused signal view in the control room followed by a fault in instrumentation.

Table 3. NKS/RAK-1.3 case studies with their methodological orientation and status**.**

Case study	Methodological orientation
BWR Large LOCA during shutdown (man-made)	PHASE I: Thorough task analysis + COGENT PHASE II: Use of expert judgement
Cold overpressurization of a BWR	Theoretical, decision analytic view, time dependent stochastic methods.
Steam generator tube rupture of a PWR	A semidynamic framework with emphasis on cognitive task analysis, PSA, HRA and thermohydraulics
Disturbed signal view in a BWR control room due to a CCF	Emphasis on creating a control room PSA model. Evaluation of the effect of different signal view set-ups

4.2 BWR cold overpressure

The cold pressurization accident sequence stems from potential BWR reactor tank overfilling. The reactor tank is filled with water from normal level (+4.0) m to flange level (+8.2) m at the end of shutdown sequence in order to start refuelling. The motivation is to decrease radiation doses in conjunction with pressure vessel lid dismantling and to make preparations for the reactor cavity and pool filling.

The following events may cause overfilling: a) wrong, poor or neglected measurement reading observations, b) simultaneous spurious start of high head pumps and c) decision to continue filling after +6.4 m with high head 327 pumps followed by lack of vigilance (violation of plant technical specifications).

The sequence was chosen due to many reasons. First, it had already been analysed in the plant specific Shutdown PSA. Secondly, the sequence can occur only during plant shut down, and the plant shut down PSA analyzes are interesting from both methodological and practical points of view. Thirdly, it offers possibilities to study the human reliability related questions by using simulator.

At the outset of the project, the following objectives were set: (1) development of time-dependent interface models between operators' decision making model and PSA; (2) quantification of the selected accident sequences with the model and (3) specification of a dynamic PSA model. Furthermore, a simulator exercise was to be used in model validation and in determining accident sequence probabilities.

4.2.1 VTT's dynamic ISA methodology

The thesis of VTT's approach is that probabilistic and psychological approaches complete each other and provide useful insights in the analysis of human reliability.

The VTT team generated an own approach to ISA in cases where human decisions have a major role. The outline of the approach is threefold. First, the decision context is identified and described by creating descriptions (reference models) of the investigated situation (i.e. qualitative task analysis). Secondly, the accident situation is

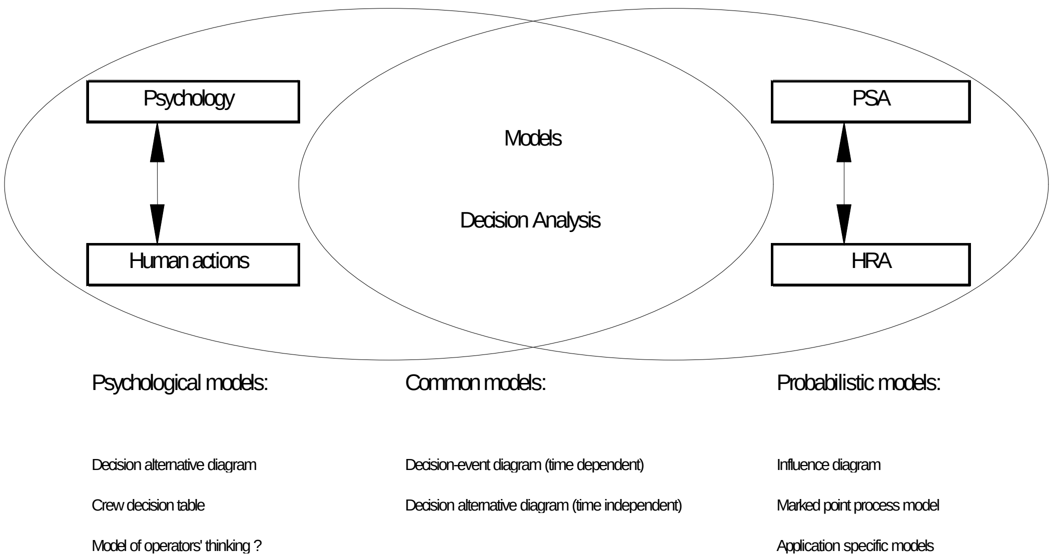


Figure 2. Overview on VTT's integrated modeling approach and models used.

modelled from the risk and reliability point of view (logical modelling). Thirdly, the operators' decision making is analysed with respect to the reference models and this information is used in the logical model.

The approach is analytical for the probabilistic use of expert judgement with normative (probabilistic) experts and substance matter experts (psychologists and process specialists). The PSA modelling and decision analytical frameworks form the integrating features of the approach, as manifested in Figure 2.

Reference models may be influence diagrams, fault and event trees, critical information matrices, decision tables, inference diagrams etc. (see Figure 2). VTT's modelling technique was based on probabilistic influence diagrams as general framework and on structured use of expert judgement (for detecting the start of an extra high head pump) and marked point process (MPP) models for detail modelling (Holmberg et al, 1996).

4.2.2 Probabilistic influence diagram and marked point process (IDMPP) approach

The probability calculus with MPP takes place by defining the intensities or hazard rates of various marks as a function of the past history of events. The intensity of an event with mark z is defined as

$$l_t(z) = P(dN_t(z) = 1|H_{t-}) / dt.$$

If the event can occur only at known time epochs, an intensity or frequency cannot be defined, but a discrete hazard measure must be used

$$d\Lambda_t(z) = P(dN_t(z) = 1|H_{t-}).$$

In our MPP approach, not only stochastic events, but also decisions, are seen as marked points. The dynamics of the system is modelled by intensities depending on the history of the system and decision making activity. MPPs are, so far, seldom reported in PSA applications.

Figure 3 presents in a graphical form the influence diagram model that we used to model the cold overpressure event.

Mathematically, Figure 3 represents the decomposition of the joint probability function

$$\mathrm{P}\{T_1, T_1', T_2, T_2', T_3, T_E, T_E', T_S, a_1, a_2, a_E\}.$$

The event of most interest, the "top-event", can be expressed as $\{T_3 < T_S\}$, which means that the pumping is stopped too late. Therefore we try to evaluate the marginal distribution of $\{T_3 < T_S\}$ over the joint probability distribution, i.e.

$$\mathrm{P}\{\text{"accident"}\} = \int \mathrm{P}\{T_3 < T_S | T_1, T_1', T_2, T_2', T_E, T_E', a_1, a_2, a_E\} \times \mathrm{dP}\{T_1, T_1', T_2, T_2', T_E, T_E', a_1, a_2, a_E\}.$$

Data for the model were collected by operator interviews and simulator runs. The data were both qualitative to validate models and for psychological analysis and quantitative. The quantitative data included e.g. observations with regard to reactor water level surveillance for MPP and expert judgement collection with regard to stopping a spuriously started auxiliary feedwater pump. In the elicitation and combination of the expert judgements, a simplified VTT methodology (e.g. Pyy & Pulkkinen, 1997) was used.

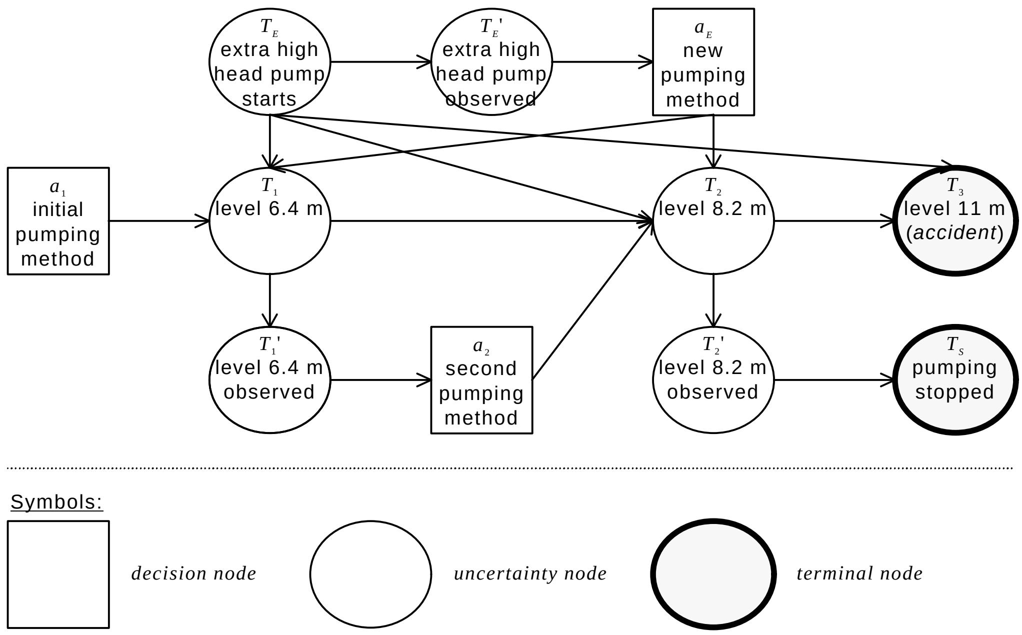


Figure 3. The influence diagram of pumping strategy selection and possible spurious start of an extra pump.

4.2.3 Psychological modeling approach

On the psychological side, a contextual and naturalistic approach to operators' decision making was applied. From the perspective of the reliability of process control activity, the operators' orientation to the situation is interesting. As an underlying factor in their interaction with the context, it contributes to their diagnostic interpretations and operational choices.

This consideration of their taking into account the possibilities and restrictions, set by the situation, makes it possible to evaluate the dynamics of their activity during the sequence. In a probabilistic decision analytic framework, this can produce information on the preferences of the personnel in decision situations, and thus, on the frequency that a certain decision option is selected. The criteria and options the operators may use in the selection of the pumping method is manifested in Table 4.

According to this approach, the way in which operators utilise available process information and co-operational possibilities manifests the coherency of the interpretation of the situation - and their ability to take into account the situation demands. It is supposed to reflect their orientation to the task performance. Critical information that the operators use to interpret the situation may be presented as the form of a table, as shown in Table 5.

Table 4. Decision table for reactor waterfilling pump selection

Criteria	Auxiliary feedwater system	Condensate system	Demineralized water + boron	Core spray system
Safety				
Way of pumping	Possibility to severe overpressure	possibility to some overpressure	no overpressure	no overpressure
Economy				
Time schedule	40 min to 6.4 m	40 min to 6.4 m, if throttled	slow, 2 h from 6.4 m to 8.2 m	less than 10 minutes
Purity of water	OK	OK	OK	not acceptable (from wet well)
Technical feasibility				
Availability	4 pumps	4 pumps, (not available if hurry in maintenance)	2 pump lines	4 pumps
Pumping capacity	22.5 kg/s	250 kg/s max.	2 x 2.5 kg/s	4 x 125 kg /s
Operational culture				
Procedures, operating orders	Legitimate at the beginning	legitimate at the beginning	legitimate after +6.4 m	not legitimate due to water source
Routines	Alternative	used, if available	slow, not preferred	

The time required to pump up to +8,2 m is dependent on the used pumping method.

Table 5. An example of the operator critical information sources and their significance.

Critical information	Source of information	Diagnostic meaning	Operational meaning
React. Level			
+4.7m,	fine and coarse level measurement (211K40X and K41X), SS5 (high level scram), light on panel PA7	high reactor level +4.7m is reached	High level scram (SS5) overridden, isolation valves do not close and pumps do not stop => enables pumping into reactor vessel
+6.4m	Measurement 211K40X and K41X (8 channels) uppermost point	uncertainty about water level increases after this point	pumping must be monitored carefully to prevent from overfilling
+8.2m	Measurement 211K424 uppermost point (1 channel) + voltage meter	flange level reached	pumping must be stopped, 211K424 is for refueling level
Estimated time	Clock, anticipation	flange level reached	pumping must be stopped

*Also other safety critical functions, e.g. pressure and residual heat removal, and their monitoring means can be taken into account in the table.

4.2.4 Analysis flow

The analysis team consisted of PSA experts, psychologists and process specialists. The integrated analysis process included common workshops, separate work meetings and individual work. In common meetings, methods and differences in discipline were discussed. Some of the topics were also discussed in NKS RAK-1 sub-project 3 workshops.

Data for the models were collected in a simulator run. After the run, the operators were debriefed and interviewed in order to consolidate the observations and to obtain more data.

4.2.5 Results and conclusions from the case study

The accident probability was calculated by a simulation model of the event sequence. In the basic case, the probability of overfilling is negligible, 3E-10 per shutdown. Given a spurious start of a high head pump within first 100 minutes $\{T_E < 100 \text{ min}\}$, the probability of overfilling / overpressurization increases to 2E-6 per shutdown. The risk increase factor of this event is over 5000, and the fractional contribution is about 90%.

The common conceptualisation of the operators' activity context contributed clearly to integration between PSA and human factors experts because 1) the often tacit presuppositions and conceptual categorisations underneath the different notions and concepts of the both research parties had to be made explicit in order to make any progress and, 2) it was easier to understand each others' views due to the possibility to refer to a concrete situation. On both sides the reference models describing the context became better as a result of the collaboration.

The simulator experiment, which is a routinely used tool of the psychological analysis and utility HRA work, turned out to be beneficial also to the probabilistic analysis.

The project could identify several improvement points with regard to instrumentation and procedures. Most of them were already implemented by the utility but not all instrumentation changes were necessarily present at the simulator.

4.3 Inadvertent opening of an isolation valve during the shutdown of a BWR

The sequence was chosen due to its importance in plant specific Shutdown PSA. The first phase of this case study included qualitative analysis of the paths leading to an inadvertent opening of an isolation valve in the shutdown cooling system (pipe diameter 250 mm) of a BWR reactor (Jacobsson, 1996). The shutdown cooling system is located below the reactor tank, and together with another disassembled valve the case results in a rather rapid reactor tank draining - time estimates vary from 30 to 60 minutes. As specific goals, creating multidisciplinary insights in the shutdown LOCA and a finding a method for shutdown specific HRA quantification were set.

4.3.1 Qualitative part of the study

During the first phase of the work, the group used COGENT (Gertman, 1993) as its modelling tool. This led to the decomposition of the event tree model into skill, rule and knowledge based human behaviour. Furthermore, the errors in these behaviour classes were divided into slips, lapses and mistakes. The group work provided very interesting practical insights such as: ergonomics and need for communication in the electrical limit testing of the isolation valve, importance of work permit handling in shutdown and the need to verify the restoration of a maintained component immediately after the maintenance.

The conclusion of the first phase of the study was, thus, that the used method was easy to use and it provided a frame under which engineers and behavioural scientists could discuss. However, the method did not provide a plausible way to probability quantification (Jacobsson, 1996). Thus, as the next step, structured expert judgement was decided to be used in order to reach probability estimates.

4.3.2 Application of expert judgment method

In an expert judgement process, there are normally three kinds of actors: decision makers, normative experts and subject matter experts. Subject matter experts where chosen from the power company specialists and they represented a wide variety of disciplines: reliability engineering, safety, operations, maintenance and psychology. The normative experts came from VTT Automation. The participants of a typical expert judgement process are described in Table 6.

Table 6. The participants of an expert judgment process

Participant	**Role**
1. Decision maker, the owner of the issue	• responsible for the decisions based on the experts' judgements • defines the resources needed in the process
2. Normative experts	• experts in expert judgement methodology • responsible for expert training, elicitation of the judgements, combination of judgements and reporting of the results • leads the expert judgement process
3. Subject matter experts	• familiar with the issue • responsible for the analysis of the issue and giving judgements on it

The phases of an expert judgement process are: 1) selection and training of experts, 2) elicitation of expert judgements, 3) modelling and combination of expert judgements, 4) sensitivity analyses, 5) discussion with and feedback from experts and 6) documentation.

In our case, we first defined the variables for the expert judgement analysis in two phases. First, the normative experts discussed with the project leader in order to define the issues for expert judgement, to agree upon the schedule and to get data from the previous analyzes. In the second phase, the variables defined preliminarily were discussed with the experts during the training session to see whether they had views about the selection. In the consequence of the discussions, the probability for causing the leakage, the time available to take balancing actions and the time available for action were selected as variables to be elicited.

The expert training was organised as a part of a common NKS/RAK-1 seminar on expert judgement and human reliability. First, expert judgement techniques, heuristics and biases in their use and human reliability were discussed. Then, the methodology suggested for the case was discussed more. The seminar ended up with the expert training session, which was directed only for the expert group. The training included further discussion about subjective probability, about properties of probability distributions, helpful hints about giving fractile assessments and about biases. Finally, ample time was given for free discussion about the case. The discussion brought up issues about the case that were then documented as boundary conditions of the analysis.

The judgement elicitation was made in two steps. First, the initial estimates for the variables were given just after the training session, in which the issues and variables were defined. In this case, the experts were asked to give their 5%-, 50%- and 95%-quantiles for the variables. After the training session, the experts were asked to make their individual analyzes about the issues and to write short reports on their analyzes. The reports were presented in the elicitation session. In their presentations, the experts were not allowed to present their quantitative estimates. The main aim of the experts presentations was to discuss and compare the experts' thinking models and approaches. After the experts presentations, the quantitative estimates were elicited from each expert individually.

The combination of the assessments took place by using VTT's Bayesian methodology (Pulkkinen & Holmberg, 1997). Used Bayesian modelling framework consists of describing the full distribution of all random variables in the model, including experts judgements, as a Bayes network. The Bayes network corresponding the model applied in this study is in Figure 4. The variable of interest is denoted by *X*. We assume that the uncertainty about the value of *X* can be represented by a Gaussian distribution, or its transformation such as lognormal or logit, with parameters μ and σ with unknown values. The uncertainty concerning the parameters is represented by non-informative prior distributions (see e.g. Gelman et al, 1995, or Box & Tiao, 1972). Experts, the number of which is *m*, are asked to express their uncertainty on *X* as selected percentiles. The expert judgements, denoted by $\boldsymbol{Y_i} = (Y_{j0.05}, Y_{j0.50}, Y_{j0.95})$, where Y_{ja} is the α-percentile given by the expert j, are related to the parameters μ and σ through a set of hidden variables $\Theta_{11,}$, Θ_{12},..., Θ_{1L},..., Θ_{mL}. These variables are assumed to be conditionally independent and identically distributed (given μ and σ) and their distributions is the similar to that of *X*. In other words, the set $\{X, \Theta_{11,}, \Theta_{12},..., \Theta_{1L},..., \Theta_{mL}\}$ consist of exchangeable random variables.

The percentiles given by expert *j* are interpreted as sample percentiles of the hidden sample of expert j. However, the values of the variables in the hidden sample $\{\Theta_{11,}, \Theta_{12},..., \Theta_{1L}\}$remain unknown, and the experts' percentiles specify this sample only partially. Thus, we may interpret the role of the hidden variables as follows: the experts have in mind a sample, of *X* e.g. based on history or on a model, of similar variables. The experts are not able to specify the sample perfectly, and, consequently, they give only some predefined percentiles of the sample distribution. Since the hidden variables depend on the parameters μ and σ, and since the experts percentiles are straightforwardly related to the hidden variables (through sample percentiles), the distribution of the parameters can be updated by using the experts' percentiles. The posterior distribution of μ and σ can be used in determination of the distribution of *X*. In practice, the posterior distributions must be determined by applying numerical methods. The Gibbs sampler (see e.g. Gelman et al, 1995) appears to be a good method for determining the posterior predictive distributions for *X*.

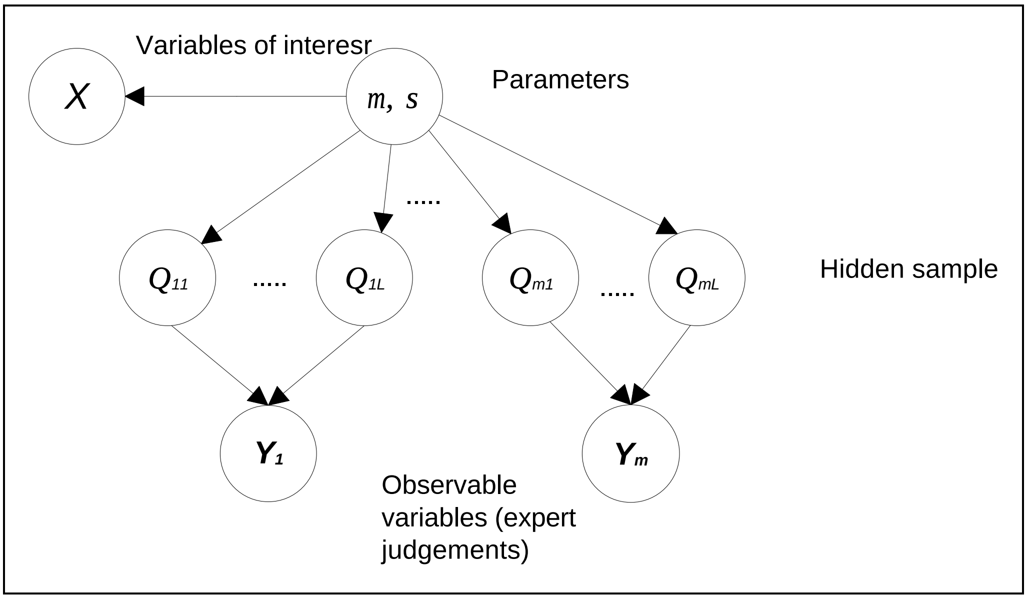


Figure 4. Bayes network for the expert judgment model, notation $\boldsymbol{Y_i} = (Y_{j0.05}, Y_{j0.50}, Y_{j0.95})$.

To compare our Bayesian approach to the direct comparison of the experts' judgements, a sensitivity analysis was performed. We also studied the effect of neglecting a single expert from the study at a time.

After the final elicitation interviews, the normative experts performed a preliminary combination of the experts' quantitative assessments and draw some preliminary conclusions with regard to their reasoning and modelling of the case. These results were, then, communicated to the experts and comments were received from them. Apart from this, a feedback session was arranged to describe the results more and get the final response from the experts about the pros and cons of the methodology and about its applicability to other cases and fields.

4.3.3 Results

The expert's estimates for time to core uncovery (T_1) first included very little uncertainty but the situation changed in the course of the analysis, since the contradictory numbers and text in different analyses were discussed. This resulted in considerably wider uncertainty bounds, as shown in Table 7.

For time taken to close the valve (T_2) some of the experts considered in the first round evaluation, whether it is even possible to enter the room to close the valve manually. This led them to overly conservative 95 % percentiles, as shown in Table 7, that then decreased in the elicitation session after they had made their own studies about the situation. On the other hand, the awareness of the experienced difficulties to remotely steer components in a shutdown conditions affected the distributions. These difficulties are due to the amount of overhaul and modifications in electrical and instrumentation systems during a refuelling outage.

Table 7. Initial and final estimates given by the experts

	Experts' *5%, 50%* and *95%* quantiles								
	Variable 1: T_1 = "Time to core uncovery", min			Variable 2: T_2 = "Time needed to balance the situation," min			Variable 3: θ = "Probability of the leakage"		
Initial estimates									
	5%	*50%*	*95%*	*5%*	*50%*	*95%*	*5%*	*50%*	*95%*
Expert A	35	40	50	5	10	15	1.0E-4	1.0E-3	1.0E-2
Expert B	35	35	35	1	15	120	1.0E-3	1.0E-2	1.0E-1
Expert C	33	35	37	3	25	180	1.0E-6	5.0E-4	1.0E-3
Expert D	25	30	60	20	30	60	1.0E-4	5.0E-3	5.0E-2
Expert E	30	45	60	5	15	60	1.0E-5	1.0E-3	1.0E-2
Final estimates									
	5%	*50%*	*95%*	*5%*	*50%*	*95%*	*5%*	*50%*	*95%*
Expert A	30	35	40	5	15	20	1.0E-6	2.0E-4	1.0E-3
Expert B	37	45	60	9	50	75	1.0E-9	1.0E-4	4.0E-4
Expert C	37	40	43	3	25	90	1.0E-7	7.5E-5	1.0E-4
Expert D	20	30	120	10	30	60	2.0E-8	2.0E-4	4.0E-2
Expert E	30	40	45	10	18	55	1.0E-6	1.0E-4	1.0E-3

The probabilistic analysis of causing the leakage included two structured models of the leakage initiation, one of them with several routes that could have generated the leakage. In addition, two experience data based quantification methods and one more philosophical discussion about probability concept and uncertainty were given.

In the analysis, the plant barriers were regarded as well functioning. On the other hand, transgressions of work permits and safety umbrellas take place in almost every refuelling outage. Wrongly timed test taking place from the valve switchgear unit dominates the other mechanisms. The risk dominance of a test taken from the plant rooms is due to the fact that it is carried out without a specific work permit. The quantitative estimates given on the second elicitation round were somewhat smaller than the first ones due to a more thorough analysis of the situation, as shown in Table 7.

As a general observation about expert's estimates, all experts changed their first judgements. Thus, we could claim that, at least, total anchoring could be avoided. The time distributions for T_1 and T_2 became closer to each other. A more thorough analysis led to the smaller probability distribution fractiles for θ. The evidence showed neither that group work had taken place, nor that the experts had intentionally arrived in lower estimates than their first guesses.

In Table 8, a summary of the combined uncertainty distributions is shown after combining the judgements by VTT's method. For variables 1 and 2, the calculation was based on lognormal transformation and for variable 3 on logit transformation. It is important to note that for variable 3, the 5 % and 50 % values are rather low but the long tail and skewness of the distribution lead to rather high mean and 95 % values.

Table 8. Summary of the combined distributions.

	The posterior means and 5%, 50% and 95% quantiles of the variables											
	Variable 1: T_1 = Time to core uncovery", min				**Variable 2: T_2 = "Time needed to balance the situation," min**				**Variable 3: θ = "Probability of the leakage"**			
	5%	*50%*	*95%*	*Mean*	*5%*	*50%*	*95%*	*Mean*	*5%*	*50%*	*95%*	*Mean*
Initial estimates	24.5	35.0	49.0	35.7	1.4	16.0	175.0	60.8	4.6E-6	1.2E-3	1.8E-1	4.2E-2
Final estimates	20.0	40.0	79.0	40.2	3.6	21.5	136.0	41.8	6.0E-9	2.6E-5	6.0E-2	3.6E-2

We determined the probability of core uncovery followed by the leakage by using Monte-Carlo simulation. The uncovery event can be presented as a combination of two events: $A_1 = \{T_2 > T_1\}$ = *" the time needed to balance the situation (T_2) is longer than the time to core uncovery" and* A_2 = *"a leakage occurs"* . Further, we assumed that the events A_1 and A_2 are independent. Thus, the probability of uncovery is calculated from

$$P(A) = P(A_1 \cdot A_2) = P(\{T_2 > T_1\})P(A_2)$$

We notice that the probability of the accident is a single number, not a random variable with a distribution. This result leans on the Bayesian interpretation of the model, and it is compatible with the "integrated uncertainty analysis" discussed by Pörn & Shen (1992). The Monte-Carlo simulation (1000 rounds) produced the expectation value 2.3E-3. In PSA uncertainty intervals are often presented for this kind of variables. In our case, "the uncertainty distribution of accident probability" is obtained by considering the probability of accident as the product of a random variable θ and the probability $P(\{T_2 > T_1\})$. The *5%* fractile of the distribution is *2.1E-9,* the median *7.8E-6,* and the *95%* fractile is *2.1E-2.* The distribution is very flat and the calculated probability (expectation value) is near the 90 % percentile. This is a feature of very skewed distributions in our case.

The sensitivity analysis with regard to importance of individual experts showed that no single expert assessment has a very strong impact on the combined distribution. This is partly caused by the fact that there are five experts; if the number of experts had been smaller the final distribution could have been dominated by an individual expert.

The approach of combining distributions by arithmetic averages has been applied e.g. in the NUREG-1150 study (1989). Thus, as a sensitivity analysis of combination method, we compared our Bayesian results with the direct mixture distributions obtained by arithmetic averages. No large differences were obtained for variables 1 and 2 but for variable 3 there was some sensitivity, as shown in Figure 5. The reason to the differences is the fact that it is not easy to fit a parametric distribution with only three fractiles. Furthermore, in our case, the experts fractiles did not always correspond well to those of lognormal or logit distributions. Generally, direct combination produced some narrower distributions. However, the numerical differences are not very large. The results for the total probability of the core upper grid uncovery would remain somewhat lower by using direct combination than those by using the Bayesian approach.

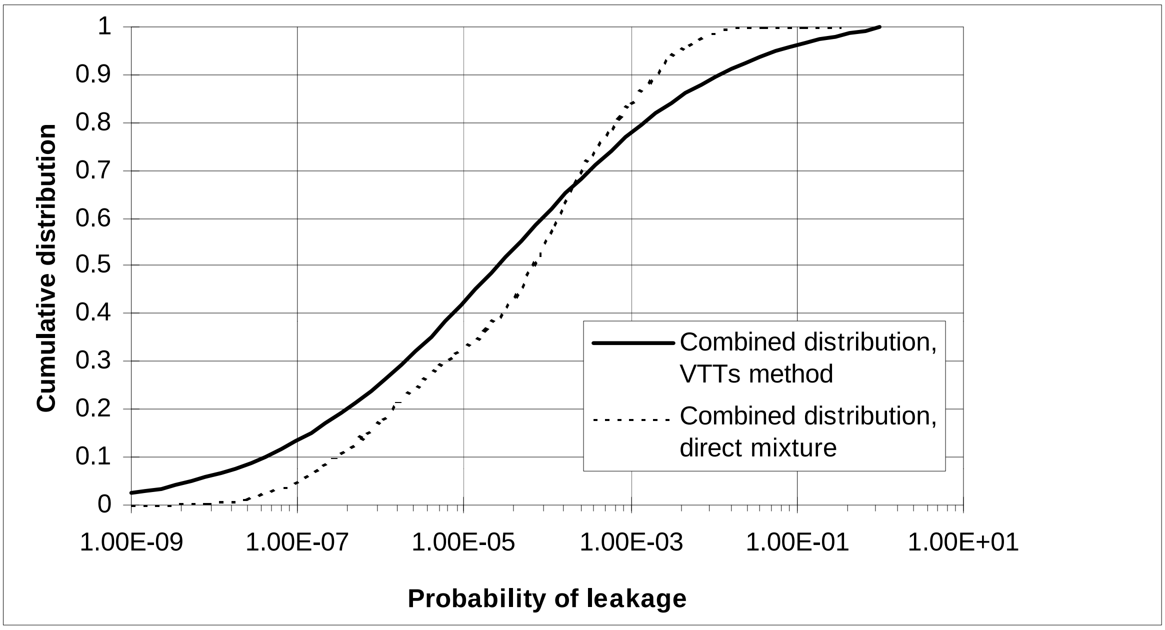


Figure 5. Comparison of combined distributions, variable 3 (θ)

4.3.4 Conclusions from the case study

The results show that the shutdown LOCA risk cannot be neglected. The simulated probability for core upper grid uncovery is relatively high. However, this does not mean the same as radioactive releases (core melt). The uncertainty related to the variables in question is high, too. Still, it is advisable to study any potential to avoid situations where irradiated fuel may uncover due to shutdown LOCA below core level.

HRA will stay among the most important application areas of expert judgement. This requires a more rigid discipline by the practitioners. Methods have to be scientifically safe and help the experts to give their judgements. The results also have to be understandable in order to form a basis for the decision making. The used method proved out to be a valuable tool for expert judgement combination and wider uses are foreseen. In addition, a careful training accompanied by expert reporting and thorough elicitation interviews is needed in order to avoid biases. By using that procedure, expert judgement forms a good completion to other data collection methods. However, it is suggested that applications to direct probability assessments are, in each case, considered with care. This is due to the fact that people cannot observe probabilities and thinking in terms of ‘lottery tickets’ or in terms of ‘bets in a race’ may be difficult.

Knowing the complexity of the probability concept, one should not ask the experts to assess "probability distributions of probabilities" but probability distributions of observable variables e.g., number of unsuccessful tasks in given a set or a given time. However, in PSA, uncertainty intervals are often presented for this kind of variables. There are, anyway, difficult interpretation problems in the concept.

The elicitation of experts’ opinions was based on *5%*, *50%* and *95%* fractiles of expert’s uncertainty about the variables under analysis. It was rather easy for the experts to give the

50% fractile (i.e. the median), but the other fractiles were more problematic. In future, an option to elicit also the maximum and minimum values for variables should be implemented into the method.

4.4 Steam generator tube rupture (SGTR)

Apart from the general goal to develop approaches to ISA, the sequence specific aims were to analyse a steam generator tube rupture of a Westinghouse type pressurized water reactor, to analyse Westinghouse EOPs by ISA, to make recommendations for improvements at site and at operator training, to benchmark simulator codes, to feedback PSA in terms of a more detailed analysis and to give further insight into uncertainties.

The methodological framework can be described as consisting of three components starting from a semi-dynamic approach for event sequence analysis, continuing with cognitive task analysis and ending up with a practical methodology for interaction between PSA and human factors methods (Andersson et al., 1996).

4.4.1 The semi-dynamic approach

The semi-dynamic approach used in the analysis of the SGTR sequence can be described as follows:

1. The analysis proceeds stepwise using the following tools: cognitive task analysis, PSA, thermohydraulic modelling, simulator runs and analysis of emergency operating procedures (EOPs). The EOPs function as the link between the different analytical tools.

2. Detailed analysis of a part of the sequence leads to a system status description with respect to process, PSA and cognitive factors. The cognitive modelling gives cognitive profiles of the emergency operating procedures with distributions of possible operator error modes. The semi-dynamic PSA analysis gives conditional probabilities at specific system states, i.e. in the interface between two EOPs.

3. Because the overall event is complicated and potentially will lead to an extensive and resource intensive analysis, it is necessary to select subsequences for further detailed analysis. These are chosen based on a brief systems description using e.g. traditional PSA/HRA methods.

4.4.2 Cognitive task analysis

A cognitive task analysis was performed for the main procedure used in SGTR (Hollnagel et.al., 1996). The analysis is based on 14 cognitive activities that are: co-ordinate, communicate, compare, diagnose, evaluate, plan, verify, execute, identify, maintain, monitor, record, regulate and scan. Furthermore, the SGTR procedure was broken down into 7 segments based on different operator goals in each segment. The segments were identification, isolation, RCS cooling, re-establishment of pressurizer level, stopping safety injection and pressure balancing. Under these topics there are, naturally, more subgoals. All the activities under these segments were classified under the basic cognitive activities. An example of this classification is given in Table 9. Similarly, different temporal behaviours of the crews e.g. in the identification phase was taken into account.

Based on the cognitive activity list, a cognitive demands profile was produced. This serves to indicate whether the task as a whole is likely to depend on a specific set of cognitive functions. The basis for constructing a cognitive demands profile is a simple model of cognition known as SMoC. The parts of the model i.e. cognitive functions, described more in (Hollnagel, 1997), are observation, interpretation, planning and execution. Each cognitive activity can then be described in terms of which of the four cognitive functions it requires. As an example, co-ordination requires planning as well as execution.

By using the SMoC functions, the activities identified in the SGTR procedure were classified. It was interesting to note that the scenario seems to place rather high cognitive demands to observation, interpretation and execution (98 activities almost evenly distributed) whereas only four activities where classified under planning. This may be due to the difficulty to identify and classify decision related activities based on procedures. Apart from the whole sequence, the cognitive profiles were generated for each scenario segment. The results showed that the cognitive demands should be at their highest in the RCS cooling phase.

Table 9: Cognitive activity list for SGTR isolation phase

Step	Event sequence description		Cognitive activity
	Goal	**Means**	
3	Ruptured SG has been isolated		
3a	*SG relief valve has been set to 79 bar*	*Set SG relief valve to 79 bar*	Execute
3b	*SG relief valve is closed*	*Check that SG relief valve is closed*	Verify
3c	*Steam line from SG to steam driven AFW pump has been closed.*	*Close steam line from SG to steam driven AFW pump.*	Execute
3d	*"Blow down" from ruptured SG is isolated.*	*Check that "Blow down" from ruptured SG is isolated.*	Verify
3e	*MSIV & bypass valves have been closed.*	*Close MSIV & bypass valves*	Execute
3f	*Steam isolation signal has been reset; supporting valves have been closed.*	*Reset steam isolation signal; close supporting valves.*	Execute
3g	*Steam dump valves are isolated.*	*Check that steam dump valves are isolated.*	Verify
3h	*FW to ruptured SG is isolated.*	*Check that FW to ruptured SG is isolated.*	Verify

Based on the principle of systematic manifestations of erroneous actions a list of potential error modes was selected. These "procedure specific" error modes are listed in Table 10 relative to the cognitive functions of the associated model.

Table 10: Procedure error classification scheme for the E-3 EOP

SmoC function	Potential error modes	
Observation errors	O1	Observation of wrong object
	O2	Wrong identification made
	O3	Observation not made (i.e., omission)
Interpretation errors	I1	Faulty diagnosis
	I2	Decision error
	I3	Delayed interpretation
Planning Errors	P1	Priority error
	P2	Inadequate plan formulated
Execution Errors	E1	Execution of wrong type performed
	E2	Action performed at wrong time
	E3	Action on wrong object
	E4	Action performed out of sequence
	E5	Action missed, not performed (i.e., omission)

The total number of occurrences for each error mode is shown Figure 6. Again, the dominating error modes are related to execution, followed by error modes related to observation and interpretation. Considering the nature of a procedure this is not very surprising. The predominant actions are of the execution type, and the error modes will necessarily match that, as in the case of cognitive actions earlier.

Finally, it is possible to define a relatively small set of Common Performance Conditions (CPC) that describe the general determinants of performance in a given context. The following CPCs were used: Adequacy of organisation, Working conditions, Adequacy of MMI and operational support, Availability of procedures / plans, Number of simultaneous goals, Available time, Execution mode, Adequacy of training and preparation.

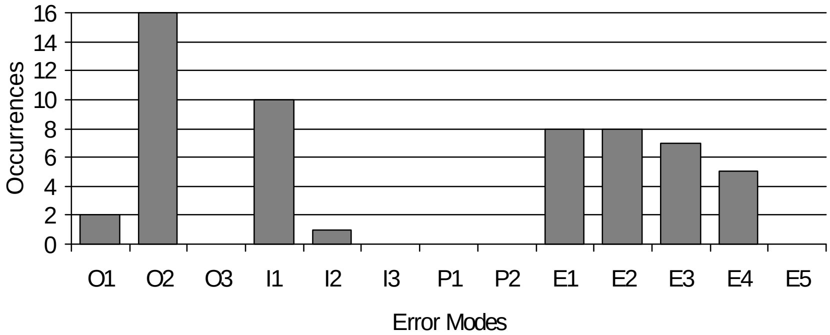


Figure 6: Distribution of error modes for SGTR EOP E-3

There is a significant overlap between the CPCs and the traditional performance shaping factors (PSFs). However, the influence of CPCs is closely linked to the task analysis i.e. context assessment rather than assessed afterwards during the human error probability assessment. The assignment of values to the CPCs must necessarily refer to a set of specific assumptions about the situation.

4.4.3 A practical methodology for interaction between PSA and human factors methods

A crucial part of the integration is the interface between the PSA, cognitive methods and HRA. This part of the methodology is described in by Andersson and Edland (1996). In summary, it consists of the following parts:

1) The first PSA analysis is performed with a standard estimate for all operator interactions. One way is to start with probability p(human error)=1.0, i.e. certain human error is assumed. Probability estimates for technical basic events such as component failures may be taken from the plant PSA data sources such as the T-book.

2) The first analysis gives a list of most important human actions. This list together with the instructors judgement of difficulty and importance are handed over to HRA specialists for rough quantitative estimates.

3) In the HRA quantification the following factors are taken into account: (1) How much time is available, on average, for each sequence segment, (2) How many steps/operations are included, (3) Which cognitive activities are included in each sequence based on the cognitive analysis. The results on this analysis are tentatively translated into a probability analysis

4) The results from the HRA are used to update the PSA model. Based on the new results, more interaction between PSA and HRA may take place.

One has to take into account that although some of the proposed principles have already been applied in PSAs, this methodology considers the cognitive dynamics of the sequences. In the cognitive HRA analysis, e.g. the following considerations are of interest:

- Loops and checkpoints in the procedure are modelled as recovery situations. To simplify, the model recovery is executed at the latest possible moment. This means that the model only allows recovery to be used once.

- The thermohydraulic calculations by CENTS give a time/parameter graphic, which is used to estimate the latest possible time to perform the actions needed. It is also possible to observe results of shorter delays of a number of actions and the number of loops that can be performed in one step of a sequence.

4.4.4 Results

The event has been studied with the KSU simulator. A preliminary semi-dynamic PSA analysis on the E-3 part of the sequence (E-3 is the main SGTR EOP, that follows a “standard” SGTR event) has given coarse conditional probabilities at specific system states (especially for exits from the E-3 to other EOPs). Validation of two thermohydraulic codes with the simulator, and studies on how to best utilise the integrated uncertainty analysis described in (Pörn, NKS/RAK-1(96)R2) have taken place (Pörn , NKS/RAK-1(97)R1). By an integrated uncertainty analysis Pörn means that uncertainty distributions for PSA model parameters are used throughout the study and not only afterwards, which guarantees the right inclusion of the uncertainties. Furthermore, Pörn has explored how influence diagrams and marked point processes following the approach described in (Holmberg et al., 1996) could be used for evaluating SGTR (Pörn, NKS/RAK-1(97)R4).

The results indicate that further attention should be given to sub-sequences, which lead to stuck open atmospheric relief valves (ARVs) of steam generators. Also, the analysis should include the use of overfill of steam generators as an end state. A number of observations could be made regarding plant behaviour and safety practices concerning the events that were analysed. It was e.g. confirmed that there is a significant probability for SG overfill given that SGTR occurs and that failing main steam isolation valves may be a dominant contributor at the present state of knowledge regarding the failure probability for these valves. The contribution of operator failure is more than an order of magnitude lower. The operators would have to do at least two mistakes to cause an overfill situation. Further analysis could focus on dependencies between a pair of mistakes. Another result is that loops in the procedure can only be allowed to take place once if top filling is to be avoided. Considering the importance of such a conclusion, it needs to be further confirmed, especially by time data from simulator runs.

The probability for the operators being instructed to go to procedure ECA-3.1 for non-isolated SGTR was estimated at $2x10^{-2}$. The high probability was mainly caused by missing operator actions to isolate the damaged SG. This result can point to an area where further human factors research is needed. The conclusion is supported by the specific uncertainty importance measure, which ranked the event “failing to identify damaged SG” highest (for the SG top filling PSA analysis). The SGTR analysis also resulted in enhanced understanding about the demands on the operators and possible error modes in different phases of event handling.

4.5 Confused signal view in the control room

4.5.1 Background and goals

There were several reasons for this part of the project. Among the most important were:

1. Several investigations have shown that during incidents, the operators’ decisions have been difficult because of conflicting signals - the Three Mile Island accident being probably the most well known example.

2. The very detailed level of PSA for a Swedish NPP, Oskarshamn 1, which was developed during the upgrading project ”Fenix” in 1995, has made it possible to analyse how and in which way the information will appear in the NPP control room.

3. Attempts had been made in USA to analyse how the NPP operators would act during different event scenarios (Drouin et.al., 1989). This was done by building fault trees and event trees based on EOPs and it brought up the idea of analysing control room work when the information to the operators is unreliable.

The idea of the Nordic disturbed signal view project was to develop an integrated analysis method for situations where the operators face an incident with confusing or even contradictory signals in the control room. Examples of such events are fires or leaks in instrumentation rooms.

In order to study the phenomena, several aspects have been accounted for. For example, the signal system of a BWR reactor has been modelled in fault trees, including components, signal cables, measurement systems, etc. Furthermore, operator’s situation during a disturbed signal picture with conflicting signals has been analysed by using simulator.

The project is an extension of a pilot project that was done during 1996 (Holmgren, 1996). In the pilot project, an initiating event (a rupture on the measurement system for water level in the reactor) was selected and analysed. Due to this event, incorrect signals of water level were sent to the control room but also to different automatic safety systems. The pilot project resulted in a method for analysing the most safety critical signal patterns of the NPP. The method has been tested in detail and modified in this project.

4.5.2 Analysis flow

At the outset of the project, the decision was made about what parameters should be analysed. The parameters ‘water level in the vessel’, ‘pressure in the vessel’, ‘reactor power’ and ‘temperature in the suppression pool’ were chosen based on EOPs and operator interviews.

For the main study (Holmgren, Jacobsson & Sörman, 1997), the water level in the vessel was chosen. After studying the different systems for water level measurement, operating personnel interviews were carried out. In the interviews, three different operator crews ranked the different displays in the control room. Eight displays were chosen for further investigation. A scheme for the analysis with its different phases is shown in Figure 7.

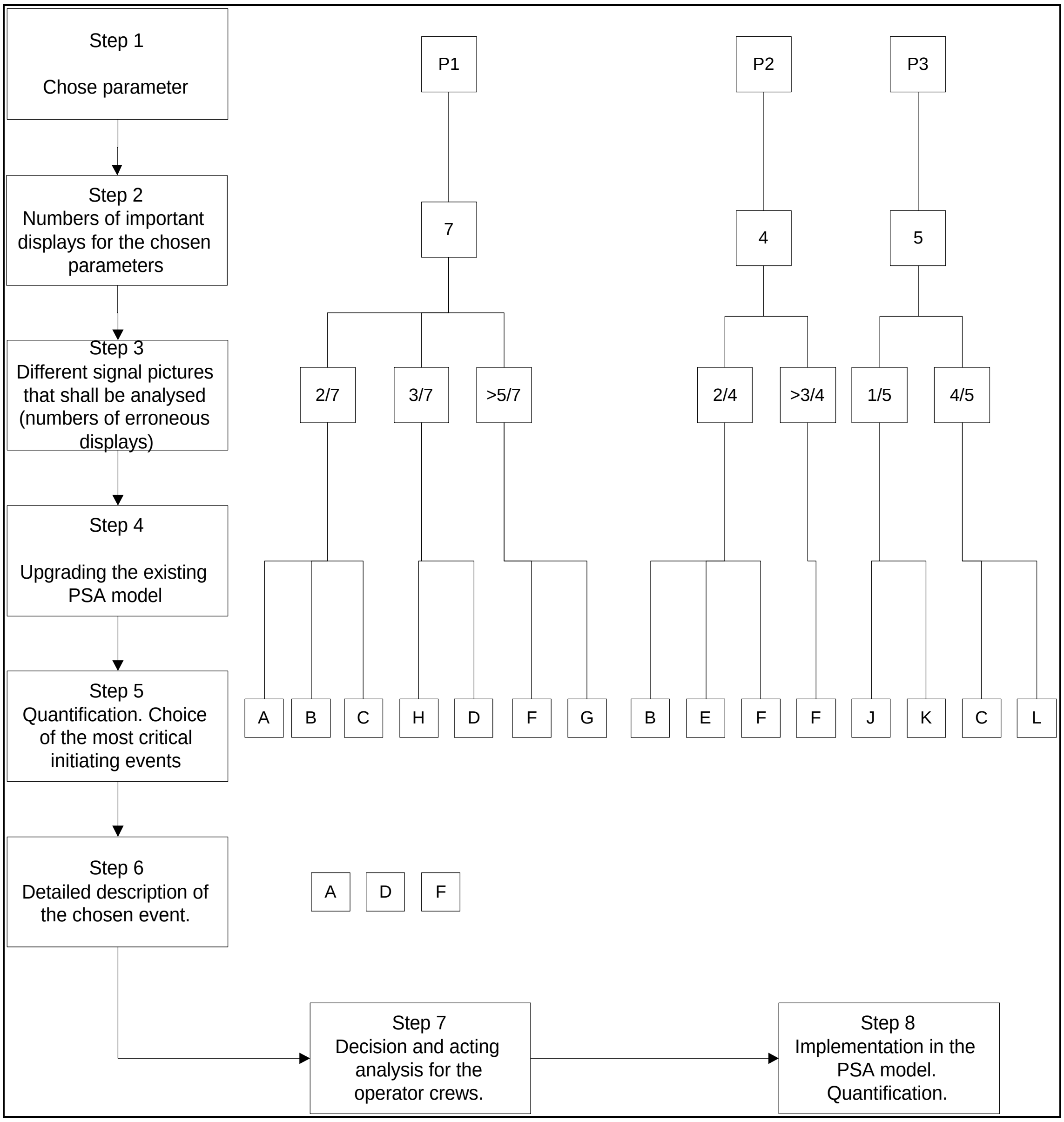


Figure 7. The flow diagram of the method applied in studies of disturbed signalview.

Different failure modes were discussed, and the failure mode ‘erroneous high’ was chosen for a closer study. It meant that the further analysis was to be made for the cases where one, two or three of the most important displays show high level (and send a ”high” signal to different systems) when the level actually is stable or decreasing.

Upgrading the existing PSA model was necessary to analyse such events with PSA. That was carried out in the next step of the project, and it led to a more detailed instrumentation model. Then, quantification of the PSA model and analysis of the results was performed. As a result, different initiating events, that lead to the most important displays showing high level, were identified.

Those important initiating events were analysed in a detailed way by interviewing operator crews, and then, by using the KSU O1 simulator. The two most significant initiating events leading to spurious ‘high’ in the two selected displays were: fire or flooding in a specific room and a leakage/rupture on one of the level measurement system.

First the simulator was used without any operators. After that, two different operator crews participated in runs of different events. Consequently, it was possible to make descriptions of the event with and without the operators’ involvement. After the simulator runs, the events were discussed with the operator crews. This step also gave input data for the operator model that was developed in the next step.

The idea of the operator model was to develop a method for analysing decisions and actions taken by operating crews in a situation with confusing signals in the control room. After an initial preliminary analysis, a quite extended analysis was performed, which was built on the model shown in Figure 8.

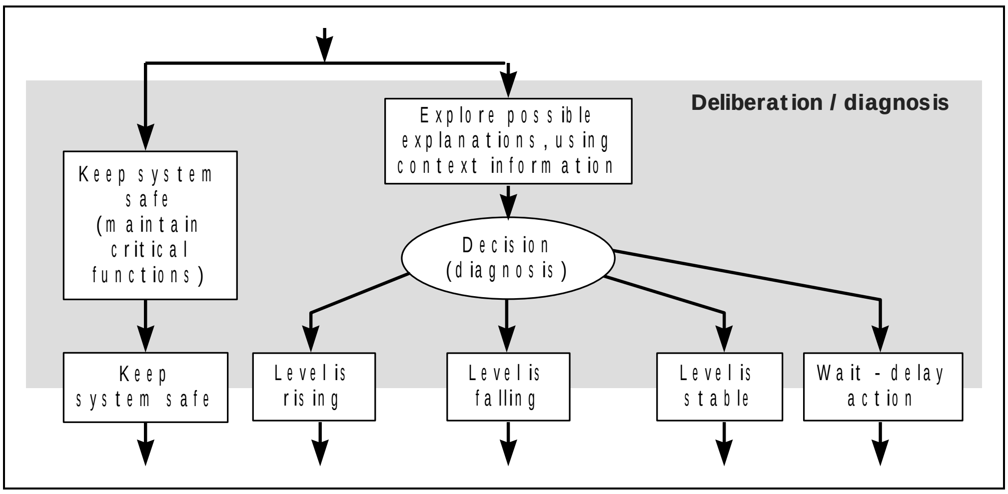


Figure 8. The operator model used in the disturbed signalview project

The model includes:

- Common Performance Conditions (CPC) for the three different steps: immediate disturbance controls, diagnosis/deliberation and acting (see Hollnagel 1997).
- Four different control modes: strategic, tactical, opportunistic, scrambled
- Cognitive activities (16 different, e.g. observe, plan, regulate and communicate)
- Cognitive functions, observation, interpretation, planning and execution
- Cognitive function failures (13 different, e.g., wrong identification, action missed)
- Quantification

4.5.3 Quantification of human error probability

The quantification is based on the CPCs that either 1) improve, 2) have no effect or 3) reduce the performance reliability for different segments of the human performance. The sum of the CPCs representing each of these three categories is then calculated. It is suggested that the result of this calculation has to do with human control modes, e.g. if there are no reducing CPCs and more than three improving CPCs the control mode is strategic. Figure 9 shows the approach used in determining control modes.

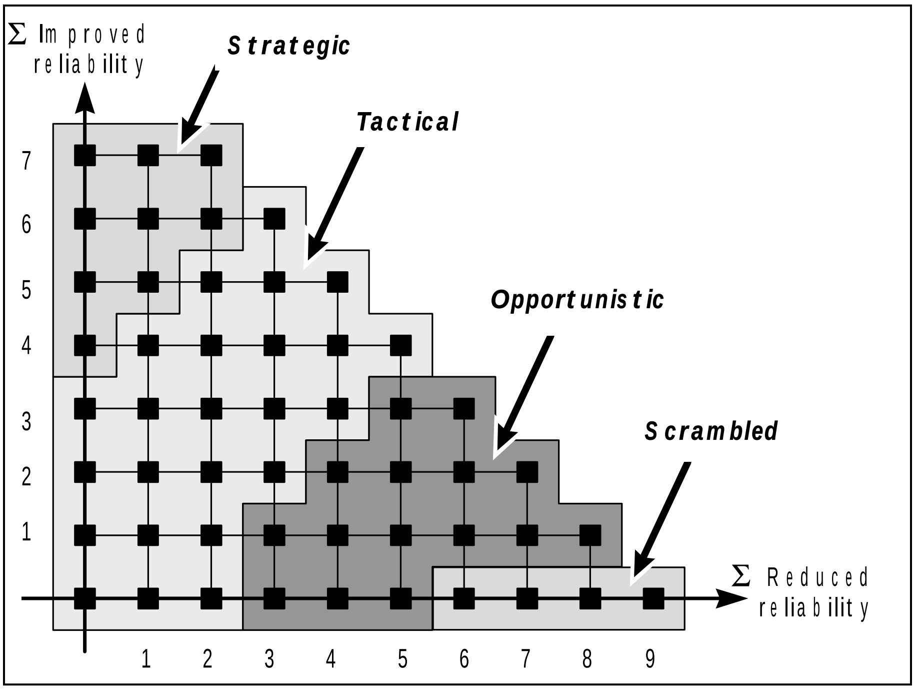


Figure 9. Relations between CPC score and control modes

The suggested relationship between the control modes and human action failure interval is shown in Table 11. The idea of the classification is that the better the CPCs are, the better the control is. The better control mode (more control) a human being has, the less is the failure probability. The aim is not to give exact estimates of human failure probability but more to give some indicators of the region.

Table 11. Control modes and probability intervals

Control mode	Reliability interval (probability of failure)
Strategic	5 E-6 < p < 1 E-2
Tactical	1 E-3 < p < 0.1
Opportunistic	1 E-2 < p < 0.5
Scrambled	1 E-1 < p < 1

In the last step the results from the quantification of the operator model and the descriptions are implemented in the PSA study. This step shows e.g. the impact of aggravating manual actions.

4.5.4 Results

The project has resulted, apart from the described method, in improved understanding about disturbed signals in the control room and about ways to analyse them, which can lead to more complete PSA studies.

The method can be used as a tool for verifying different aspects of the work in the control room, for example: instructions, practices and control room design. The method might be used in future projects of verifying and validating of upgraded control rooms.

The project has also resulted in practical enhancements of the design, training and work in the control room. Examples of such enhancements are: changed checklists, background material for the yearly training of the operators and also background information for creating a new level measurement system in Oskarshamn 1.

The quantitative results show that the contribution of the analysed cases to the core damage frequency is very small in comparison to the original PSA results for Oskarshamn 1.

5. Case study learnings

In this Chapter, we will discuss the generic viewpoints and teachings produced by our case studies. Technical results of each case study have been presented in Chapter 4.

5.1 Teachings with regard to plant safety work

Right information is required in all plant operating modes for successful operation and disturbance management. This was highlighted by all the case studies. The confused signal view case explicitly considers conditions, where operators may have difficulties in getting correct information from instrumentation. This should lead to re-assessment of human reliability in e.g. fire, flood and other external event cases.

In the shutdown LOCA case, and to a certain extent also in the SGTR case, safety critical information may be obtained from other sources than the control room measurements and alarms. Physically observable information is most valuable in order to achieve a detailed diagnosis, and it should not be underestimated in HRA studies. Therefore, it is natural to take into account this local information often provided by field operators and fitters. Another important point is that actions outside the control room are more distributed than those taking place only in the control room. Ex-control room actions are vulnerable to several pitfalls, but are vital in order to master an NPP during a wide spread disturbance - or during an outage. Thus, the focus of the design should not only be upon the control room but also upon the communication channels outside the control room.

In SGTR analysis, it was confirmed that there is a significant probability for SG overfill given that SGTR occurs and that failing main steam isolation due to technical reasons may be a dominant contributor. The SGTR analysis also resulted in enhanced understanding about the demands of the operators and possible error modes in different phases of disturbance handling. Similar results were obtained from the confused signal view project. Another finding of that project were some dependencies in the instrumentation in the older Nordic BWR reactors.

Maintenance is often neglected in safety studies. However, maintenance may have a significant role for the possibilities to bring the plant back to safe state by keeping the systems operable in normal conditions and recovering systems in accident conditions. In rare conditions, maintenance may also have side effects, e.g. LOCAs in shutdown conditions, unintended unavailability of components or false instrument readings. Even if such cases are rare, more emphasis should be put to prevent them from happening due to their potential severe consequences.

One important lesson from the cold overpressure and shutdown LOCA studies is that there are good reasons for the increased attention that is now given to shutdown conditions. In earlier phases of reactor safety work, increasing the safety for full power operation was in focus. Now, the weaknesses of the plants in shutdown states, e.g. due to poor reliability of instrumentation and the potential of ‘single’ human errors to cause serious initiating events, become more obvious. Here, the term “single human error” may include several faulty activities if the overall goal of the activity is not suitable to situational constraints, i.e. a person believes he is doing the right thing but fails due to a co-ordination slip.

As discussed, the case studies led to an amount of different views on how to enhance NPP safety practices. They are discussed in Table 12.

Table 12. Case study teachings dealing with NPP safety work

Case study: Plant level teachings	SGTR	Shutdown LOCA	Cold overpressure	Confused signalview
Design	For SG overfill, given SGTR, failing main steam isolation valves is an important factor - emphasis on increasing automated isolation reliability	There are certain weaknesses with regard to outages in plant design, e.g. large diameter valves below the core level in the main circulation loop	There are certain weaknesses with regard to outages in plant design, e.g. cold overpressure protection and instrumentation	Preliminary ideas on how to validate future control rooms for external event scenarios. BWR reactor instrumentation dependencies can be analysed in a new way.
Instrumentation	Some indications are located outside the control room - add-on information may come from field operators	During shutdown, information on events e.g. LOCAs may come from field operators and other staff	See shutdown LOCA	Some events may cause misleading signal patterns - better separation of I & C systems
Procedures	A comprehensive set of procedures for 'all possible cases' exists, in principle	Maintenance carried out based on work orders rather than on procedures	There may sometimes be differences between procedures and operating orders	Focus on maintaining the critical safety functions and not on following detailed instructions
Operations	There is an amount of uncertainty related to the operators capability to isolate the steam generator in time	Operators have wide spread sources of critical information in outages - performance in such conditions is difficult	Operating is difficult in the context of limited instrument support - even in long time scale scenarios	Operating is difficult in the context of misleading instrument support in highly dynamic disturbances
Maintenance	Maintenance can help in isolating the overfilled SG as a part of accident management	Maintenance, apart from its known importance, can in the case of a rare error, cause hazardous consequences in outages	Wrongly timed or erroneous maintenance can lead to wrong instrument readings	Apart from external events, wrongly timed or erroneous maintenance can lead to wrong instrument readings
Safety practices	In order to enhance the decision making quality it would be most valuable to acquire more knowledge about operator-related events (e.g. fail to identify damaged SG)	Considerable uncertainty with regard to leakage probability during a refuelling outage – opportunities for such leaks shall be avoided	Knowledge on restricted instrumentation support should always lead to instructions to compare and operate with care	Understanding confused signals in the control room and I & C systems behaviour in the case of external events should lead to better safety practices

5.2 Human factors and HRA

The prerequisites for human factors and HRA analysis were different between the four sequences. For the SGTR sequence, there is the Westinghouse package of procedures that should be, in principle, able to catch all possible secondary events after a SGTR has occurred. This is not the case for the other sequences. In fact we have found many situations where procedures are not typically used or not applicable. Such case is e.g. maintenance activities leading to utmost adverse conditions to shutdown LOCA. There may also be small contradictions between procedures and annual operating orders as e.g. in cold overpressure case. Confused signal view may represent a case where there either are no valid procedures or where it is not overall possible to write good procedures. Thus, HRA shall be rather based on real plant practices rather than just on the procedures.

In certain situations, the operators have to act with limited support from control room information and procedures, e.g. if the signal view is confusing as in one of our cases. This kind of decision making is not taken into account in standard HRA methods and need to be subject to more careful analysis.

One important teaching has been that HRA needs to be naturally integrated, since at least process, human factors and reliability engineering knowledge is required for meaningful probabilistic results with sound coupling to reality. This topic is discussed more in Chapter 6.

In all case studies, a practical framework for interaction between human factors and PSA was established, which resulted in certain kinds of expert judgement on human failure probabilities. This underlines the role of expert judgement - practically no other data is available on human reliability apart from some simulator runs and laboratory tests.

One problem in the interaction between PSA and human factor is to find suitable interaction models and a suitable level of aggregation. A too high level will be too coarse to produce results plausible to both disciplines, and a too low level will be impractical with regard to resources. In the SGTR analysis, it was found that segments in the procedures is a suitable level of aggregation. However, procedures are only one viewpoint to the HRA work and they should be integrated with other means such as interviews, simulations and on-site visits. In shutdown LOCA and cold overpressure cases, the level was chosen to represent the reliability model events. Thus, the level of decomposition was higher. The confused signal view produced an extremely detailed model of signal system and a rather high level model of operator and human reliability.

5.3 PSA

The project has given a significant feedback to the PSA analysis of all the four sequences. For the shutdown LOCA case, expert judgement gave more detailed PSA values when compared to plant shutdown study. The simulated probability for core upper grid uncovery is relatively high. One has to bear in mind that this does not mean the same as radioactive releases (core melt). The uncertainty related to the variables in question is high, too. This is manifested both by the expert’s judgements and by the resulting uncertainty distribution, although in the latter case there are conceptual interpretation problems. Consequently, it is advisable to study any potential to avoid situations where irradiated fuel may uncover due to shutdown LOCA below the core level.

The TVO cold overpressure sequence analysis also gave a much more detailed estimate of event probability. For that purpose, a package of tools was developed during the project. The quantitative results also remained low showing that the risk of cold overpressure is negligible. Another related point is that cold overpressure does not automatically mean reactor tank rupture.

For the SGTR case, the new PSA approach, which essentially follows the EOP structure, includes improvements with respect to both technical and human failure analysis as compared to the standard approaches to HRA and PSA. However, the event has so far only been partly analysed. It remains to proceed the analysis to sub-sequences outside the 'normal' procedure case following E-3. On the other hand overfill of damaged SG potentially leading to ARV opening was also subject to PSA analysis. This highlights that sometimes there may be other end states than core damage that may be equally important to include.

The confused signal view produced a well decomposed PSA model of signal systems with a high level operator model. Probabilities for human errors in the consequence of disturbed signals remained rather high. However, the analysed cases had little impact on the already calculated core damage frequencies for Oskarshamn 1.

A specific topic related to PSA is uncertainty assessment. This should rather be an integrated part of parameter estimation than something taking place at the end of PSA. Otherwise, the uncertainty has no sense as 'the probability of probability'. Point estimates or distributions have to be used where they are naturally generated in the analysis, not artificially. Where significant uncertainty exists, simply more accurate data has to be collected. The uncertainty analysis related findings of NKS/RAK-1.3 are discussed more in Tabel 13.

In summary, the NKS/RAK-1.3 experiences show that it is possible to improve the PSA analysis to a much higher level of confidence with focused efforts on specific sequences, and with involvement from experts in different areas.

5.4 Process evaluation

Cold overpressure and shutdown LOCA analyses showed that simulating and making HRA related exercises for shutdown states is not easy. On one hand, simulators and thermohydraulic codes may operate on their limits. On the other, much activity takes place outside the control room. Fortunately, the related physical calculations are often easy and manual calculations may be run as a first approximation.

In the SGTR case the physical process was evaluated with the CENTS code. Although limited to the procedure E-3 case, the analysis showed what would be the role of the model in full analysis of the sequence. It was e.g. shown how time windows serve as the link to HRA and PSA within the overall semi-dynamic approach. From the point of view of the utility the verification of the code against the simulator was valuable, and increased the confidence in the code for future applications.

In the confused signal view case, the process was analysed and evaluated by using the KSU O1 simulator. This included different test runnings with and without operational crew.

5.5 Overall methodology and integration

In general, a fruitful interaction has taken place between experts in different disciplines, which has increased the understanding across the disciplinary borders. The analysis accomplished so far has also increased the depth of understanding about the sequences.

The semi-dynamic approach has so far only been tested on a limited part of the SGTR sequence tree. Still, it has been demonstrated as a tool for more comprehensive analyzes. Practical methods have also been developed for the integration between disciplines. The software tools used (PSA software, thermodynamic codes etc.) have, however, not been developed for this kind of analysis. Software development may thus be needed for future applications.

Table 13. Methodology and analysis related findings

Analysis	SGTR	LOCA	Cold overpressure	Confused signalview
ISA methodology	A feasible level of communication and exchange between experts of information was established Each discipline worked separately but common workshops were regularly held and common reference models used EOPs was the integrating framework	Application of expert judgement methodology with normative experts steering the communication between substance matter experts PSA model as integrating framework	Common workshops between disciplines were regularly held and common reference models used - PSA model was the integrating framework Reference model approach helped in the communication between different disciplines PSA model as integrating framework	Integrated competencies: maintenance, operations, PSA, HRA, cognitive science, I&C. The work was performed as workshops and as individual work in between. The intention of the analysis was to study effect of some cases to human reliability.
HRA / PSA	A detailed PSA model with HRA analysis, although limited to the E-3 EOP. For this part of the sequence the calculated core damage frequency was reduced in comparison with the plant PSA	A high level HRA model based on expert judgement was generated Results showed that the probability of leakage and failure probability of recovery are rather high	A dynamic and detailed PSA model was created Results show the overpressure risk to be very small and consolidate the utility's analysis results	An approximate HRA model based on operator control modes A more complete and detailed PSA model through modelling signal systems
Behavioural scientific analyses	Cognitive profiles for EOPs with error classes: A high proportion of human error modes linked to observation, interpretation and execution.	A large number of human error modes due to misinterpretation of work orders or/and misunderstanding between the control room and maintenance	Concepts of critical information, contextual behaviour and descriptive decision analysis developed	Creating link between cognitive model (CREAM) and HRA
Physical analyses	Verification of CENTS model against plant simulator	Observing discrepancies in some physical calculations	Observing some simulator limitations in low power conditions	Observing some limitations in the simulator. Defining different failure modes for instruments.
Uncertainty assessment	The use of uncertainty importance measure showed that it is advantageous to get more information about 'identification of faulted SG'	Large uncertainties in variables 'time to stop the leak' and 'probability of leak' - conceptual difficulty with uncertainty as 'probability of probability'	As in shutdown LOCA, uncertainty manifested in expert judgement distributions and in psychological analyses of operator decision making	Uncertainties in the knowledge of failure modes for the instruments. Uncertainty in the probabilities for manual actions.

The shutdown LOCA case study proved that it is possible to carry out well-structured expert judgement assessment in a limited period of time. The used method proved out to be a valuable tool for expert judgement combination and wider uses are foreseen. In addition, a careful training accompanied by expert reporting and thorough elicitation interviews are needed in order to avoid biases. By using that procedure, expert judgement forms a good completion to other ISA methods.

The NKS/RAK-1.3 project has shown that that different disciplines can work together successfully. As a complex topic, systems / sequences with remarkable human contribution deserve a multidisciplinary treatment in direct contact with plant operators and instructors. One of the most important functions of the NKA/RAK-1.3 project is to provide methods for a scientifically correct analysis and means for integration of different discipline views.

6. Discussion

At the outset of NKS/RAK-1.3 we defined ISA as event analysis with active participation from different disciplines. In the course of the project there has been ample time to reconsider the nature of an integrated sequence analysis.

To be able to answer the question about the nature of ISA, we have to understand the nature of integrating scientific disciplines, as a whole. Apart from mathematics, integration is often defined as creating compatibility between several interest groups. It is clear that ISA has a lot in common with that definition, since a great deal of time is devoted to creating reference models, and defining suitable breakdown levels in modelling, in order to enhance communication. Creating improved ways to communicate and cooperate is undoubtedly one of the most important objectives of an ISA. That is manifested in Figure 10, where communication between the disciplines takes place in ISA approach.

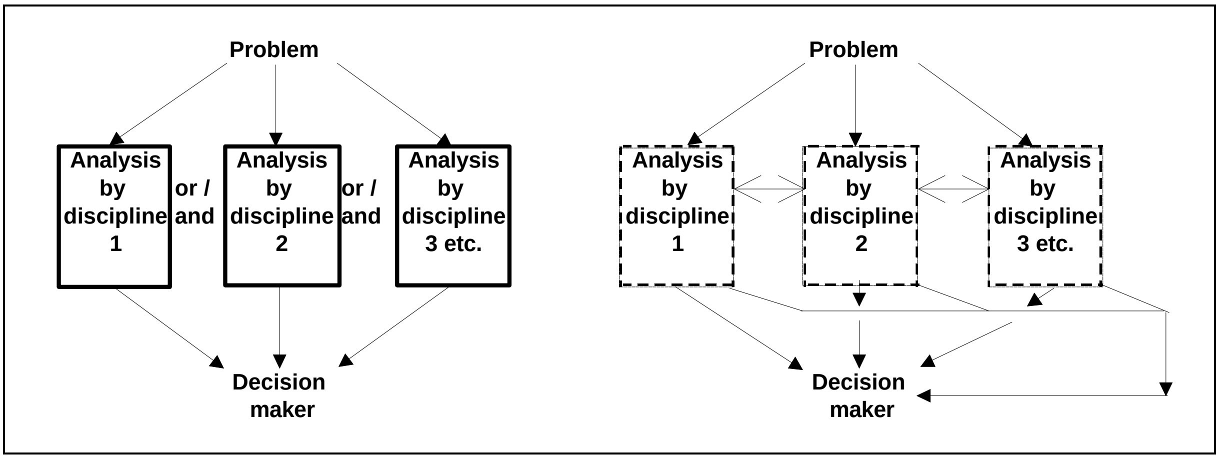


Figure 10. A diagram comparing separate scientific discipline analyses (left) and an interdisciplinary ISA (right) approach where more information is generated through information exchange.

Thus, by enhancing communication between different disciplines, more information is created for decision-makers. In that purpose, ISA should select a feasible level of communication / modelling. Using moderators / decision analysts may help in the task. It is important that somebody controls the communication exchange in order to avoid biases discussed in Chapter 4.

6.1 Three organisational approaches

Sometimes the discussions between different scientific disciplines are not trivial. This is due to the very different research traditions, nomenclature and approaches to research problems. Complete unification of different scientific disciplines is not feasible. However, there are some potential structured approaches to create a functioning ISA, and there are many similarities between them.

In the decision analytic approach (left part of Figure), experts of different disciplines look at a problem from different viewpoints and present their analyzes to decision maker(s) and decision analysts. An amount of information exchange is normally required between the experts to provide a common understanding of the decision problem. Decision-makers, or decision analysts, then weight the collected pieces of information by using a selected method, and form a synthesis for the basis of the decision. This kind of an approach i.e. prescriptive decision analysis is commonly used in operations research field (e.g. Keeney & Raiffa, 1976).

In the second approach, the goal is to assess values of certain interesting variables - that may be used as a basis for decision making. An example of such a case is the probability assessment of a sequence including significant human actions. There, experts in probability calculus elicit the data from substance matter experts, e.g. behavioural scientists and process experts. The method differs from the first one that all experts / disciplines give replies to same questions. This procedure is common in expert judgement elicitation (Otway & von Winterfeld, 1992).

The third structured method for ISA is to create a working group of different disciplines to work on the same problem. An analyst or a group steers their work and moderates discussions. The idea of this is to ensure a proper communication so that the results of an integrated analysis will be more than just the sum of separate disciplinary analyses. At the same time, the idea is to restrict dominating personalities to upset the whole group work. This approach is common in Nominal group technique presented in Chapter 3.3. The right part of Figure represents the two last approaches.

The analyses in NKS/RAK-1.3 have mainly followed the second and third alternatives. Especially, the BWR shutdown sequences followed alternative 2. In the SGTR sequence analysis the dominant approach was according the third alternative, with elements of alternative 1. Also the organisation of the analysis teams has a significant effect on the form of ISA. For example, the two BWR shutdown analysis teams mainly consisted of representatives of the same enterprise whereas the PWR SGTR team consisted of several organisations.

Our ISA studies have focused upon HRA framework. This is not obligatory - for example similar topics have been raised in NKS/RAK-1.2 project on pipe rupture probabilities. Furthermore, PSA is not a compulsory framework for disciplines to work together. However, it is a comprehensive systems modelling framework which attempts to take into account uncertainties. Facing considerable uncertainties is a natural factor that makes people to work together.

Figure 11 shows how our model of ISA improves the human reliability modelling by bringing a wider view into the analysis. For example, forgetting the probabilistic dimension of HRA can result in good cognitive models for certain accident sequences, but it may be impossible to quantify them by probability measure. On the other hand, forgetting physical calculations leads only to an academic HRA. Finally, the traditional HRA analyses discuss little with the latest psychological theories. A connection to real applications such as an NPP, is always required.

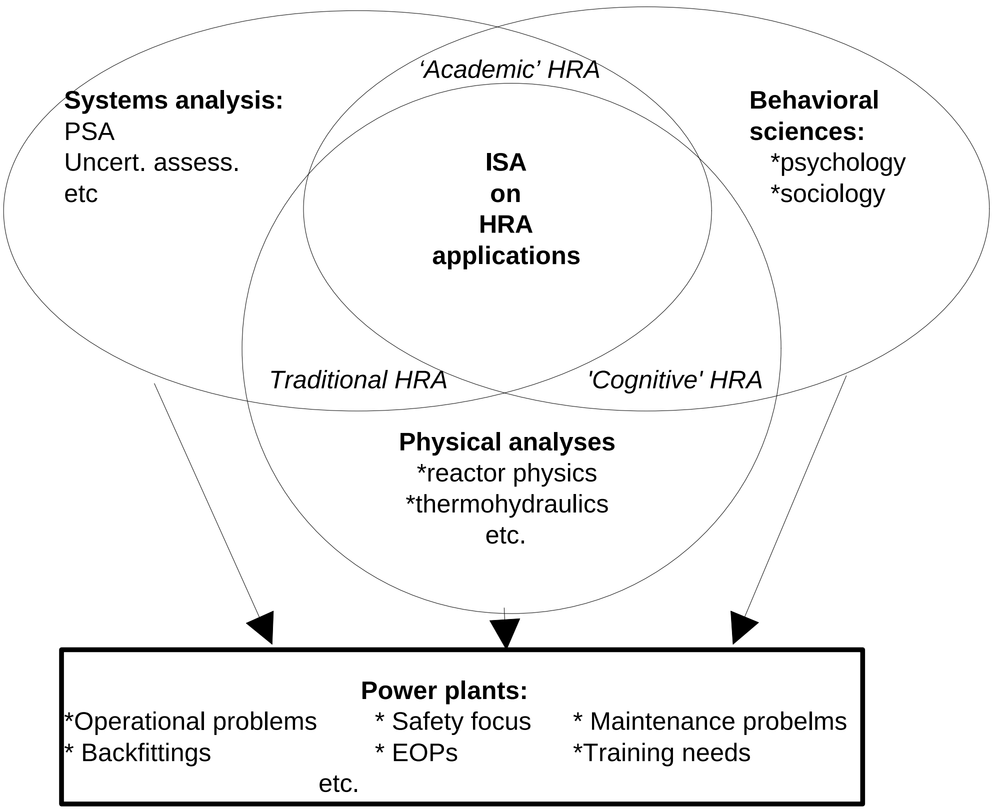


Figure 11. A presentation of the structure NKS/RAK-1.3 ISA on HRA.

Of course, there are many forms of unstructured ISA. They normally manifest themselves in situations, where people with different backgrounds are simply put to work together. By vast historical experience, one has to admit that these forms of integration seem to work very effectively - especially if there is a strict time limit they may be superior. From a scientific point of view one has to observe, however, that this type of ISA is most vulnerable to social biases discussed earlier in this report.

6.2 Static models - dynamic models

The traditional PSA methodology using fault tree – static event tree technique provides a coarse first order approximation of the plant or system behaviour. Real behaviour is often strongly dynamic with respect to the time dependent evolution of the processes that depend on temperature, pressure, flows etc. and the plant system status including degraded or failed components etc. The process system and the plant status are closely correlated, not least to the logic of automatic triggering of safety systems. The dynamic nature of events is even more emphasised when the evolution involves operator interventions, as is the case for sequences considered in this study.

In the static event tree approach, the set of system states is restricted to extreme conditions; a system either functions or it fails. Implicitly, the correlation to the physical process is considered in the definition of various system success criteria, which may differ depending on in what phase of the process the system initiation takes place.

Complete mathematical description of the physical process and the system status is provided by the theory of probabilistic dynamics (Devooght & Izquierdo, 1996), presented also in an alternate form, called dynamic event trees (DET). This rigorous approach, however, requires complex computations, which are difficult to accomplish without certain simplifications. The concept of integrated safety assessment, described in terms of probabilistic dynamics, has been applied by (Izquierdo et al, 1994), in order to verify that the software of the automatic and manual protection systems satisfy certain general protection design criteria.

A practical approach between the static event tree and a fully dynamic approach would be a semi-dynamic methodology, illustrated earlier in the text. However, we lack technical tools for semi-dynamic analysis, especially regarding PSA. The CAMS software system being developed for accident management support is one candidate to potentially, in future, provide tools for more dynamic analysis (Fantoni et al, 1995).

6.3 A comparison between the VTT's IDMPP and the semi-dynamic approach

Technically, the two approaches used by VTT for the cold overpressure sequence and the Swedish group for the SGTR sequence look rather different. However, there are some striking similarities. Both approaches use event diagrams for the overall structure and integration. In the TVO case, the event diagram is a key part in the reference model and in the SGTR case it is mainly built on the family of EOPs. Furthermore, both analyses used PSA and cognitive models as important components in the analysis. Also simulators were used by both groups, although the TVO group used simulators to produce data directly for PSA whereas this was not the case in Sweden.

One difference is that the Finnish analysis was more directly driven by PSA than the Swedish analysis. If PSA was the driving force in the TVO analysis it was the EOPs in the case of Ringhals. The VTT method also used more mathematical tools than the Swedish group. This was due to the different orientation to the analysis.

During the RAK-1.3 project, an application study of the VTT's method to the SGTR sequence was carried out (Pörn, 1997). The study concluded that the methodology was feasible. According to the study, the methodology provides an efficient and compact tool for modeling probabilistic dependencies and a way to carry out dynamic reliability calculations.

7. Conclusions

This project gave many results and experiences of value for future work. The tested methods showed capability for important contributions, e.g. with regard to:

- **Structured frameworks for integration** between PSA, behavioral sciences and physical analyses
- Next generation **HRA**
- More detailed **PSA** models
- Improved **cognitive models**
- Improved uses of **expert judgement** and uncertainty analysis
- **Dynamic PSA** models
- **Feedback** to safety practices, operator training, plant operation and maintenance
- Increased understanding about **shutdown risks**
- **Use of simulators** for event analysis

Still, the area of integrated sequence analysis is at a relatively early stage. Much research and development remains with the goal to obtain a comprehensive methodological package. There is a need to develop dynamic and semi-dynamic safety analysis approaches. Current PSA models need to be developed for practical and illustrative use for this type of applications. There are already early developments in this direction in areas such as accident management and PSA Level 2.

The use of simulators was an important part of our ISA / HRA framework. In this project, simulators were used in three out of the four sequences. Only in the TVO case, the simulations were used directly to provide data for PSA. In the SGTR, simulations provided data to the analysis on the timing of different actions and for the verification of codes. It is recommended that future ISA projects will use simulators, and similar kinds of tools, to an increasing extent to validate models and to collect human reliability data.

We also used expert judgement in the project as a source of data. We feel that expert judgement will remain as an important data source also in the future. A great deal of ill-structured subjective knowledge is used in everyday life. The ISA project showed some structured ways to utilise it. Expert judgement is recommended for use in cases where there are no ways to directly measure values of unknown variables or the measurements are not enough, alone. This is the case e.g. in HRA. However, it is clear that more work e.g. to master biases will be required in the area.

The experiences from the integration of disciplines are good. Our project offers several models for interdisciplinary communication. Still, there is a need for developing structured interface approaches that can be used with confidence by all disciplines. One aspect seen in the project is that e.g. PSA and NPP operation needs generalists and people with engineering background, whereas representatives of scientific organisations are characterised by research culture. Academic culture still gives interdisciplinary efforts a rather low priority.

Efforts of the NKS/RAK-1.3 project became more extensive than was originally foreseen and involved plant personnel to a great extent. The greater the involvement, the greater the benefit to the NPPs. For example, the project could come up with rather interesting results with regard to instrumentation, shutdown period and widely spread human actions (e.g. fires and management of a SGTR). More emphasis should be put to them in safety studies, in future.

Time did not allow cross-comparisons between methods to a desired extent. The used approaches should be more extensively tested in other sequences. There are also other methods and tools that should be subject for testing and implementation. For future, this kind of projects should always aim at benchmarking from the beginning.

The NKS project has led to commencing a Concerted Action within the Nuclear Fission Safety Program of the European Union. The Concerted Action in which Sweden, Finland and Norway participate from the Nordic countries, will considerably widen the perspective of ISA compared to the NKS project. This is an example of how NKS projects may lead to a continuation as a European Program.

References

Andersson, K., Strategies for Reactor Safety, NKS/RAK-1 Final Report, 1998

Andersson, S.O. & Edland, A., NKS/RAK Subproject 3, Integrated safety analysis, steam generator tube rupture, method description, April 1996, NKS/RAK-1(96)R4, Vattenfall GES 35/96

Andersson. K., et al, Integrated sequence analysis – semidynamic analysis of an SGTR sequence, NKS/RAK-1(97)R7

Andersson, K., Andersson, S.O., Edland, A., Hollnagel, E., Josefsson R., Ljungqvist, B. 1996. Integrated sequence analysis - semidynamic analysis of an SGTR sequence. Proceedings of PSA-96, Park City, USA, pp. 1507-1514

Apostolakis, G.E., Bier, V.M., Mosleh, A., 1988. A critique of recent models for human error rate assessment. Reliability engineering and system safety 22 (1988) 201–217.

Arjas, E. and Holmberg, J. 1995. Marked point process framework for living probabilistic safety assessment and risk follow-up, Reliability Engineering and System Safety, 49, 59–73.

Box, GEP., Tiao, GC. 1972. Bayesian inference in statistical analysis. Addison-Wesley Publishing Company, Reading. 588 p.

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

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

Cojazzi, G., Pedrali, M. & Cacciabue, P. C. 1993. Human performance study: Paradigms of human behaviour and error taxonomies (ISEI/IE/2443/93). JRC Ispra, Italy: Institute for Systems Engineering and Informatics.

Comer, M.K., Seaver, D.A., Stillwell, W.G. et. Al. 1984. Generating human reliability estimates using expert judgement. NUREG/CR-3688.U.S. Nuclear Regulatory Commission, Washington DC.

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

Dalkey, N. 1969. An experimental study of group opinion: The Delphi method. Futures 1969;1:408-426.

DeGroot,M. 1974. Reaching a consensus. Journal of American Statistical Association, 1974;69:118-121.

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

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

De Finetti, B. 1974. The theory of probability, Vols. I and II. New York, John Wiley & Sons.

Devooght, J., Izquierdo, J.M. and Melendez, E. 1996. Relationships between Probabilistic Dynamics, Dynamic Event Trees and Classical Event Trees. Reliability Engineering and Systems safety 51 (1996).

Dougherty, E. 1990. Human Reliability Analysis - where shouldst thou turn? Reliability Engineering and System Safety 29(1996), Elsevier Science Publishers. pp. 283-299.

Drouin. M. et. Al. 1989. Event Tree Modelling of Emergency Operating Procedures. Nuclear Regulatory Commission, Office of Nuclear Regulatory Research, Washington D.C, (1989).

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

Fantoni P., Meyer G., Nurmilaukas P., Sirola M., Sörenssen A.1995. The CAMS prototype. NKS/RAK-2(95)TR-B1. Halden, Norway.

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

Gelman. A., Carlin, J., Stern, H., Rubin, D. 1995. Bayesian Data Analysis. Chapman & Hall. 526 pp.

Gertman .D.I.. 1993. Representing Cognitive Activities and Errors in HRA trees. Reliability Engineering and System Safety, 39 (1993) 25 - 34

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 (1992) 127 -136

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

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

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.

Hollnagel, E. 1995. Summary of Approaches to Dynamic Analysis Of Man-Machine Interaction. Human Reliability Associates R94/31, NKS/RAK-1(95)R1.

Hollnagel, E. 1996. Reliability Analysis and Operator Modelling. Reliability Engineering and System Safety 52(1996), Elsevier Science Publishers. pp. 327-337.

Hollnagel, E. 1997. CREAM - Cognitive reliability and Error Analysis Method. Elsevier, Oxford. In print.

Hollnagel, E., Edland, A., Svenson, O. 1996. A cognitive task analysis of the SGTR scenario. NKS/RAK-1(96)R3 (1996).

Holmberg, J., Hukki, K., Norros, L., Pulkkinen, U., Pyy, P. 1996. Integrated sequence analysis - cold overpressurization accident sequence. Report TAU-6009/96, NKS/RAK-1(96)R5

Holmgren, P. 1996. Modeling of confused signals in the control room, Pilot study, NKS/RAK-1(96)R9, (In Swedish).

Holmgren, P. Jacobsson, P. and Sörman, J., Modeling of confused signals in the control room, Main study, NKS/RAK-1(97)R17, (In Swedish).

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

IPSN. 1990. EPS 900, A Probabilistic Safety Assessment of the Standard French 900 MWe Pressurized Water Reactor, Main Report. Institut de Protection et Sûrete Nucleaire, Commissariat a l'Enerqique Atomique. 224 p.+ App.30 p.

Izquierdo, J.M., Sanchez-Perea, M. 1994. Application of the Integrated Safety Assessment Methodology to the Emergency Procedures of a SGTR of a PWR. Reliability Engineering and Systems Safety 45 (1994), pp. 159-173.

Jacobsson, P. 1996. NKS/RAK-1.3: Analysis of inadvertent opening of an isolation valve during the shut-down period at the Barsebäck NPP using the COGENT method, Sydkraft Konsult ES-9603m007, NKS/RAK-1(96)R10.

Kahlbom, U., Holmgren, P. 1995. Survey of Methods for Integrated Sequence Analysis with Emphasis on Man-Machine Interaction, NKS / RAK-1(95)R2, RELCON - 20/95. 14 p.

Keeney, R. & Raiffa, H. 1976. Decisions with Multiple Objectives - Preferences and value Tradeoffs. Cambridge University press.

Kirwan, B. and James, N.J. 1989. A Human Reliability Management System, in Reliability 89, Brighton Metropole, June, (1989).

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

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.

NUREG-1150. 1989. Reactor risk reference document. Washington D.C., U.S. Nuclear Regulatory Commission, Office of Nuclear Regulatory Research, 1989.

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

Parry, G.W., Bley, D.E., Cooper, S.E., Wrethall, 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, 1996. Pp. 671-677.

Poucet, A. (Ed.). 1990. Final report of the CEC Benchmark on Human reliability Analysis. JRC Ispra.

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

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

Pyy, P., Himanen, R. 1996. A praxis oriented human reliability analysis method for Olkiluoto NPP PSA. PSAM III, Crete, Greece.

Pyy,P., Laakso, K., Reiman, L. 1997. A study on human errors related to NPP maintenance activities. IEEE Sixth Conference on Human Factors and Power Plants, June 8-12, Orlando, Florida, USA.

Pyy, P., Pulkkinen, U. 1997. Use of expert judgement methodology in the analysis of Barsebäck shutdown LOCA case. Work report TAU-7008/97, NKS/RAK-1(97)R6

Pörn, K., A Decision oriented measure of uncertainty importance for use in PSA, Reliability Engineering and System Safety 56 (1997) 17-27, NKS/RAK-1(96)R2

Pörn K., Tillämpning av nytt viktighetsmått för parametrisk osäkerhet i PSA, NKS/RAK-1(97)R1, SKI Rapport 97

Pörn, K. 1997. On the use of influence diagrams and marked point processes for evaluating SGTR of a PWR. NKS/RAK-1(97)R4, august 1997.

Pörn, K., Shen, K. 1992. On the Integrated Uncertainty Analysis in Probabilistic Safety Assessment. In Petersen, K.E., Rasmussen, B (eds.), Safety and Reliability '92. Proceedings of the European Safety and Reliability Conference '92. Copenhagen, 10-12 June 1992. Elsevier Applied Science, London. pp. 463 - 475.

Rasmussen, J. 1995 Converging Paradigms of Human Sciences. Swedish Centre for Risk Research and Education, Karlstad (unpublished paper).

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

Siegel, AI, Bartter WD, Wolf JJ, Knee HE, Haas HE, Haas PM. 1984. Maintenance Personnel performance simulation (MAPPS) model, Vol. 1. Summary Description. NUREG/CR-3626.

Svenson, O. 1989. On expert judgements in safety analyzes in the process industry. Reliability Engineering and Systems Safety 25, pp. 219 -256.

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.

T-Boken version 4, Tillförlitlighetsdata för komponenter i nordiska kraftreaktorer, TUD-Kansliet, 1994. ISBN 91-7186-303-6.

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

Tversky, A., Kahneman, D. Judgement under uncertainty: Heuristics and Biases. Science 1974; 185:1124-1131.

van Steen, J.F.J., Oortman Gerlings, P.D. 1989 Expert Opinions in Safety Studies, Volume 2: Literature Survey Report. Technical University of Delft, Safety Science Group, March 1989.

Zamali, J.H. (Baltimore Gas and Electric, Lusby, MD (United State)); Hubbard, F.R. (FRH Inc., Baltimore, MD (United States)); Mosleh, A.(Univ. of Maryland, College Park (United States)); Waller, M.A. (Delta Prime, Inc., Glen Burnie, MD (United States)). 1992. Evolutionary Enhancement of the SLIM-MAUD Method of Estimating Human Error Rates. Transactions of the American Nuclear Society (United States)Volume: 65, 508-510.