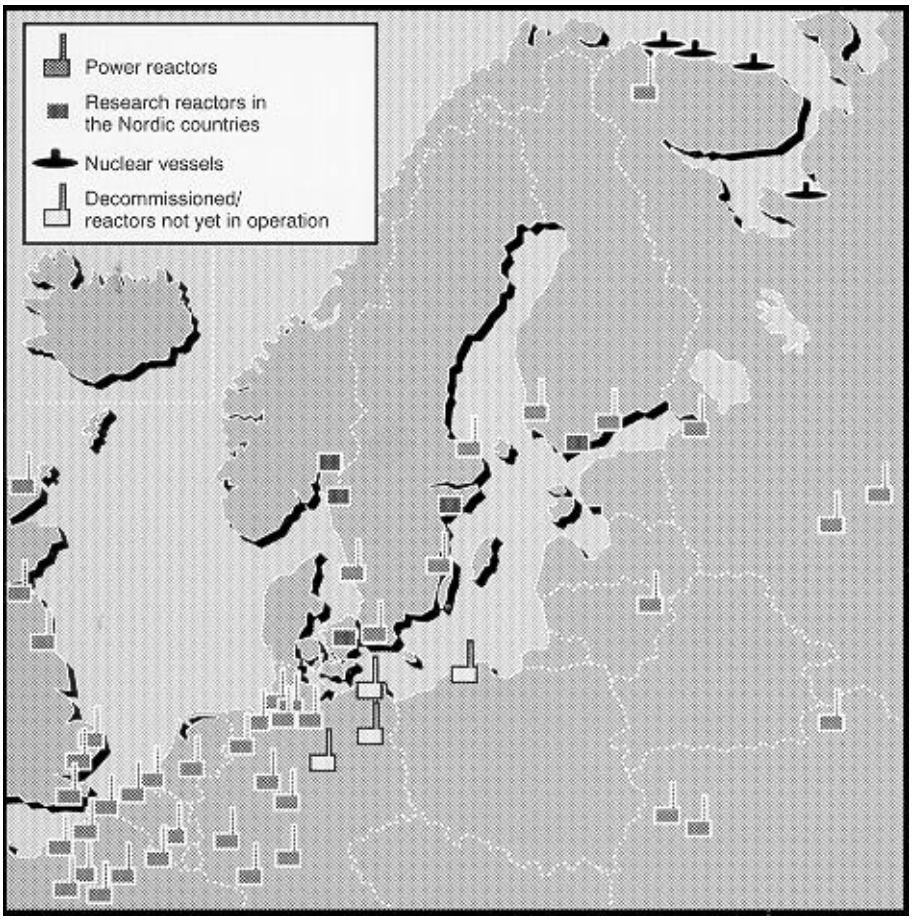
Strategies for Reactor Safety



nks

Nordic Nuclear Safety Research (NKS)
organizes joint four-year research programs involving some 300 Nordic scientists and dozens of central authorities, nuclear facilities and other concerned organizations in five countries. The aim is to produce practical, easy-to-use background material for decision makers and help achieve a better understanding of nuclear issues.

To that end, the results of the fifth four-year NKS program (1994 – 1997) are herewith presented in a series of final reports comprising reactor safety, waste management, radioecology, nuclear emergency preparedness and information issues. Each report summarizes one of the ten projects carried out during that period, including the administrative support and coordination project. A special Summary Report, with a brief résumé of all ten projects, is also published. Additional copies of the reports on the individual projects can be ordered free of charge from the NKS Secretariat.

The final reports – together with some technical reports and other material produced during the 1994 – 1997 period – have been collected on a CD-ROM, also available free of charge from the NKS Secretariat.

klæbel's offset tryk a-s 1998

NKS(97)FR1
ISBN 87-7893-021-9

The report is published by:
NKS Secretariat
Building 100
PO Box 49
DK-4000 Roskilde

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

NKS(97)FR1
ISBN 87-7893-021-9

Strategies for Reactor Safety

Final report of the Nordic Nuclear Safety Research Project RAK-1

Kjell Andersson

December 1997

This is NKS

NKS (Nordic Nuclear Safety Research) is a scientific cooperation program in nuclear safety, radiation protection and emergency preparedness. Its purpose is to carry out cost-effective Nordic projects, thus producing research results, exercises, information, manuals, recommendations, and other types of background material. This material is to serve decision-makers and other concerned staff members at authorities, research establishments and enterprises in the nuclear field.

The following major fields of research are presently dealt with: reactor safety, radioactive waste, radioecology, emergency preparedness and information issues. A total of nine projects have been carried out in the years 1994 - 1997.

Only projects that are of interest to end-users and financing organizations have been considered, and the results are intended to be practical, useful and directly applicable. The main financing organizations are:

- The Danish Emergency Management Agency
- The Finnish Ministry for Trade and Industry
- The Icelandic Radiation Protection Institute
- The Norwegian Radiation Protection Authority
- The Swedish Nuclear Power Inspectorate and the Swedish RadiationProtection Institute

Additional financial support has been given by the following organizations:

In Finland: Ministry of the Interior; Imatran Voima Oy (IVO); Teollisuuden Voima Oy (TVO)
In Norway: Ministry of the Environment
In Sweden: Swedish Rescue Services Board; Sydkraft AB; Vattenfall AB; Swedish Nuclear Fuel and Waste Management Co. (SKB); Nuclear Training and Safety Center (KSU)

To this should be added contributions in kind by several participating organizations.

NKS expresses its sincere thanks to all financing and participation organizations, the project managers and all participants for their support and dedicated work, without which the NKS program and this report would not have been possible.

Disclaimer

Abstract

The NKS/RAK-1 project formed part of a four-year nuclear research program (1994-1997) in the Nordic countries, the NKS Programme. The project aims were to investigate and evaluate the safety work, to increase realism and reliability of the safety analysis, and to give ideas for how safety can be improved in selected areas.

An evaluation of the safety work in nuclear installations in Finland and Sweden was made, and a special effort was devoted to plant modernisation and to see how modern safety standards can be met up with. A combination of more resources and higher efficiency is recommended to meet requirements from plant modernisation and plant renovations. Both the utilities and the safety authorities are recommended to actively follow the evolving safety standards for new reactors.

Various approaches to estimating LOCA frequencies have been explored. In particular, a probabilistic model for pipe ruptures due to intergranular stress corrosion has been developed. A survey has been done over methodologies for integrated sequence analysis (ISA), and different approaches have been developed and tested on four sequences. Structured frameworks for integration between PSA and behavioural sciences have been developed, which e.g. have improved PSA. The status of maintenance strategies in Finland and Sweden has been studied and a new maintenance data information system has been developed.

Key words

cognitive factors, control room PSA, HRA, human error, human factors, reactor safety, safety analysis, plant modernisation, LOCA, IGSCC, in-service inspection, initiating event frequency, integrated sequence analysis, intergranular stress corrosion, ISA, maintenance, maintenance outage, nuclear safety, pipe rupture, PSA, probabilistic fracture mechanics, SGTR, shut-down risk, steam generator tube rupture

Summary

The general objective of the NKS/RAK-1 project was to explore strategies for reactor safety as applied in Finland and Sweden. On a more concrete level the project aims were to investigate and evaluate the safety work, to increase realism and reliability of the safety analysis, and to give ideas for how safety can be improved in selected areas. The project has consisted of five sub-projects:

- RAK-1.1 made a survey of safety work in nuclear installations, and addressed the issue how we can assess the suitability and effectiveness of the safety work
- RAK-1.2 tackled the problem of how to improve WASH-1400 values for LOCA frequencies for pipe ruptures and explored LOCA risk dominating mechanisms
- RAK-1.3 addressed how complex event sequences can be analysed with new approaches integrating different disciplines. The concept of Integrated Sequence Analysis (ISA) was introduced
- RAK-1.4 discussed how we can one optimise maintenance and testing with improved maintenance strategies, and developed tools for this purpose
- RAK-1.5 was devoted to plant modernisation and explored how we can meet up with modern safety standards.

In this summary we briefly introduce some of the observations regarding the safety work that came out from subprojects 1 and 5, then we summarise other achievements made in the study.

Some observations regarding the safety work

Subproject 1 made an overview of the safety work in Finland and Sweden and comparisons between the two countries were made. The subproject report is based on extensive interview work done at utilities and authorities. Subproject 5 has explored how the needs for modernisation of the plants are dealt with.

The operation of nuclear power plants demands considerably more resources than was earlier expected. Despite efforts for increased efficiency both utilities and authorities seem to be heavily engaged with work due to reasons such as plant modernisation and plant renovations due to ageing degradation. A combination of more resources and higher efficiency seems to be the way forward. One factor that needs to be taken into account in Sweden is the ongoing decentralisation of responsibilities from the utility headquarters to the reactor sites and the individual reactor

units. Generally this is judged as a positive development provided the individual units get the “critical mass” of competence and other resources for key functions.

The resources and the working efficiency on part of the authorities is also an important issue. There is e.g. a need to evaluate selective approaches for reviewing safety-related modifications. There is accordingly a need to consider possible approaches with regard to increasing the efficiency of inspections and safety reviews performed by the authorities.

The RAK-1.5 report advises both the utilities and the safety authorities to actively follow the evolving safety standards for new reactors, e.g. the development of the European Directives. This is irrespective whether new reactors are planned or not since the new standards may have implications for assessing the safety of the existing reactors as well.

Some NKS/RAK-1 contributions to reactor safety

The NKS/RAK-1 project has contributed to the development of methods to evaluate and enhance reactor safety in many areas. Here some of the achievements are summarised.

Initiating event protection

NKS/RAK-1.2 has produced a model that calculates the probability that a given pipe weld will break due to intergranular stress corrosion (IGSCC). In cases when IGSCC dominates the LOCA frequencies, which may well be the case especially for large LOCA, application of the model has potential to produce PSA results that are not based on WASH 1400 values, but on actual conditions. Such applications will be quite resource demanding since they require a much more detailed modelling of the pipe systems than is usually done in PSA. Furthermore, data will be needed on material data and loading for individual welds. The effort, however, will not just give new PSA results but also data for decisions on risk based in-service inspection.

The approach of probabilistic fracture mechanics needs to be further developed and, above all, applied in real PSA applications. Finally it must be emphasised that an increasing co-operation between PSA experts and fracture mechanics experts is of utmost importance for better estimations of LOCA frequencies.

Integrated sequence analysis

Development and application of methodologies for integrated sequence analysis (ISA) has been a major effort in NKS/RAK-1. There were several reasons for this:

- Problems with the traditional PSA/HRA approach with respect to human performance
- The dynamic evolution of disturbances with interaction between the technical and the human systems in a plant
- A need for feedback from the safety analysis to control room personnel and emergency operating procedures

The project started with methodological surveys that gave a basis for the NKS work. Different methodologies were then tested on four sequences with much of human interaction. The work gave many results and experiences of value for future work in the area. The tested methods showed capability for important contributions, e.g.:

- Structured frameworks for integration between PSA and behavioural sciences
- Improved PSA for certain sequences
- "Control room PSA"
- Improved knowledge about cognitive factors related to procedures
- Feedback to operator training
- Increased understanding of risks associated with maintenance outages
- Use of simulators for event analysis

The NKS project has lead to initialisation of a Concerted Action within the Nuclear Fission Safety Programme of the European Union. The Concerted Action, in which Sweden, Finland and Norway participate from the Nordic countries, will considerably widen the perspective of methods compared to the NKS project.

Maintenance

Subproject 4 has contributed to the further development of maintenance programmes by:

- Exploring the status of maintenance strategies and mapping needs for development in Finland and Sweden
- Development of a maintenance data information system (RelDAT).The system was first installed at the Barsebäck plant
- Testing tools for decision analysis with respect to maintenance programmes
- Bringing insights into the important issue of human errors in maintenance

It is believed that the NKS/RAK-1 contributions will be of value when the utilities develop their programmes for reliability centred maintenance.

The future

Utilities and authorities should now evaluate NKS/RAK-1 achievements in order to see how they can be implemented in the safety programmes. The active utility participation in the project as well as the organisation with a co-ordinating group with representatives from both utilities and authorities should give good prerequisites for this.

The NKS/RAK-1work has highlighted the need for more research and development in a number of areas: evaluation of complicated programmes (such as nuclear safety), application of basic sciences in PSA, evaluation of LOCA frequencies, methods and tools for integrated sequence analysis, and further development of maintenance strategies.

Svensk sammanfattning

Denna rapport sammanfattar resultaten från projektet ***Strategier för Reaktorsäkerhet, NKS/RAK-1,*** som bedrivits inom det program för nordisk kärnsäkerhetsforskning som organiserats av NKS under åren 1994-97.

Målet med projektet, som det formulerades av NKS, var att "utreda hur en tillräcklig säkerhetsnivå kan uppnås i den praktiska verksamheten och vilka krav detta ställer på de strategier och metoder som används". På projektnivå översattes detta till mer konkreta målsättningar: att kartlägga och värdera säkerhetsprogrammet, att öka säkerhetsanalysens realism och trovärdighet, och att öka säkerheten med insatser inom utvalda områden. Projektet har bestått av delprojekt inom fem områden:

- RAK-1.1: Kartläggning och värdering av säkerhetsarbetet
- RAK-1.2: Inledande händelser - bestämning av frekvenser för rörbrott
- RAK-1.3: Integrerad sekvensanalys - specifikt mänskligt felhandlande
- RAK-1.4: Underhållsstrategier och åldring
- RAK-1.5: Ändringsarbeten, renovering och förnyelse

För projektet fanns en samordningsgrupp med representanter från projektets "avnämare" på kraftbolag och myndigheter. Denna grupp fungerade också som styrgrupp för delprojekt 3. Organisationen i övrigt har anpassats efter de olika delprojektens innehåll, behov av styrning och insyn från kraftbolag och myndigheter och i övrigt så att arbetet skulle kunna bedrivas så effektivt som möjligt. Appendix 1 redogör för projektets organisation, och Appendix 2 ger en lista på de rapporter som framställts inom projektets ram. Här sammanfattas först några observationer gällande säkerhetsarbetet i allmänhet som framkommit inom delprojekten 1 och 5, sedan arbetet inom delprojekten 2, 3 och 4.

Utvärdering av säkerhetsarbetet

Det ursprungliga förslaget till delprojekt 1 baserades på en modell där samhällets övergripande säkerhetsmål successivt avsätter sig i mer detaljerade mål för att till slut avspegla sig i det konkreta säkerhetsarbete man gör på kraftverken. Det gällde i stora drag att kartlägga och värdera de aktiviteter som är till för att kontrollera dels om konstruktionsförutsättningarna står i överensstämmelse med målen och dels om anläggningarna uppfyller dessa specifikationer. Det skall betonas att delprojektet inte bara handlade om säkerhetsarbetet på anläggningarna utan också om myndigheternas funktion i sammanhanget. Parallellt med delprojekt 1 gjordes inom delprojekt 5 en särskild insats beträffande ändringsarbeten och modernisering.

Arbetet bedrevs i stor utsträckning med intervjuer på kraftverk och myndigheter. Också danska och norska representanter deltog i arbetet och i intervjuerna på myndigheter och kraftbolag, vilket för deras del bedömdes som en effektiv form för

insyn i säkerhetsarbetet. Här diskuteras några av de iakttagelser som gjordes inom delprojekten 1 och 5.

Säkerhetsarbetet har med tiden kommit att bli mer resurskrävande än vad som tidigare förutsågs. Huvudsakliga orsaker till detta är modernisering och renovering i kombination med särskilda insatser för att dokumentera de befintliga anläggningarna. NKS/RAK-1 rekommenderar fortsatta insatser för att effektivisera arbetet i kombination med tillskott av resurser för att möta detta problem. Detta gäller både kraftbolag och myndigheter.

I Sverige pågår en ökad decentralisering av säkerhetsarbetet så att allt större ansvar läggs på reaktoranläggningarna och även på de enskilda reaktorblocken. Detta bedöms i huvudsak som en positiv utveckling under förutsättning att ansvariga enheter ges en ”kritisk massa” av kompetens och resurser för nyckelfunktioner.

Rapporten från NKS/RAK-1.5 rekommenderar både kraftbolag och myndigheter att aktivt följa den utveckling av säkerhetskrav som sker, inte minst inom EU, med avseende på nya reaktorkoncept. Denna utveckling kan ha stor betydelse också för befintliga reaktorer.

Utveckling av säkerheten inom valda områden

Frekvenser för LOCA

Delprojekt 2 har behandlat frågor avseende bestämning av frekvenser för inledande händelser som kan leda till förlust av kylmedel, LOCA (Loss Of Coolant Accident). Specifikt har delprojektet tagit fram en modell som beräknar sannolikheten för rörbrott beroende på spänningskorrosion , IGSCC (InterGranular Stress Corrosion Cracking), som bedöms vara den effekt som har störst betydelse för stora rörbrott. Tillämpning av modellen i PSA bör därför kunna ge bättre sannolikheter för LOCA än vad som traditionellt tillämpas. Nuvarande värden har i stort sett varit oförändrade sedan WASH 1400 studien (den s.k. Rasmussenrapporten).

Tillämpning i PSA kommer dock att bli resurskrävande beroende på att rörsystemen då måste beskrivas mycket mer i detalj än vad som hittills är vanligt i PSA och data kommer att behövas för enskilda svetsfogar. Resultaten kommer emellertid också att kunna användas för att styra provning av rörsystem på kraftverken. Det är viktigt att få sådan typ av information så att provningen skall kunna göras rationellt utifrån en samlad riskbedömning. Den modell som utvecklats behöver data bl.a. om effektiviteten hos oförstörande provning. Modeller för detta har också tagits fram inom projektet.

Modellen för rörbrott behöver utvecklas vidare, men nu framför allt tillämpas på verkliga rörsystem. Det måste betonas att fortsatta framsteg inom detta område är beroende på ökat samarbete mellan PSA-specialister och materialexperter.

Integrerad sekvensanalys

Detta delprojekt tillkom från ett behov av ökad samverkan mellan olika discipliner för att analysera sekvenser som kan leda till allvarliga tillstånd med avseende på säkerheten. Grundläggande orsaker bakom detta behov är:

- Problem med traditionella sannolikhetsbaserade metoder med avseende på mänsklig tillförlitlighet
- Dynamiken i den händelseutveckling som kan ske efter en inledande händelse återspeglas inte i PSA
- Behov av återkoppling från säkerhetsanalysen till driften av kraftverken, gällande operatörsingripanden och haveriinstruktioner

Inom delprojekt 3 genomfördes först en inventering av metoder för integrerad analys. Avsikten var att göra en relativt bred genomgång av metoder och erfarenheter från integrerade analyser. Således omfattade inventeringen också metoder utanför ramen för vad som brukar betecknas HRA ("Human Reliability Analysis"). Efter metod-genomgången testades olika analysmetoder på fyra utvalda sekvenser:

1. LOCA under avställning (BWR)
2. Kall övertryckning (BWR)
3. Tubbrott i ånggenerator (PWR)
4. Störd signalbild i kontrollrummet (BWR)

De fyra sekvenserna täcker tillsammans ett brett spektrum av händelseförlopp och olika metoder har använts för att analysera dem. Sekvenserna 2 och 3 ger de största möjligheterna till att integrera metoder mellan olika discipliner genom att de innefattar många olika aspekter (PSA, termohydraulik, mänskligt felhandlande mm), medan sekvenserna 1 och 4 är mer specifika. Å andra sidan fokuserar de senare på särskilda problem av generell natur som svåra beslutssituationer i kontrollrummet (sekvens 4) och fel i administrativa rutiner (sekvens 1). Resultat från analyserna bör därför vara av generellt värde. Sammanfattningsvis har framsteg gjorts främst inom följande områden:

- Strukturerad metodik för samverkan mellan PSA och beteendevetenskap
- Mer realistisk PSA för sekvenserna
- ”Kontrollrums-PSA”
- Kunskaper om kognitiva faktorer i hanteringen av sekvenserna (s.k. ”kognitiva profiler”)
- Återkoppling till operatörsträning

- Ökade insikter om riskerna vid avställning
- Användning av simulatorer för sekvensanalyser

Arbetet har också bidragit till ökad samverkan och förståelse mellan tekniska analytiker och beteendevetare.

Strategier för underhåll

Delprojekt 4 har haft som mål att värdera och utveckla metoder för underhåll. I en inledande fas sammanställdes och värderades kunskap om metoder för underhåll av säkerhetsrelaterade system som finns inom och utanför kärnkraftbranschen. Delprojektet har vidare utvecklat ett system (RelDAT) för att analysera och presentera information från olika centrala och lokala underhållsdatabaser. Beroende på användare finns många olika behov att presentera data, och RelDAT kan anpassa sig till detta. Mjukvarusystemet finns nu färdigt för användning och har redan installerats, bl.a. i Barsebäck.

Ett annat moment i delprojektet har varit att analysera rapporter om mänskliga fel i underhållsarbete. Den framtagna metodiken för detta har visat sig mycket användbar för att identifiera vilka typer av del som kan uppstå. En möjlig framtida uppgift kan vara att systematiskt använda sådan metodik för att få data till PSA-analyser. I brist på erfarenhetsbaserade data utnyttjades expertbedömningar för detta i delprojekt 3.

Att utforma strategier för underhåll innehåller många olika aspekter som säkerhet, tillförlitlighet och ekonomi. Delprojektet har funnit att det finns behov av, men också goda möjligheter till, framsteg inom detta område. Bland annat har beslutsanalys testats i detta sammanhang. I ett vidare perspektiv har delprojektet visat på en strukturerad metodik för tillförlitlighetsbaserat underhåll.

Fortsatt arbete

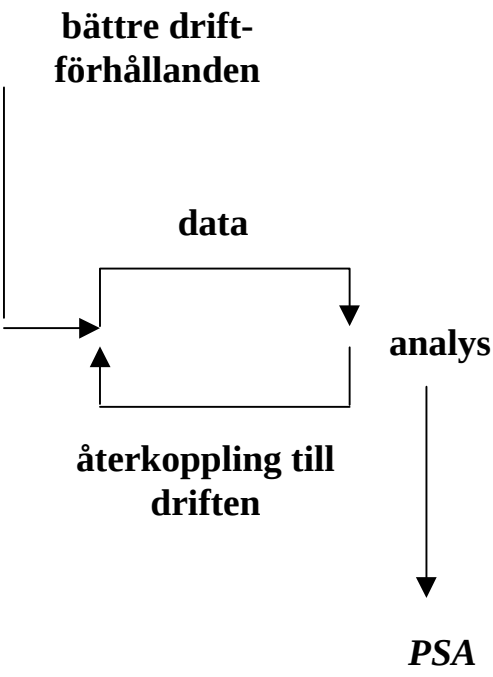
NKS/RAK-1 har utvecklat och provat metoder inom en rad områden som bestämning av frekvenser för rörbrott, integrerad sekvensanalys och underhåll. Resultat och metoder behöver dock i många fall testas ytterligare och framför allt tillämpas i det dagliga säkerhetsarbetet. Kraftbolagens och myndigheternas aktiva deltagande i de olika delprojekten och i projektets samordningsgrupp bör ge goda förutsättningar för detta.

Mycket av arbetet inom projektet har vilat på principen om återkoppling som en grundsten i allt säkerhetsarbete. En verksamhet som inte ger återkoppling är inte effektiv och ändamålsenlig. Figuren på nästa sida illustrerar återkopplingsprincipen när det gäller PSA-verksamheten. Data för PSA måste också ge direkt återkoppling till driftpersonalen. Projektet har kunna bidra till att stärka sådan återkoppling inom ett antal områden, som:

- Samverkan mellan probabilistisk analys av rörbrott och provning av rörsystem
- Samverkan mellan integrerad säkerhetsanalys och arbete i kontrollrum
- Samverkan mellan tillförlitlighetsdatabaser och underhållsstrategier

Delar av det arbete som bedrivs med syfte att höja säkerheten har inte denna återkoppling tillräckligt tydligt uttalad för berörd personal. Förhoppningsvis har NKS/RAK-1 bidragit till en positiv utveckling i detta avseende.

Projektets rekommendationer gäller också fortsatt forsknings- och utvecklingsarbete inom ett antal områden: metodik för att utvärdera komplexa program (som t.ex. reaktorsäkerhet), tillämpning av resultat från grundforskning i PSA, bestämning av frekvenser för LOCA, metoder för integrerad sekvensanalys och utveckling av underhållsarbetet.



PRINCIPEN OM ÅTERKOPPLING I PSA-VERKSAMHETEN

Table of contents

1 Introduction

The NKS/RAK-1 project forms a part of a four-year nuclear research program (1994-1997) in the Nordic countries, the NKS Programme. Other projects of the program deal with severe accident research (RAK-2), emergency preparedness, nuclear waste disposal, ecosystems and information. The program is financed partly by NKS and partly by national bodies. NKS is a Nordic Committee for Safety Research with members from authorities, research organisations and enterprises in the nuclear field.

The general objective of the NKS/RAK-1 project is to explore strategies for reactor safety as applied in Finland and Sweden. On a more concrete level the project aims are:

1. to investigate and evaluate the safety work
2. to increase realism and reliability of safety analysis
3. to give ideas for how safety can be improved in selected areas.

RAK-1 has consisted of five sub-projects (see Table 1.1). Separate summary reports (see Appendix 2) describe each subproject.

Each subproject had a subproject leader. The RAK-1 project was organised to ensure insight and influence from all participating parties. Thus, all subprojects were co-ordinated in working groups composed of members from several of the involved parties, see Appendix 1. As the transfer of results from the NKS programme to the end-users is a particularly important aspect, the project also had a co-ordinating group with representatives from utilities and authorities with special responsibility in that regard. In the later phase of the project, the co-ordinating group also served the purpose as working group for sub-project 3. The project organisation is given in Appendix 1.

The NKS has supervised the project by a reference group. The reference group has been in common for the two reactor safety projects in the NKS programme, i.e. NKS/RAK-1 and NKS/RAK-2 (Severe Accident Research). The chairman of the reference group was also member of the board of the NKS. The total NKS funding for RAK-1 has been approximately 4 000 kDKK altogether for the four years. According to NKS rules each project must have funding from national sources to at least the same level as the NKS funding. In the case of RAK-1 this has been achieved with great margin.

Table 1.1: Subprojects of NKS/RAK-1

SUB-PROJECT	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 scope of RAK-1 has been broad, following the initial directives from NKS. Activities have included broad overview studies as well as development and application of technical methods for e.g. the safety assessment and component data analysis. The focus of the different subprojects can be described using a model for the safety work, illustrated in Figure 1.1. The idea behind subproject 1 was to map and evaluate how general safety principles - reflecting the society's demands for safety - are broken down via safety criteria and rulemaking to specifications of systems and procedures and concrete implementation practices. In chapter 3 we describe how this work was done and give some insights into the findings of the study after a brief description in chapter 2 of how safety is regulated in Finland and Sweden. How the needs for modernising the plants for safety are met was subject to a special analysis in subproject 5, which is related in chapter 4.

Documentation and analysis are key components in the safety work and their importance in construction, operation and maintenance (see Figure 1.1) is a common issue in all five subprojects. Chapter 5, which illustrates how reactor safety may be improved through improved means of assessing the reliability of reactor primary piping, deals with the interaction between testing of passive components and the safety analysis. In the same way chapter 7 (“maintenance”) deals with documentation and analysis of active component failures. In chapter 6 we describe the RAK-1 effort to develop and test methods for the analysis of event sequences that could lead to serious situations. The sequences originate from events during normal operation or shut down conditions.

In the previous NKS programme the SIK-1 project gave considerable attention to the Living PSA concept (Laakso, 1994). Also in the RAK-1 project development and application of safety assessment tools is in focus, especially in subprojects 2 and 3. Furthermore, one of the activities in the RAK-1.1 effort was to evaluate the PSA work and its linkages to other parts of the safety work. In chapter 8 we give some results from this evaluation with special consideration to Living PSA and how it has been applied. Finally in chapter 9 there is a summary of RAK-1 achievements and some recommendations for future work are given.

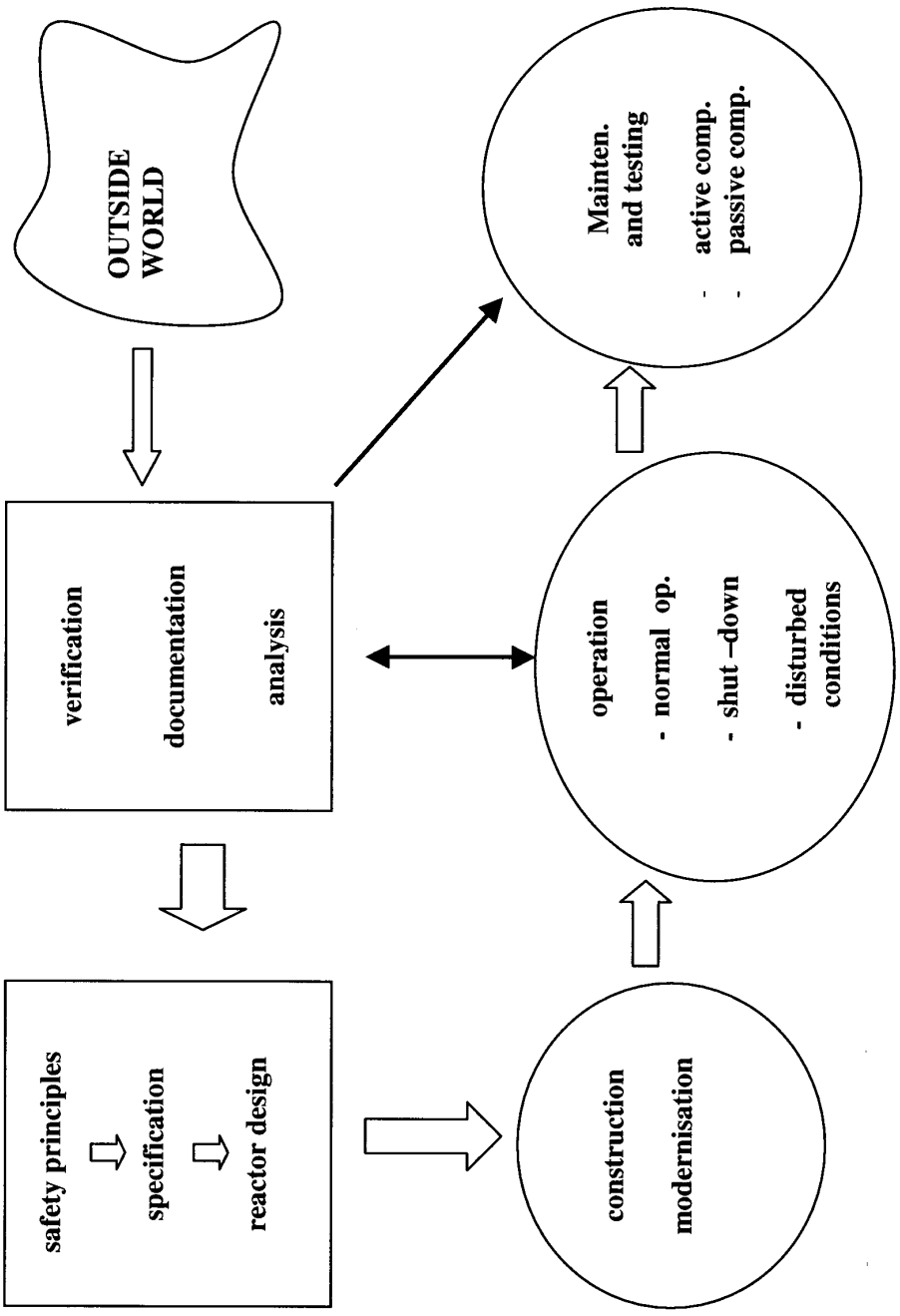


Figure 1.1 A model of the safety work

2 Nordic Regulatory Approaches

As a background to the following two chapters we here describe some of the main features of the regulatory systems in Finland and Sweden on the basis of the sub-project 1 study (Wahlström and Gunsell, 1997). In the report it is concluded that the similarities between the two countries are predominant. The main principle is the same: the utilities have the full responsibility for safety whereas the authorities have the mission to seek assurance that the utilities take this respon-sibility. However, there are also differences.

According to the ”Swedish model”, SKI promotes its safety goals on the basis of the willingness, competence and ability for achieving them as naturally to be expected on part of the utilities, being ultimately responsible for the safety. The aims are similar in Finland, but the approaches differ in the degree to which full and detailed verification against prescribed rules is required.

There is an outspoken strategy of SKI to gain the required assurance of safety by assessing the quality of the processes as being conducted by the utilities, and to lesser extent by taking direct part in double-checking on technical matters. This strategy is for some part forced upon SKI due to having at its disposal significantly lesser manpower resources per nuclear unit as compared with STUK, but it is mainly driven on account of its conceived merits in general. This does not, however, exclude thorough technical assessments being made by SKI in many instances, particularly when dealing with plant modifications of major safety significance.

One difference between Finland and Sweden is that STUK has a set of well-established guides, the YLV Guides, which define, in general, the safety requirements. The practice in Sweden has for long time consisted mainly in applying, for each individual operating license, conditions as required in regard of safety. The reason for the difference between the two countries is mainly historical and relates to the initial phases of the nuclear programme in the two countries. In Finland there was no domestic reactor supplier which meant that the authorities had to develop their own requirements. In Sweden, which had a reactor supplier, ASEA-Atom, the basic safety principles as developed in USA were directly included in the design process.

The YLV Guides have been subject to considerable development in recent years due to the fact that a fifth reactor was planned in Finland in the first part of the 1990s although the plans ultimately were abandoned. In Sweden, general rule-making is in progress since 1993 when SKI was granted the required legal competence for this by the Government.

There is a notable difference between the STUK YVL guides and the Swedish general rulemaking in that the latter aims at being legally binding which is not the case for the YLV Guides. The application of the YLV Guides is subject to confirmation in each specific case, in terms of conditions actually imposed by STUK for the operating licenses. The particular advantage of the Finnish YVL guide system lies in effecting consistency of the safety requirements at an advanced level while avoiding the disadvantages of legally binding rules in having to be complied with by all reactors representing various generations.

In Finland, the operating licenses are typically granted for 10 years. The required renewal of the licenses in Finland provides for thorough re-assessment of the overall safety of the nuclear plants, largely on the basis of a compilation of the inspection and assessment work done during the previous license period. The license renewals thus serve as an important complement to the ongoing inspection and assessment activities.

In Sweden the operating licences are usually not limited in time. The purpose served by the licence renewals in Finland is instead served by periodic safety reviews, the ASAR programme. ASAR has been concerned, in particular, with management and quality issues, performance records, past and current safety issues and plans for future safety improvements. The efforts were in the early eighties for a large part devoted to developing the PSA methodology and undertaking the first plant specific PSA analyses. The reviews of the first and second generations of the Swedish reactors have all been completed in the second ASAR round. The first ASAR round is about to be completed for the newest reactors, i.e. Forsmark 3 and Oskarshamn 3.

The safety targets applied in Finland and Sweden, in regard of limiting the probabilities for core damage accidents and severe releases, remain similar and essentially in agreement with previously established international recommendations (IAEA). Strict limits in regard of quantitative releases in the event of severe accidents apply since the eighties, essentially equivalent to those presently proposed for the European Utility Requirements (EUR) regarding releases of radioactivity causing land contamination.

3 Insights into Reactor Safety Work

The RAK-1 project included two subprojects that addressed the problem of assessing how the safety work meets its objectives. Figure 3.1 illustrates the problem. Subproject 1, described in this chapter, was broad in scope whereas subproject 5, described in the next chapter, focussed on plant modernisation.

3.1 To map and evaluate the safety work

It is not obvious how to ensure that specifications of systems and procedures, as well as their practical implementation, harmonise with the overall safety objectives set by society. There are a large number of safety activities set up by the utilities and the authorities to achieve this, but still three questions should be addressed:

- Is the safety work adapted to its purpose and adequately comprehensive, or are there gaps?
- Is the safety work well balanced and efficient?
- Are the persons involved in the different activities aware of their roles in the total safety work? Do they ask proper questions? Do they get correct answers?

Initially was intended to develop a simplistic conceptual model of the safety work (Figure 3.1) into a more detailed ”map” for better overview of the various interrelated activities and improved understanding of how they work together in providing for the required safety. Having such a map it should be possible to address these questions and to evaluate the safety work.

A working group with representatives from authorities, utilities and research organisations was set up for the work. Eventually it was decided, because of the magnitude and complexity of the task, that the project would be confined to suggesting how such ”mapping” could possibly be done in practice and providing instead a thorough description the safety work from a number of different perspectives. This has been done in a systematic manner in the RAK-1.1 report.

The problems associated with the development of a good and detailed map of a complex reality, such as nuclear power installations, can be explained with organisational theory. According to Ashby (Ashby, 1994) and Espejo et.al. (Espejo et.al., 1996) the complexity of an organisational system must be reflected in its

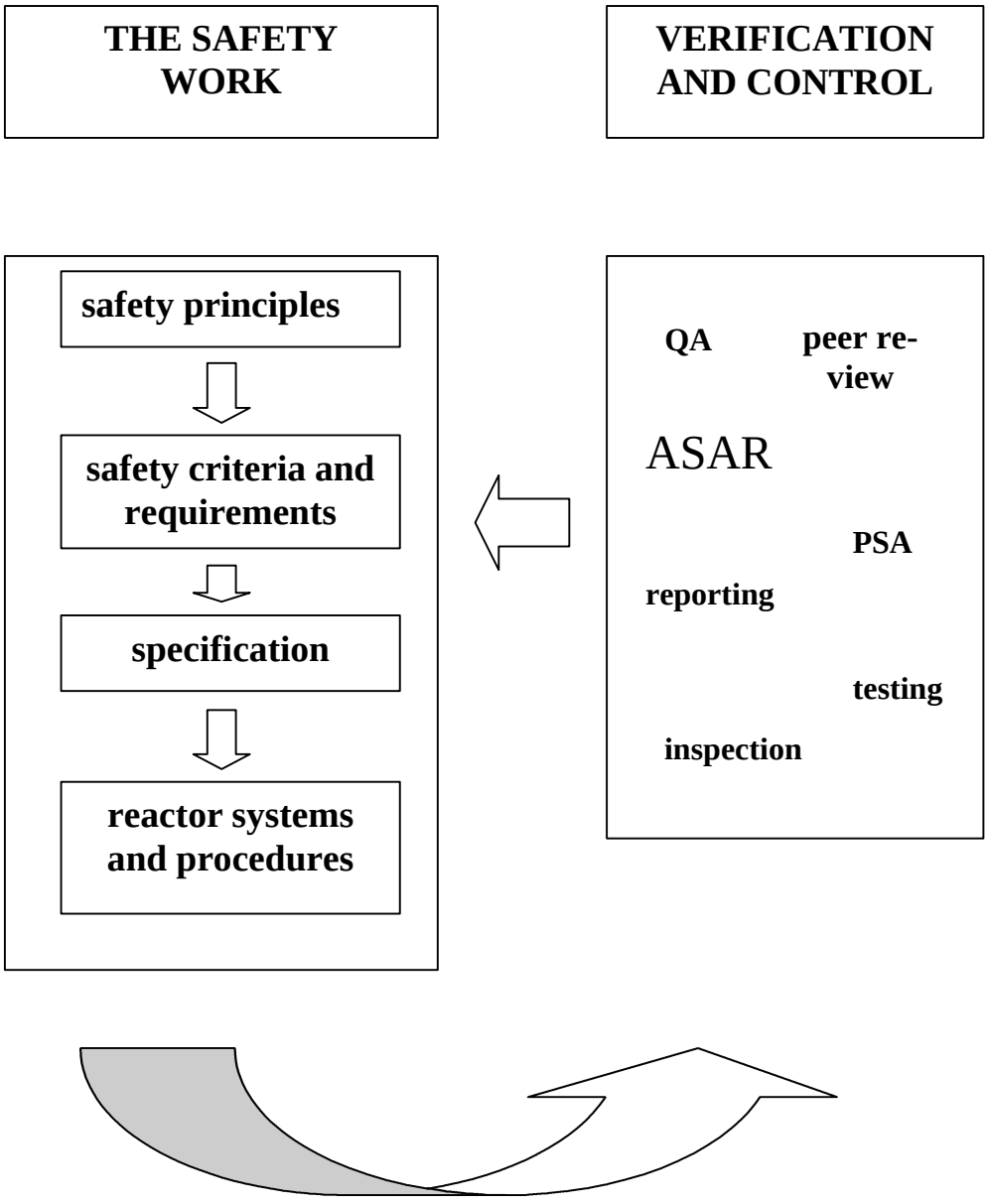


Figure 3.1 The RAK-1.1 problem: to map the verification and control processes, how they link together, how they supervise the design process and the fulfilment of safety principles and specifications

control systems. A simple map may thus be trivial and a more complicated (better) one may be too difficult to overview and share between people.

The subproject report (Wahlström and Gunsell, 1997) is based on extensive interview work done at utilities and authorities in Sweden and Finland. Some activities were studied more in detail. These were the safety analysis, experience feedback, and review work. The PSA activity was subject to a special study (Andersson, Johansson, Karnik and Stokke, 1997). Finally, modernisation work was studied in particular in subproject 5 (see chapter 4). In order to understand certain aspects more deeply the RAK-1.1 study focussed on case studies (a fire at TVO, erroneously adjusted safety valves at Ringhals, modernisation of Oskarshamn 1, and a strainer event in Barsebäck).

The RAK-1.1 report includes a normative model of the safety work with a few basic principles about organisation, planning, models, information handling and experience feedback. Evaluation can thus be done by comparing the findings from interviews, case studies and analysis of activities with the normative model. Another way to get insight into the safety work in Finland and Sweden was to compare practices in the two countries. A special study was performed to compare how the safety authorities STUK and SKI work (Wahlström, Nyman and Reiman, 1997).

3.2 Some observations

For an account of study results the reader is referred to the RAK-1.1 report. Here we only give some general observations.

It appears that the operation of nuclear power plants demands considerably more resources than was earlier expected. There was a conception that after the construction phase there would follow an “administrative” phase that should be less demanding. Instead, the amount of work seems to have increased during the latest years due to a number of reasons:

- Although the reactors were designed according to basically sound safety principles, they were not perfect, and some deficiencies have been discovered, which have required large plant modifications.

- The reactor plants and early modifications have not been fully documented, which in Sweden have caused the initiation of large projects for the reconstitution of FSAR.

- In the early phases it was not fully recognised how important documentation would be for the daily work. Means and procedures for this need to be further developed. Modern development of software tools provides efficient means for this, as demonstrated by (Strandell, 1997). These tools also give ample oppor-

tunities to build in feedback to the plant operation and maintenance, something which is necessary for efficient documentation and improved operations.

- Now also modernisation is needed for a variety of reasons. One reason is that the equipment becomes obsolete and needs to be replaced, another is that modern safety requirements have impact also on older reactors. It has been shown that modernisation projects require much time and consideration at both utilities and safety authorities.

The RAK-1.1 work leads to the conclusion that the industry is overloaded with work despite efforts for increased efficiency, and that measures need to be taken in order to improve the balance between goal setting and resources. Another area that needs attention is the on-going decentralisation of responsibilities, sometimes combined with dividing central functions into smaller units outside the mother organisation. Basically, this is a positive development that enhances the safety culture by increasing the responsibility of smaller groups and individuals. The development is fully consistent with trends in modern management and is also enhanced by new information technique.

However, decentralisation may not always be consistent with reducing resources. In order to take responsibility for a certain area there must be a “critical mass” of competence at the site. In addition, the development of the Living PSA concept requires both increasing resources and that the individual reactor units take a high degree of responsibility for the conduct of PSA. Furthermore, Living PSA also means that groups in e.g. operational units take part in the PSA work. It may be that this altogether means increasing, rather than decreasing, resources for the PSA work.

3.3 The goal-means-feedback loop

As emphasised in RAK-1.1 all activities in the safety work need goals, means and feedback in order to be effective, see Figure 3.2. An activity that can not be described with such a loop needs improvement. Again, PSA can be used to illustrate the issue. Sometimes groups of personnel have been required to provide data to PSA as a “distant” activity (Figure 3.3a). This would give little involvement of the data producers and possibly low quality data for PSA. If the data gathering and analysis could give direct feedback to the operative activities the situation would be much improved (Figure 3.3b). Much of the work in RAK-1 subprojects 2, 3 and 4 had the purpose to establish such interaction between data analysis and operation. We will thus come back to the feedback loops later in this report.

3.4 Information handling

The nuclear industry has considerable problems in managing the vast amount of information associated with operation, maintenance and modification of the nuclear

plants so as to ensure keeping all data properly updated. For example a single modification may generate need for updating maybe 20 documents. It is also important to document work routines. Within RAK-1.1 a study was made, as a masters thesis ("diplomarbete") of how formal modelling techniques may be used for description and documentation of safety related procedures in order to facilitate review for completeness and consistency (Strandell, 1997).

The goal of the masters thesis was to find a method, with which safety related work in nuclear power plants can be modelled. The intention was that the constructed models would be easy to review in order to get an overview of the safety work and how its components are related to each other.

A few modelling paradigms were examined. Of these OMT (Object Modeling Technique) was considered best suited for the purpose for a number of reasons. OMT is an object-oriented analysis method, in which the real world is divided into objects. The real world is explained by defining the meaning of the objects and by explaining the relationships between different objects. From a model of a work routine, a relational database management system, RDBMS, can easily be constructed. The RDBMS combined with the original model can be used to check that the work routine is carried out consistently. Models constructed with OMT are clear and expressive. Complex systems are handled with decomposition. Existing models are easy to extend and can also be combined with each other.

The study examined OMT by applying the method to various components of the safety work. In addition it showed how RDBMS's can be constructed on the basis of OMT models. The applicability of the modelling technique was demonstrated with a few examples concerning work routines at the Olkiluoto nuclear power plant. Parts of the protection system of the reactor were considered, as well as a maintenance work order system. A way to check that the maintenance work is carried out in the way that quality assurance system implies was presented.

The results indicate that OMT is a versatile and expressive modelling technique, with which models of the various routines and activities that the safety work consists of can be constructed. These models can be combined with modern information technology in order to verify that the safety work is carried out in an appropriate manner and to assure that nothing important is left out. In the future OMT-methodology may be used to improve the work routines that are in use today.

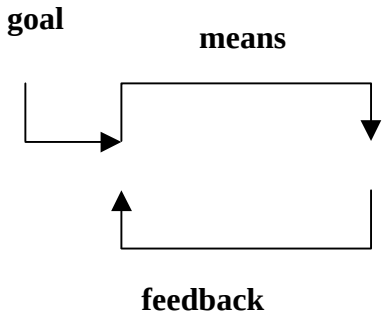


Figure 3.2 The feedback loop principle

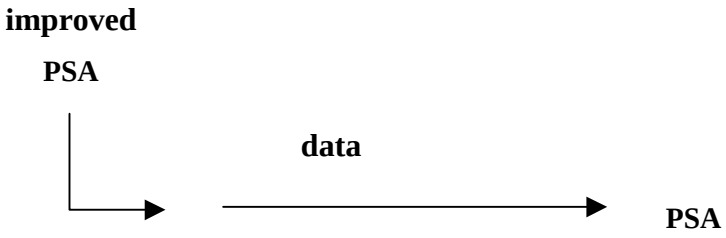


Figure 3.3a Data production for PSA

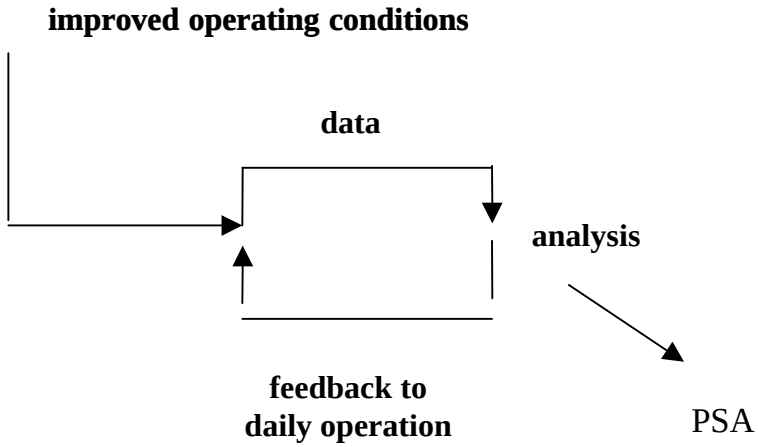


Figure 3.3.b Data analysis in support of operation and for PSA

4 Modernisation for Safety

Background

The design, construction, maintenance and operation of the nuclear plants are all subject to fairly frequent modifications both in Sweden and Finland. Major modification projects have also been conducted. This development will continue also in the future. There is e.g. a need to change control room equipment in several of the reactors within the coming decade because the currently used technology is becoming obsolete.

Obviously, for any attempted modification, careful consideration of the safety implications will be necessary to ensure, at the very least, that safety will not be impaired. The implementation of new technology for improving the safety raises, in itself, questions about possibly associated new risks, and how to ensure that the expected safety benefits will be gained in practice. The advanced software based digital control systems, offering not only great potentials but in addition some unusually intricate quality assessment problems, is a good example.

On the other hand, proposed modifications of the nuclear plants, e.g. for enhanced performance or economy, offer additional opportunity for pursuing improvement of safety. This is partly as the safety authorities will become directly involved in their capacity of granting required permits. Modern regulatory development will also have an impact on older reactors, as the safety requirements will increase.

Study approach

The RAK-1.5 study aimed at assessing and comparing strategies and practices at the nuclear utilities and the authorities in Finland and Sweden for ensuring that the nuclear plants keep reasonably well in pace with the development in regard of safety, considering new knowledge and technology, operating experience and generally advancing safety requirements. Information and views were obtained by means of questionnaires and interviews at the plants and at the safety authorities.

A formal modelling technique was used to describe the procedures involved in the modification process. The approach taken, largely in accordance with the so-called Structured Analysis and Design Technique, SADT (Ross, 1977), proved to be quite helpful, allowing the processes to be broken down in detail as required to account fully for all factors. The modelling focuses on the basic concepts of processing inputs, outputs, controls and resources. It aims at facilitating review of the process for completeness and consistency of applied procedures. Figure 4.1 shows the model structure, and Figure 4.2 gives an example of how the technique was applied.

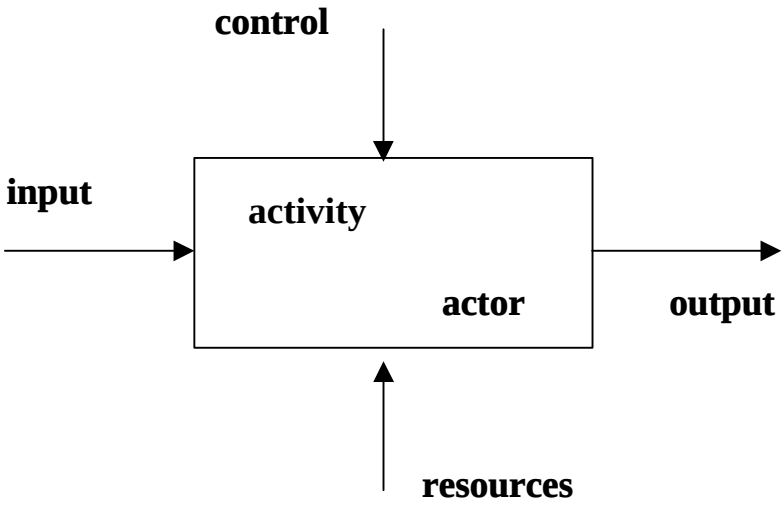


Figure 4.1 Formal modelling of activities, the SADT technique

Approaches to modernisation

The corporate strategies in regard of modernisation reflect the desire of the utilities to stay in reasonable control of the future of the business by maintaining the plants at highest possible performance/cost ratio and preventing at all times the operation of the plants to be questioned in regard of their safety.

The main strategy of the safety authorities consists in actively promoting continuous improvement of safety by repeatedly questioning the current safety level in relation to safety standards and technology and current methods for assessing the safety. The utilities are, furthermore, required by the authorities to consider, at all times, making safety improvements whenever appropriate and reasonably achievable.

The needs for modernisation with regard to safety are explored by the safety authorities in dedicated inspections and safety reviews, in reviewing applications for ***relicensing*** of the plants, as practised mainly in Finland where licenses are typically granted for ten years, and in ***periodic safety reviews*** of all plants at intervals of about 8-10 years, as practised in Sweden.

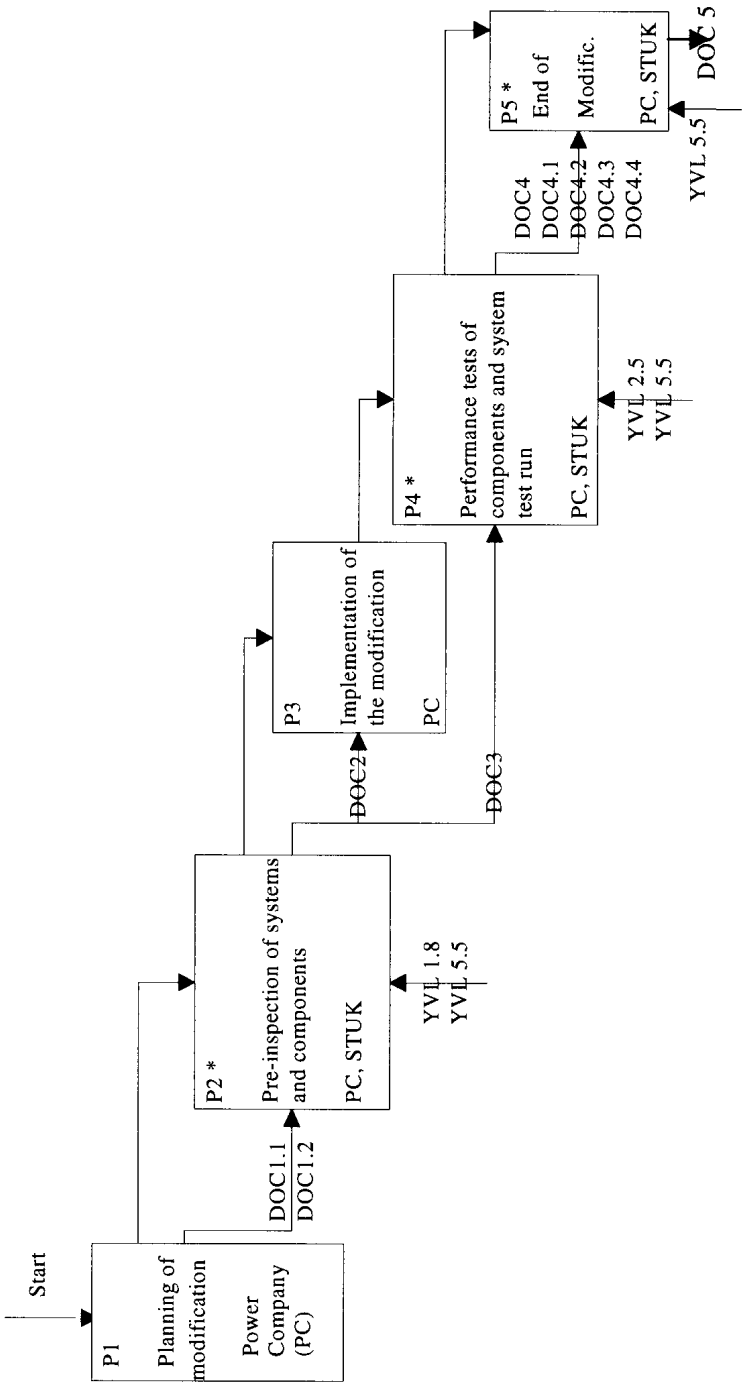


Figure 4.2 Application of the SADT technique with an example from TVO. Modification of a system consisting of electrical and instrumentation components

The procedures in Finland and Sweden follow largely a common pattern. There is a difference, however, in that the Finnish safety authority requires to review and approve, in principle, all safety related modifications while the Swedish authority requires to be presented with all planned modifications for selection of those requiring regulatory review and approval.

Experiences

Major modernisation projects are now, since 1994, under way for the two BWRs at Olkiluoto and since 1996 at the two PWRs at Loviisa. The projects aim mainly at verifying the safety, increasing the power rating of the reactors, improving the thermal efficiency and providing for life extension; all on the basis of recent engineering developments and accumulated experience. They include renewal of a number of main components, mainly in the turbine and electrical generating systems.

The early generations of the Swedish reactors are presently due for comprehensive modernisation efforts. Also the recent generations of reactors are subject to ongoing, long-range investment programmes aimed at meeting the future demands as foreseen for the first decades of the new century. All current modernisation plans still continue to be pursued despite the recent decision taken by the Swedish Parliament, in June 1997, to commence winding up the Swedish nuclear programme by phasing out one of the Barsebäck units (BWR) by 1 July 1998.

The renovation and modernisation of the Oskarshamn 1, the oldest Swedish reactor and essentially a prototype of its kind, is illustrative. Complete reconstitution of the design basis is aimed at so as to meet the safety targets at par with modern reactors, for large part also in compliance with modern design principles.

Some observations and recommendations

In comparing the actual course of actions with prescribed procedures, it can be noted that this does account for the possibility that additional requirements may be made in response to proposals received by the authority. The problems encountered in handling modifications in a safe and reliable way seem often to be related to too tight time schedules. In some cases, it may be advisable to consider temporary modifications in order to give some more time for finding the best possible solution and PSA needs to be early involved in the planning process.

The utilities should consider applying formal modelling of the management and the processing of plant modification, for further improved management control of plant modification work.

Certain weaknesses could be identified in regard of the rigour of the Swedish practice in selecting the modifications that require regulatory review and approval. The

safety authorities should thus evaluate concepts of selective approach to review safety related modifications to economise with the available resources.

Finally, the RAK-1.5 report advises both the utilities and the safety authorities to actively follow the evolving safety standards for new reactors, i.e. the development of the EUR, in regard of their implications for assessing the safety of the existing reactors as well as their possible application to them.

5 Protection against LOCA

5.1 Initiating event frequencies

The ultimate purpose of all reactor safety work is that severe events must be avoided. The reactors were constructed in accordance with a few basic safety principles aimed to prevent from severe events. One of these principles is that of *safety defence in depth* which says that there should be multiple physical barriers to confine the radioactivity and multiple provisions for defending the barriers, should an initiating event occur with potential impact on safety. Defence in depth thus consists of both technical safety systems and human performance. In the next chapter we deal with methods to analyse sequences following an initiating event. I this chapter, however, we deal with the initiating events themselves. As a starting point we take the perspective of probabilistic safety assessment (PSA). PSA often use core damage frequency (cdf), i.e. the calculated probability per year for core damage, as measure.

Figure 5.1 shows the dominating events leading to core damage in a BWR with internal main circulating pumps (MCPs) according to (Gunsell , Forss and Andersson, 1997). The figure shows that some initiating events occur relatively often. This is the case e.g. for transients that occur more than once per year. For such events the reactor system must have enough barriers so that the calculated cdf becomes sufficiently small. For large LOCAs, the initiating event frequencies are much lower than the average LOCA value shown the figure. For such cases, the low frequency of the initiating event is itself an important safety function. However, in order to keep the required reliability of the safety systems at a reasonable and realistically achievable level, it is obviously essential to ensure good verification that the initiating event frequencies are indeed as low as being assumed.

In current PSA studies LOCA has a rather rough modelling with the pipe ruptures classified in large, medium and small LOCAs, which is in accordance with the WASH-1400 study from 1975. This is a mismatch with other parts of the PSA in which components with safety functions and their electrical and physical dependencies can be modelled with a high degree of detail. Also some initiating events such as “loss of external grid” are modelled in detail with probabilistic techniques. Furthermore, the frequency values for LOCA are still mostly assumed to be the same as in WASH-1400. Altogether this is not a satisfactory situation if the goal with PSA is to reveal potential weaknesses in the safety barriers and to provide a basis for prioritisation off safety improvements of the plants.

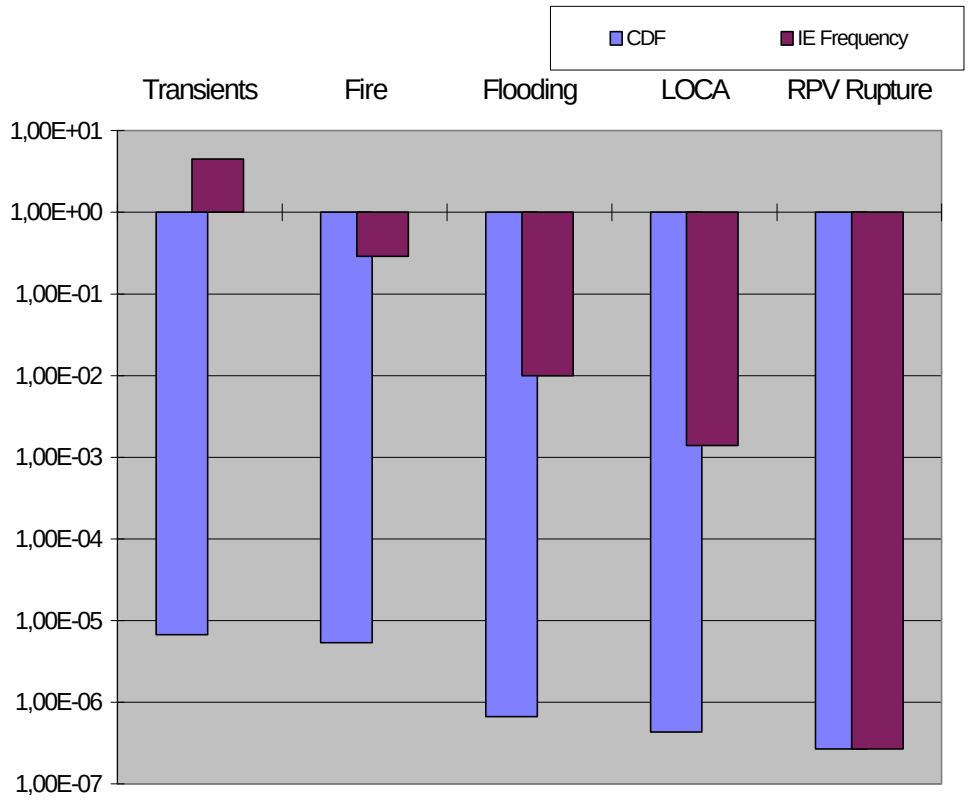


Figure 5.1 Dominating events leading to core damage in a BWR with internal main circulating pumps (Gunsell , Forss and Andersson, 1997)

5.2 Risk based in-service inspection

Already from the PSA point of view there is thus justification for an increased level of detail in the LOCA modelling, i.e. in probabilistic fracture mechanics, PFM. There is also a reason from the operational point of view (Gärdinge, 1997). In the Swedish regulations is required that a full volumetric inspection should be done on welds that, if failing, could cause a LOCA accident. In practice, it is clear that a 100% volumetric test of some test areas is not possible during a single outage due to e.g. radiation doses. Furthermore, the contribution to the cdf of a particular weld is time dependent due to crack growth. A detailed modelling of pipe break probabilities and locations would thus allow to select the areas where the in-service inspection (ISI) should be conducted during a set of outages, i.e. we would have risk based ISI.

Furthermore, performing ISI in an environment with heat, small space and radiation is a difficult task. It is then especially important that the personnel doing ISI is aware of the safety importance of good performance. A risk based ISI would enhance this awareness. This a good example of a feedback loop discussed in Chapter 2 (see Figure 5.2). Risk based inspection will give:

- optimised inspection intervals
- higher motivation for in service inspection
- better data for PFM and PSA

In the end this way of looking at ISI leads to a complete testing of all areas susceptible to have any probability for a break or wall-through crack, although the frequency of inspection would vary between individual welds depending on risk based considerations.

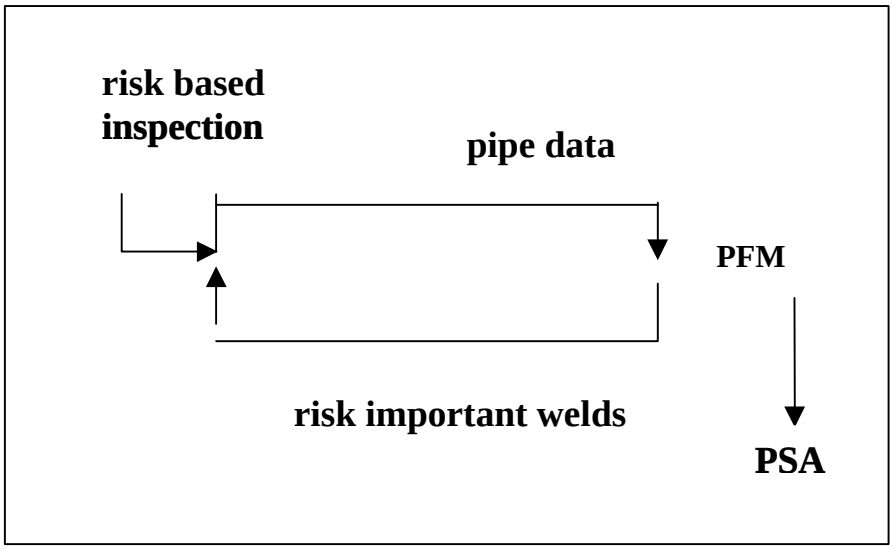


Figure 5.2 Risk based inspection gives pipe data to PFM/PSA and information on risk important welds for optimised inspection intervals

5.3 A case study: IGSCC

Background

From the previous sections it is obvious that there are good reasons to improve the probabilistic modelling of pipe rupturing. For the engineered safety systems fairly reliable failure frequencies are available and databases exist that can be used in the assessment. For other types of equipment such as pipe systems this is only the case

to a limited extent. Especially, for pipes with large diameters for which ruptures could cause large LOCAs there have been no ruptures in nuclear plants, and this state of affairs precludes any estimation of the failure probability based on observed data. Instead, analytical methods have to be used to estimate the failure probabilities. It should, however, be observed that this would have been the case also if a few large ruptures had really occurred (the failure frequencies would still be very uncertain).

Efforts to develop analytical methods have so far been limited to Intergranular Stress Corrosion Cracking (IGSCC), which both theoretical considerations and practical experience (Bush, 1988) indicate is the most important process for pipe failure in Boiling Water Reactors. An early procedure, developed by Nilsson et.al. (Nilsson, Brickstad and Skånberg, 1990), was a simplified model taking into account randomness in initial crack lengths, crack initiation rate, crack detection capability and loads. The work within NKS/RAK-1.2 builds on this experience.

The model

The goal of the NKS/RAK-1.2 study was to develop a procedure with accompanying computer software that can be used to estimate the failure probability for a specific pipe section with prescribed local loading. The failure probability is strongly dependent on the actual loading conditions which makes it necessary to treat pipe systems on joint by joint basis.

The model (Bergman, Brickstad and Nilsson, 1997) is intended for calculation of the failure probability of a specific pipe cross section with a certain stress state and possibly containing a circumferential crack growing due to stress corrosion cracking. A number of assumptions were made for the probabilistic analysis:

- The stresses are deterministic
- The crack growth is deterministic
- The initial crack depth is fixed to 1.0 mm
- The initial length of the crack is random (based on Swedish distribution data)
- The probability of not detecting a crack at an in-service inspection depends on crack length and crack depth (the actual function used was not dependent on the crack length, but a possible dependence on length is retained in the general equations)
- There is a detection limit for leakage flow, and above this limit there is a probability of not detecting a leakage flow.

Due to the assumptions made, the growth of the crack will be deterministic and will only depend on the initial crack length for a given geometry and given stresses. A procedure for calculating growth of such cracks was developed, resulting in a computer code named PIFRAP. Probabilistic data to the code are:

- The probability that a crack with an assumed depth is initiated during a certain time interval
- The initial length of the crack (initial crack length/depth is calculated from statistical data backwards, to a calculated length when the depth is 1 mm)
- The probability of not detecting a crack at an in-service inspection
- The probability of not detecting a leak rate for a given leak rate detection limit

In addition the code requires deterministic data on pipe geometry, loading conditions and material data.

It was the intention of the project to formulate the procedure and the software in such a way that operators of nuclear facilities can use it as an instrument in their continuing safety assessments. The structure of the model was thus made simple and robust as well as easily adaptable to changes of input assumptions such as probability distributions.

Variations

In order to check the model and to obtain some information about the importance of different quantities a number of computer runs were performed. A specific set of data referred to as the basic case was defined from which variations of parameters were performed as a sensitivity analysis. Some observations from the sensitivity analysis are:

- Leakage detection is a very important factor to obtain a low failure probability
- Inspections must clearly be done with intervals less than 10 years in order to give a real reduction of failure probability
- The failure probability varies orders of magnitude between pipe diameters (less probability for large diameters)

For more information on the PIFRAP code and results from the variations the reader is referred to the report (Bergman, Brickstad and Nilsson, 1997).

Detection probability

As illustrated by the PIFRAP variations the leakage detection probability is a very important factor. The PIFRAP code uses data from (Simonen and Woo, 1984). Within NKS/RAK-1.2 there was also an effort to estimate this factor. The report (Simola and Pulkkinen, 1997) describes the use of statistical models for the evaluation of the reliability of ultrasonic inspections. The objective of this study was to model the uncertainty in the flaw size determination, and the flaw detection probability as a function of flaw size. The approach is based on the modelling of the flaw size as a random variable, and two alternative models were applied.

In the first model, a lognormal model for the flaw size was considered. This is an assumption which has been commonly used in reliability analyses of non-destructive examinations. The second model introduced is based on the logit transformation of the relative flaw size. In order to illustrate the use of these models, they were applied to flaw detection and sizing data from the PISC III exercise (PISC-III Report no 33, 1995). Based on the models and the statistical data, the flaw sizing performance was evaluated and the probability of flaw detection was estimated. The models applied in this study could be routinely used to evaluate the performance of ultrasonic inspection teams. However, this requires rather extensive calibration measurements in order to reliably estimate the model parameters and to make statistical inferences on the teams' performance.

5.4 International data bases

Independent of the NKS/RAK-1.2 project, the Swedish Nuclear Power Inspectorate (SKI) in 1994 initiated a 4-year R&D project on piping reliability, the SLAP Project (Nyman et.al., 1997). The technical scope included the development of an analysis framework for the estimation of piping reliability parameters from service data. Based on systematic analysis of the service experience with piping systems in nuclear power plants worldwide, the SLAP project was prompted by requirements for an integrated, "data-driven" analysis approach to support PSA applications. The project responded to one basic PSA-oriented question: Does the worldwide industry experience with leaks and ruptures change the consensus perception of small-, medium- and large LOCAs?

A consolidation of insights and results from NKS/RAK-1.2 and the SLAP project was pursued through an international seminar on piping reliability (Seminar on Piping Reliability, 1997). From the Nordic perspective, the merging of insights from the two projects has broadened the analytical perspectives on piping reliability analysis as it applies to LOCA frequency estimation.

5.5 The way forward

The NKS/RAK-1 project has produced a model that calculates the probability that a given pipe weld will break due to IGSCC. A practical application to a plant specific PSA remains to be done. The Oskarshamn 1 power plant is a good candidate for a first application since an earlier study had provided a detailed PSA model for the pipe systems. In this study the pipe components were grouped into a number of categories and engineering judgement was used to estimate relative rupture frequencies with weighting factors between the categories. Finally, however, the total rupture frequency was normalised to WASH 1400 values. The total pipe rupture probability was thus assumed to be the same as in WASH 1400 whereas an improved basis was provided for estimating the probability distribution beween various pipe break categories.

The Oskarshamn 1 PSA model contains all pipe joints in the plant (about 3 500). The application of PIFRAP to the PSA model requires input data in principle for all welds. It remains to be seen whether all welds should be treated individually or if one can find some reasonable basis for grouping into categories. The results of such an effort will be data that can be used for designing the in-service inspection program and for new core damage frequencies for IGSCC. If IGSCC dominates the LOCA frequencies, which may well be the case especially for large LOCA, this will be a PSA result not based on WASH 1400.

If, however, as the SLAP project suggests, the “traditional“ causes (such as IGSCC) is only a limited part of LOCA events, the model approach to the estimation of LOCA will only be able to take care of a limited part of the problem. In that case we would also need to rely on the data base approach, as applied in SLAP, to LOCA frequencies. It may be that the roles of the two approaches will vary between different pipe diameters. In particular in one end of the scale, for large diameters, there will be no real statistical data for ruptures. In the other end of the scale causes like design failure and human error, which hardly can be modelled by the PFM approach, may dominate.

The PFM is likely to contribute considerably to improving the assessment of the pipe rupture probabilities. However, this approach should be combined with continued, comprehensive follow-up of all operating experience related to cracking phenomena, to be collected in data bases, in order to provide for the basic understanding required in preventing pipe ruptures from at all occurring. It can thus be concluded that both the modelling approach and the data base approach have a role and that they need to be further developed and applied. Both approaches will require increasing co-operation between PSA experts and fracture mechanics experts.

6 Integrated Sequence Analysis

6.1 The importance of barriers and human interaction

Figure 6.1 shows the dominating events leading to core damage in a PWR PSA analysis (Gunsell , L., Forss, A. and Andersson, 1997). As Figure 5.1 was taken as an incentive for improving the analysis of initiating event frequencies, Figure 6.1 illustrates the use of improved analysis of certain event sequences.

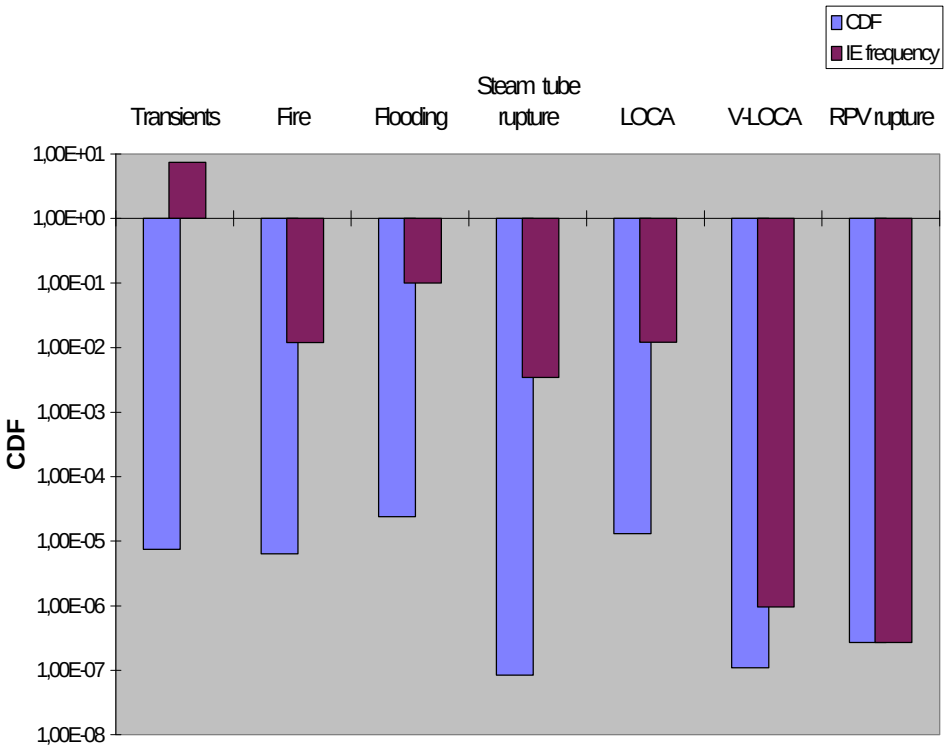


Figure 6.1 Dominating events leading to core damage in a PWR (Gunsell , Forss and Andersson, 1997)

The figure shows for example that the steam generator tube rupture (SGTR) frequencies are relatively high (in the order of 10^{-2} per year), whereas the associated core damage frequency is several orders of magnitude lower (in the order of 10^{-7} per year) in the PSA. This shows that there are significant barriers against a severe accident, but also that the functioning of these barriers is critical. This motivates a

thorough analysis of the event sequence, especially when taking into account that the sequence is complex with many interactions between the technical reactor system and the operators.

Another important event is fire as can be seen from both Figures 5.1 and 6.1. This is a case where the operators could be mislead by disturbed signals in the control room, due to a damaged signal system.

One type of initiating events, not included in Figures 5.1 and 6.1, are events during the shut down period that eventually could lead to LOCA and core damage. Also in this case the human factor is important, e.g. due to possible mistakes during maintenance or inadequate administrative systems.

All these event sequences (SGTR, confused control room signals and serious events during the shut down period), in which human performance is important, have been subject to special analyses in Subproject 3.

6.2 Why integrated sequence analysis?

Probabilistic safety analysis, PSA, has been developed as a comprehensive framework for the analysis of reactor safety. However, the probability estimates of human failure events often vary considerably and their basis are vague in many cases. The completeness problem of PSA is also well recognised, especially with respect to human error. 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 illustrated by Figure 6.2.

It has thus been recognised that further development is needed to complement existing methodologies for safety analysis with more fully integrated approaches to the interaction between human and technological systems. There are many methods that potentially could be building blocks in integrated approaches. Most probably each one of the methods has its own merits and limitations and may be best suited for certain types of application. The overall goal of NKS/RAK-1.3 has been to develop and test methods for integrated sequence analysis (ISA).

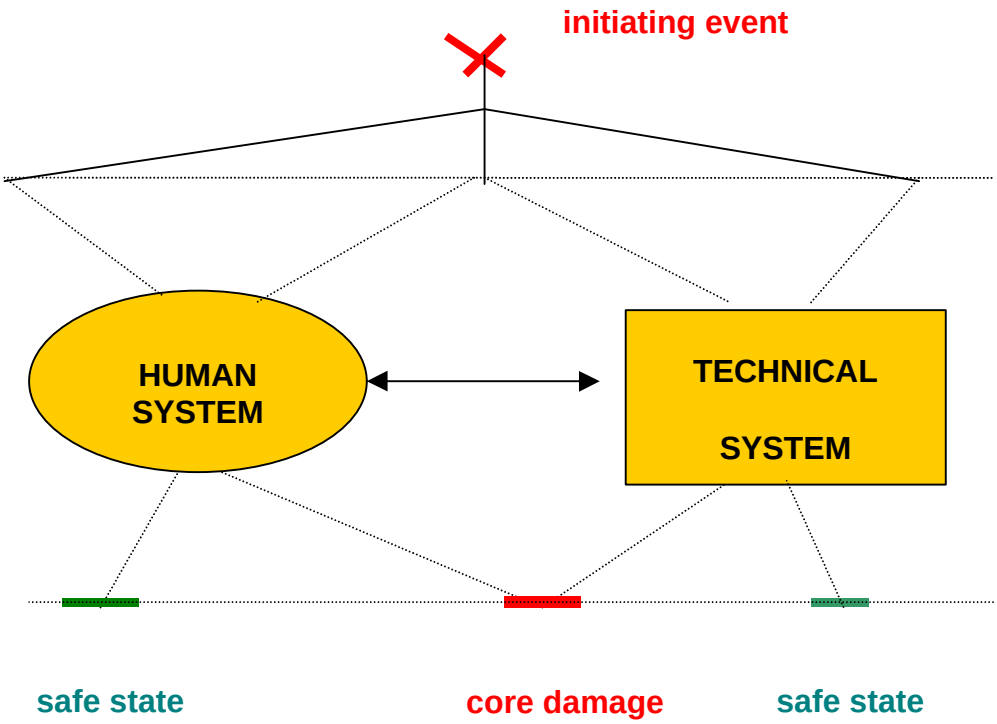


Figure 6.2 Event sequences are complex interactions between the human and the technical system. The task of ISA is to analyse how sequences leading to unwanted end states can occur and how to avoid them

So far we have mentioned the PSA perspective and the dynamic nature of events as motives for ISA. As a third reason we can go back to our feedback loops, in this case in terms of interaction between PSA and the operators. Figure 6.3 illustrates that ISA should give feedback to the operators e.g. in terms of evaluation and possible improvements of the emergency operating procedures, apart from contributing to PSA with estimating human error probabilities.

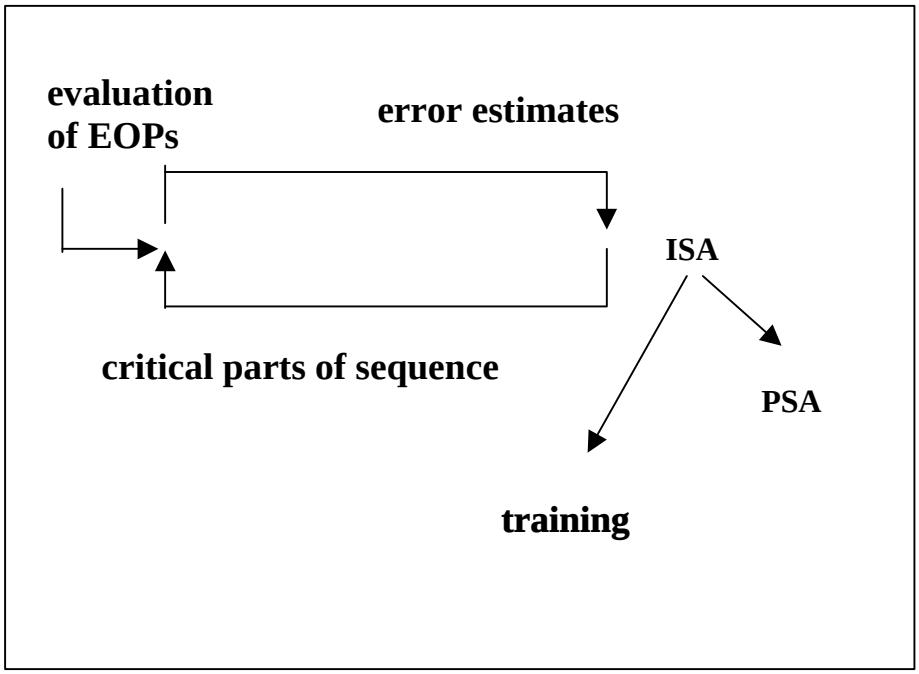


Figure 6.3 Integrated sequence analysis should give feedback to operators

6.3 Methodological survey

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 concentrated upon man-machine system simulation. The second survey presented recent developments in HRA approaches that did not explicitly use man-machine system simulation. During the project a third survey was performed on available methods for expert judgement elicitation.

6.3.1 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 systems. The objectives of the study were to present principles for dynamic event analysis (joint system simulation), 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, CES, COSIMO, MIDAS, OASYS, SRG and SYBORG.

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 analysis is not limited by the possibilities that have been included in the event tree.

Developing a joint system simulation requires a substantial amount of work and financial resources in specifying the knowledge needed by the two models (for the technical and the human systems) and the interface between them. Finally, one must realise that the developments of techniques for joint system simulation are still at an early stage.

To summarise the survey, the seven systems are characterised with their initial purpose and by using three criteria. The three last columns of Table 6.1 describe the criteria: degree of relevance to PSA/HRA, how flexible the system is, that is, how easy it will be to apply it to another application, and how mature it is, that is, how far it has come in its development.

As the table shows, none of the systems was considered to be 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, it was not found practical to apply any of these methods within Subproject 3 considering available time and resources.

In the context of man-machine system simulation, one should also mention the Computerized Accident Management Support System (CAMS) developed by the 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.

Table 6.1: 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 modelling 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

6.3.2 Survey on new HRA methods

The purpose of the second methodological survey of NKS/RAK-1.3 (Kahlbom and Holmgren, 1994) 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 this 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. Furthermore, there were many enhancements concerning the treatment of psychological and cognitive behaviour in already well established methodologies. The methods discussed in the study are the enhancement of SLIM-MAUD (Zamali et al., 1992), INTENT (Gertman et.al., 1992), COGENT (Gertman, 1993), HIET (Drouin, 1989), HITLINE (Macwan and Mosleh, 1994) and HRMS (Kirwan and James, 1989).

The methodological HRA method survey (Kahlbom & Holmgren, 1994) concluded by giving recommendations of the usability of the COGENTand HIET EOP in RAK-1.3, since they were identified as being the best candidates for the continued work among the surveyed methods. 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 EOP-driven. These methods were also applied in the analysis of different sequences, as discussed under section 6.4.

6.3.3 Survey on existing expert judgement methods

The survey on existing expert judgement methods was carried out as a part of one of the case studies of RAK-1.3. Human reliability and PSA can be seen as one of the areas where expert judgement will always be required. In literature, several methods and their variants to elicit and to combine expert judgements have been reported (e.g. Cooke 1991, 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).

6.4 The four sequences

Four case studies were selected in RAK-1.3 in order to test approaches to ISA. The common rationale for selecting these sequences has been discussed in section 6.1. Two of the case studies, large man 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 the primary and the secondary side of the installation. In addition, there is a risk of early radioactive release through an atmospheric release valve on the secondary side. The fourth case study deals with confused signal view in the control room followed by a fault in instrumentation.

Besides the primary objective to test methods for ISA, additional objectives were formulated for the individual cases. Typically these objectives were given with respect to the practical safety work, e.g.:

- Evaluation of emergency operating procedures and possible recommendations for improvements
- Better understanding of different types of operator action
- Improved risk evaluation of the sequences, thereby also a more realistic and credible PSA.

An important aspect of the project has also been a role as an educational tool for the participants, concerning the sequences and about all areas of importance for their evaluation.

Table 6.2 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

6.4.1 BWR cold overpressure

Sequence

The cold pressurisation accident sequence stems from potential BWR reactor tank overfilling. The reactor tank is filled with water at the end of the shutdown sequence in order to start refuelling. The aim of the action 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) violation of plant technical specifications with respect to the filling procedure.

The VTT methodological approach

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 approach builds on a three-stage procedure. 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 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.

Reference models can be influence diagrams, fault and event trees, decision tables, etc. The modelling technique was based on probabilistic influence diagrams as general framework and on structured use of expert judgement and marked point process (MPP) models for detail modelling (Holmberg et al, 1996).

The analysis team consisted of PSA experts, psychologists and process specialists. The integrated analysis process included common workshops, separate work meetings and individual work. Data for the models were collected in a simulator run. After the run, the operators were debriefed and interviewed.

Results

The accident probability was calculated by a simulation model of the event sequence. In the basic case, the probability of overfilling was $3x10^{-10}$ per shutdown. Given a spurious start of a high head pump within the first 100 minutes, the probability of overfilling/over-pressurisation increased to $2x10^{-6}$ per shutdown.

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 on the simulator.

6.4.2 Inadvertent opening of an isolation valve during shutdown of a BWR

Sequence

The studied event was 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. The sequence was chosen due to its importance in plant specific shutdown PSA. As specific goals, creating multidisciplinary insights in the shutdown LOCA and a finding a method for shutdown specific HRA quantification were set.

Methodologies

During the first phase of the work, the group used COGENT (Gertman, 1993) as modelling tool. The method was easy to use and it provided a frame under which engineers and behavioural scientists could discuss. However, the COGENT method did not provide a plausible way to probability quantification. Thus as the next step, structured expert judgement was decided to be used in order to reach probability estimates.

In an expert judgement process, there are normally three kinds of actors: decision-makers, normative experts and substance matter experts. Substance 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 6.3.

Table 6.4 shows the different phases of an expert judgement process. In our case, 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,

Table 6.3 The participants of an expert judgement 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. Substance matter experts	• familiar with the issue • responsible for the analysis of the issue and giving judgements on it

Table 6.4 The phases of an expert judgement process

Phase
1. Selection and training of experts
2. Elicitation of expert judgements
3. Modelling and combination of expert judgements
4. Sensitivity analyses
5. Discussion and feedback from experts
6. Documentation

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 an expert training session, which was conducted only for the expert group.

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. The experts were asked to make their individual analyses about the issues and to write short reports on their analyses. 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 expert's presentations was to discuss and compare the experts' thinking models and approaches. After the expert's presentations, the quantitative estimates were elicited from each expert individually. The probability values were discussed in detail by the normative experts and certain consistency checks were made.

Results
This case study proved that it is possible to carry out a well-structured assessment in a limited period of time. The results show that the shutdown LOCA risk cannot be neglected. Somewhat large uncertainty bounds in the results do not decrease the value of the results. This is due to the fact that the goal of the assessment was rather to express the uncertainties than to "sweep them under the carpet".

The used method proved out to be a valuable tool for expert judgement combination and wider uses are foreseen. In addition, 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 complement to other data collection methods.

6.4.3 Steam generator tube rupture (SGTR)

Sequence
The sequence was selected mainly because it represents a type of sequence, which evolves with intense interaction between the reactor process and operator action. Therefore, it is well suited for testing methods for integrated analysis. Furthermore, SGTR gives a significant contribution to the calculated core melt probability for Swedish PWRs which means that the sequence is relevant to study from the PSA point of view.

A tube rupture causes leakage of radioactive coolant from the primary to the secondary side of a PWR. This leads to decreasing pressure in the primary system and a falling pressurizer level. Reactor scram and safety injection is automatically initiated. The safety injection replaces the loss of primary system water and maintains the primary system pressure.

During an SGTR radioactive steam may be released outside the reactor system through valves on the secondary side. If the leak flow continues, the level in the damaged steam generator increases. Without appropriate actions from the control room, the steam generator could be top filled with water leading to release of contaminated water, further loss of reactor coolant and possibly other failures in the secondary system.

The operators have a set of Emergency Operating Procedures (EOPs) that should give them optimal guidance in handling the situation. The EOPs also include measures to be taken if additional failures occur in the reactor system. When the reactor scrams, the operators start to work with the procedure E-0 for diagnosis and, in our case, the verification of SGTR by radiation monitoring on the secondary side or by uncontrolled SG-level increase. When SGTR is identified, the operators switch over to procedure E-3, which is the main procedure for a tube rupture event. In addition to E-3 there are other procedures for handling the depressurization phase in an SGTR situation, should complicating circumstances occur.

Methodology

The methodological approach used in the SGTR analysis can be described as a semidynamic approach as follows:

1. The analysis proceeds stepwise using the following tools:
   - Cognitive task analysis
   - PSA
   - Thermohydraulic modelling of the process
   - Simulations with operators and training personnel

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 cognitive factors, PSA and process.

The cognitive modelling gives cognitive profiles of the emergency operating procedures with distributions of possible operator error modes. The semidynamic PSA analysis gives conditional probabilities at specific system states (i.e. probabilities to arrive at the specified states, given that SGTR has occurred), e.g. in the interface between two EOPs.

3. Because the overall event is complicated and potentially will lead to a very cumbersome 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. The system status description thus includes two parts:

- One retrospective part based on detailed analysis using all available tools

- One predictive part, which briefly overlooks the remaining part of the sequence tree with a screening analysis.

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

1) The first PSA analysis is performed with a standard value for all operator interactions. Probability values for technical components are taken from the plant specific PSA with statistical data from the T-book (T-Boken version 4, 1994) .

2) The first analysis gives a list of most important actions according to standard PSA. This list together with the instructor's 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 for each sequence segment, (2) How many steps/operations are included,

4) The identification of which cognitive activities are included in each EOP segment is based on the cognitive analysis. Based on this the results may be translated into a probability analysis.

5) The results from the HRA are used for a new PSA. Based on the new results, more interactions between PSA and HRA may take place.

Results

The work has given cognitive profiles for the E-3 procedure and distributions of possible error modes for segments in the E-3 procedure (see Figure 6.4). Based on the cognitive profiles and other factors, such as number of operator actions and available time, degrees of difficulty was estimated for each segment in the procedure.

Furthermore, a practical framework for interaction between human factors and PSA has been established, which has resulted in expert judgements on human failure probabilities. It was found that for this case, segments in the procedures is a suitable level of aggregation for the interaction between the two disciplines.

The project has given significant feedback to the PSA analysis of SGTR. The new PSA, which essentially follows the EOP structure, includes improvements with respect to both technical and human failures as compared to the standard PSA, which e.g. includes only two basic events for human failure.

The PSA analysis done can not be said to have improved the “risk picture” for the entire SGTR scenario, because only the normal case with the E-3 procedure has been analysed. However, the improved PSA plant model already developed within this project will be useful if such studies will be done in the future. This is also the case for methodological improvements such as modelling loops as recovery situations and the interaction with human experts and thermohydraulics experts.

The application of a thermohydraulics code (CENTS) has shown how time windows serve as the link to HRA and PSA within the overall semidynamic approach. The project has contributed to the verification of CENTS against the simulator code, which was quite important for the confidence in the code from the utility point of view.

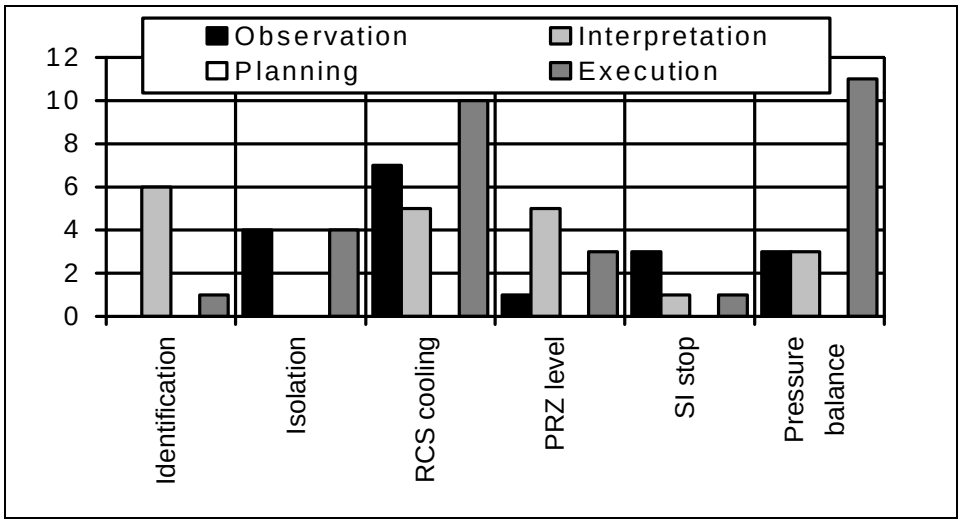


Figure 6.4 Distributions of possible error modes for segments in the E-3 procedure

6.4.4 Confused signal view in the control room

Sequence

The idea of this 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.

The project started with a pilot project (Holmgren, 1996) for which a rupture on the measurement system for water level in the reactor was selected and analyzed as initiating event . Due to this event, incorrect signals of water level was sent to the

control room but also to different automatic safety systems. The pilot project resulted in a method for analyzing the most safety critical signal patterns of the plant.

For the main study (Holmgren, Jacobsson, and 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.

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 when the level actually is stable or decreasing.

Methodology

It was necessary to upgrade the PSA model, which lead 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.

The important initiating events were analysed in detail by interviewing operator crews, and by using the O1 simulator at the KSU training centre . The two most significant initiating events leading to spurious “high” in the two selected displays were: 1) fire or flooding in a specific room and 2) 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. This 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

The quantification was based on the CPCs that either 1) improve, 2) have no effect or 3) reduce the performance reliability for different segments of the human per-

formance. In the last step the results from the quantification of the operator model was implemented in the PSA study.

Results

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

The method can be used as a tool to verify different aspects of the control room work, such as instructions, practices and control room design. The method may be used in future projects of verifying and validating 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 background information for creating a new level measurement system in Oskarshamn 1.

6.5 Discussion

At the outset of the NKS/RAK-1.3 project 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 what ISA is, 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 much 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 co-operate is undoubtedly one of the most important objectives of an ISA.

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 and modelling. Using moderators and decision analysts may help in the task. It is important that somebody controls the communication exchange in order to avoid biases.

There are different approaches to create a functioning ISA. In the decision analytic approach, experts of different disciplines look at a problem from different viewpoints and present their analyses 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 deci-

sion analysts, then weight the collected pieces of information, and form a synthesis for the basis of the decision.

A second approach to ISA is to create a working group of different disciplines to work on a 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. The NKS/RAK-1.3 study cases has more resemblance with this approach.

7 Maintenance Strategies

7.1 Background

The Nordic subproject “maintenance strategies and ageing” (NKS/RAK-1.4) has compiled methods and development needs for maintenance and safety within the Nordic nuclear power industry (Laakso, 1997). Clearly there is a continuous need to optimise maintenance taking safety, reliability and economic factors into account.

The maintenance area provides a good example of possible improvements by stronger feed-back loops. Having reliability centred maintenance as the basic strategic element it is necessary to get good information on maintenance indicators guiding e.g. how to mix preventive and corrective maintenance. The NKS/RAK-1.4 subproject has contributed a tool for this by software development, the RelDAT system (see Figure 7.1).

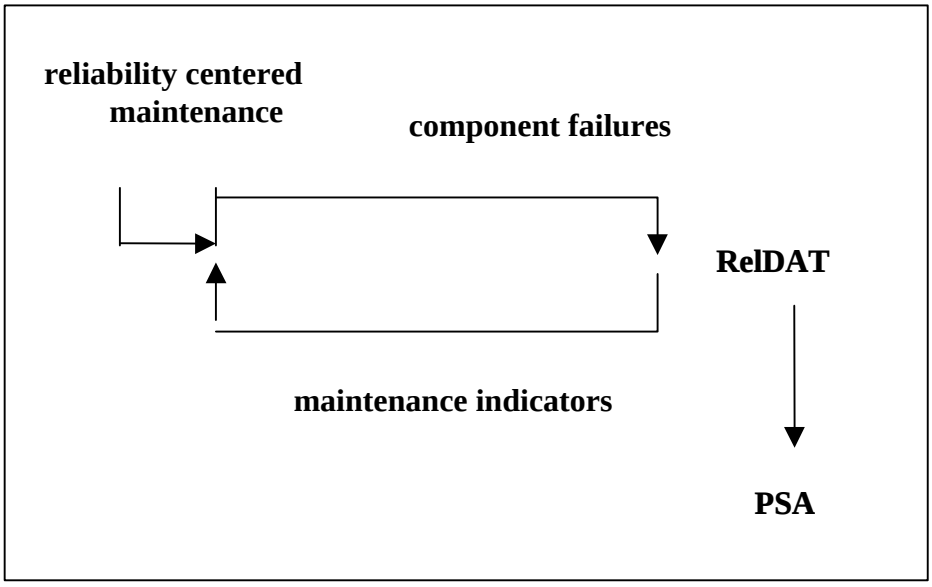


Figure 7.1 The RelDAT system as a tool in reliability centred maintenance

7.2 Survey

A survey of maintenance strategies and development needs has been carried out and interviews have been made with utilities, authorities and researchers. The sur-

vey has provided important input to the identification of need of improvements in existing maintenance programs, in order to create opportunities to carry out an effective maintenance with regard to safety, availability and cost. The work, which has covered Finnish and Swedish reactors in general with a special effort at the Barsebäck plant, included:

- description of existing maintenance activities including planning, and follow-up
- evaluation of the need of information for maintenance programmes
- identification of possible improvements
- building a basis for improved maintenance strategies

Both strengths and weaknesses were identified which resulted in proposals of actions to improve the effectiveness of the maintenance program. This work also resulted in a structure and documentation of the maintenance process.

The survey addressed component ageing problems and related corrective measures, component condition monitoring and maintenance indicators, and decision criteria for maintenance and replacement of components. The maintenance analysis pinpoints proposals on adjustment of testing and maintenance intervals and tasks justified for fault detection and system availability. The results indicate that a relaxation of excessive testing and preventive maintenance may in specific cases be justified to keep control of system unavailability and maintenance costs.

7.3 Development of a maintenance data information system

Various data systems have been designed for different purposes such as to give data to PSA on component reliability and to give support to the maintenance at a local level. In particular the TUD data basis collects component reliability data from all Swedish plants and also from TVO. Within NKS/RAK-1 a special software system, RelDAT (Reliability Data Analysis Tool), has been developed to improve the analysis and presentation of data from TUD and local maintenance data systems. The tool is used as a support in order to make fast exploring and analysis on the workorder history.

RelDAT has been installed at Barsebäck, where it has on-line access to the local maintenance information system (IDUN) and TUD. It now remains to integrate the system as a living tool in the maintenance work at the plants. The software can be applied to specific systems of interest and adapted to specific needs at the individual plants.

7.4 Human error in maintenance

Human reliability analysis of nuclear power plants has traditionally been concentrated upon human performance in disturbance conditions. On the other hand, also maintenance errors, taking place earlier in plant history, may have an impact on the severity of a disturbance, e.g. by disabling safety-related equipment. Thus, 4 400 maintenance history records and licensee event reports from a Nordic nuclear power plant were looked through. From this data, 334 human errors could be identified and screened for analysis. As the common cause failures generally affect core damage risk in a significant extent in Nordic BWRs, a special effort was put to study them.

The study presents a model for screening and analysis of single and dependent human errors from the fault history records and utility reports. According to the results of the study, the instrumentation is prone to human errors and in the dependent errors, the plant modifications are an important source class.

7.5 The future of maintenance programs

A systematic decision support structure can be used for identifying and ranking significant decision criteria and decision options to change the maintenance task programs. The results from maintenance analysis can be used in decision analysis, together with expert judgement and possible other analyses, to evaluate how well the decision criteria are met.

Internationally, maintenance strategies are now often discussed within the concept of Reliability Centred Maintenance (RCM). A key issue in its development is to have appropriate tools for decision support. Within RAK-1.4 a decision analysis software tool has been demonstrated.

Reliability Centred Maintenance at Barsebäck

Development of the RCM-concept has started during 1997 in the area of reliability and maintenance optimisation as a part of the R&D-program at Barsebäck Kraft AB. The basic approach is to evaluate existing maintenance programs at the plant. The main goal is to develop a methodology for systematic maintenance analysis and to demonstrate its usefulness in evaluation of the maintenance task programmes of technical systems. Another important goal is to develop a model for introduction of justified improvements in system reliability and maintenance effectiveness by using results from analysis of historical data on faults and maintenance. The plant information system and reliability data analysis tools are utilised effectively and interactively with the RCM analysis in order to limit the need of excessive analysis resources. In this approach, a preliminary selection of the analysis significant items (ASIs) from a larger study object (e.g. system) is done.

The screening is based on a survey of the existing maintenance task program and rough searches from the plant failure data base. Items covered by extensive preventive actions or repeated faults are selected as ASIs. Safety significant items are taken into account by using results from PSA. A detailed re-assessment of the maintenance task program is then performed only for the identified ASIs in order to verify, or justify changes in, existing maintenance and testing tasks and intervals. For the significant items, detailed analyses of experience are performed. The maintenance indicators (MI) cover several years of the plant operational history, when the trends of the number of faults and maintenance work (man-hours) are followed up. A decision logic tree analysis (LTA) is used to evaluate how the number of faults could be reduced or detected earlier by more effective preventive tasks, monitoring or tighter intervals.

The main steps of the RCM- concept are illustrated in Figure 7.2, see below.
The first phase of the work consists of development of a practical RCM analysis model, and a demonstration case study (hydraulic scram system). This will be followed by phase 2, which covers a practical decision analysis approach to support complex maintenance and safety related decisions such as justification and selection of adjusted maintenance or testing intervals.

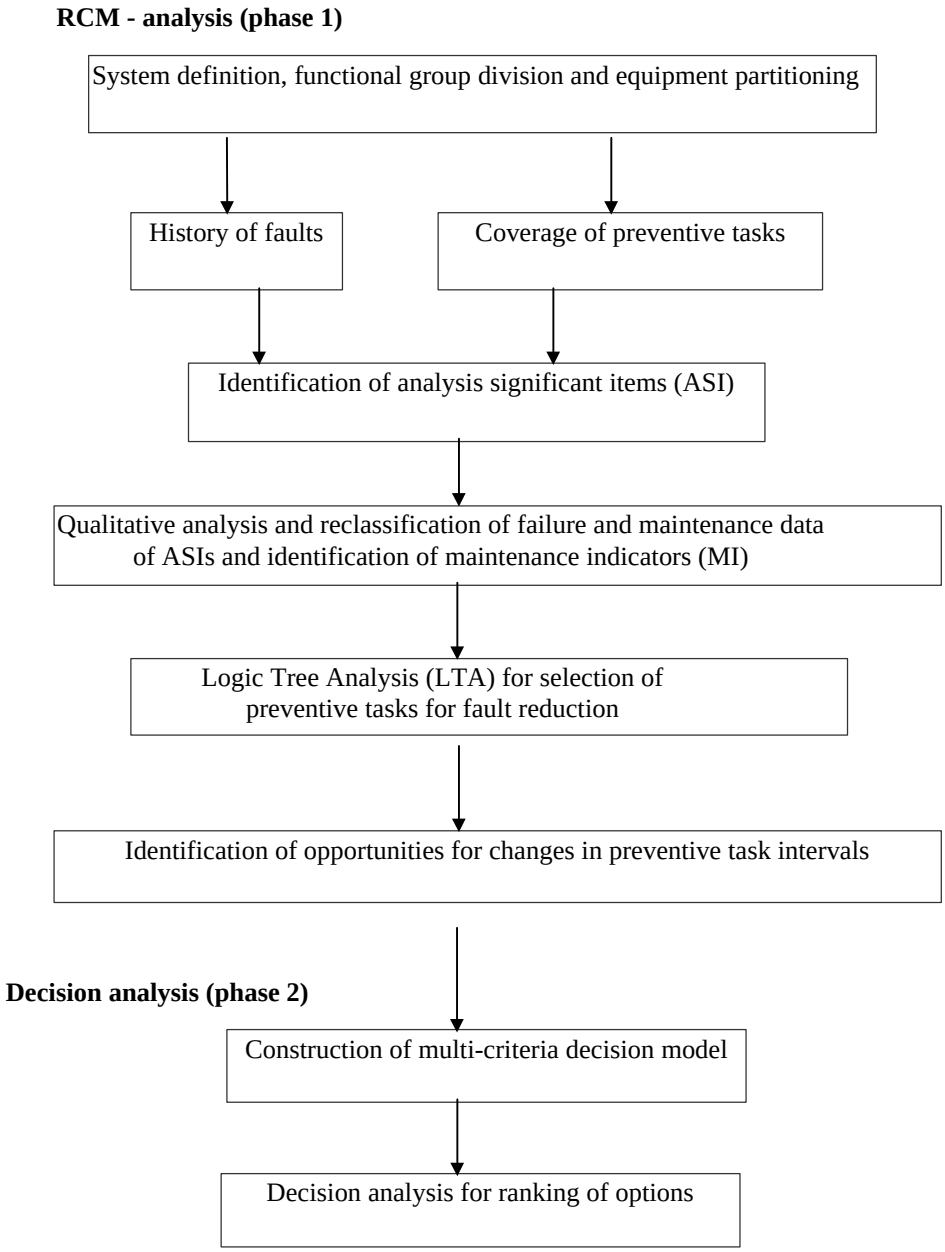


Figure 7.2 Brief steps of a reliability centred maintenance process and decision analysis

8 The Role of PSA in the Safety Work

One of the aims of the NKS/RAK-1 project has been to explore ways to increase the realism and reliability of the safety analysis. Subprojects 2, 3 and 4 have all contributed to this aim in different areas such as LOCA initiating event frequencies, more in-depth analysis of certain event sequences and better analysis of component failure data. The PSA activity has also been subject to a special study within subproject 1.

Essential parts of NKS/RAK-1 thus leads back to the concept of Living PSA (LPSA) that was studied in great detail in the previous NKS programme SIK-1 (Laakso, 1994). There is therefore reason to put the RAK-1 work into the context of LPSA as developed in SIK-1 and to see how LPSA in general has developed since SIK-1 was ended.

8.1 LPSA in SIK-1

The LPSA concept was in SIK-1 described as a process to update the PSA model to represent the current or planned configuration and to use the model to evaluate and suggest changes in the configuration. Following the SIK-1 Report, LPSA consists of three main applications:

1. Safety assessment using PSA on a daily basis in the safety work in choosing the most proper designs and operational procedures with respect to safety.

2. Risk follow up of operation and incidents

3. Risk monitoring (ultimately as on-line risk monitoring during operation) which may have many applications in operation, maintenance and testing.

With LPSA the availability of the PSA work for operational safety management increases and PSA becomes a more dynamic tool. The LPSA concept was illustrated in the SIK-1 report by a number of test cases.

8.2 Developments of LPSA

PSA has been subject to a special study within subproject 1 of NKS/RAK-1 (Andersson, Johansson, Karnik and Stokke, 1997). It appears that LPSA is making progress both in Finland and Sweden and that both regulators and utilities have developed philosophies for applying the concept. The STUK view of LPSA can serve as an example according to Figure 8.1.

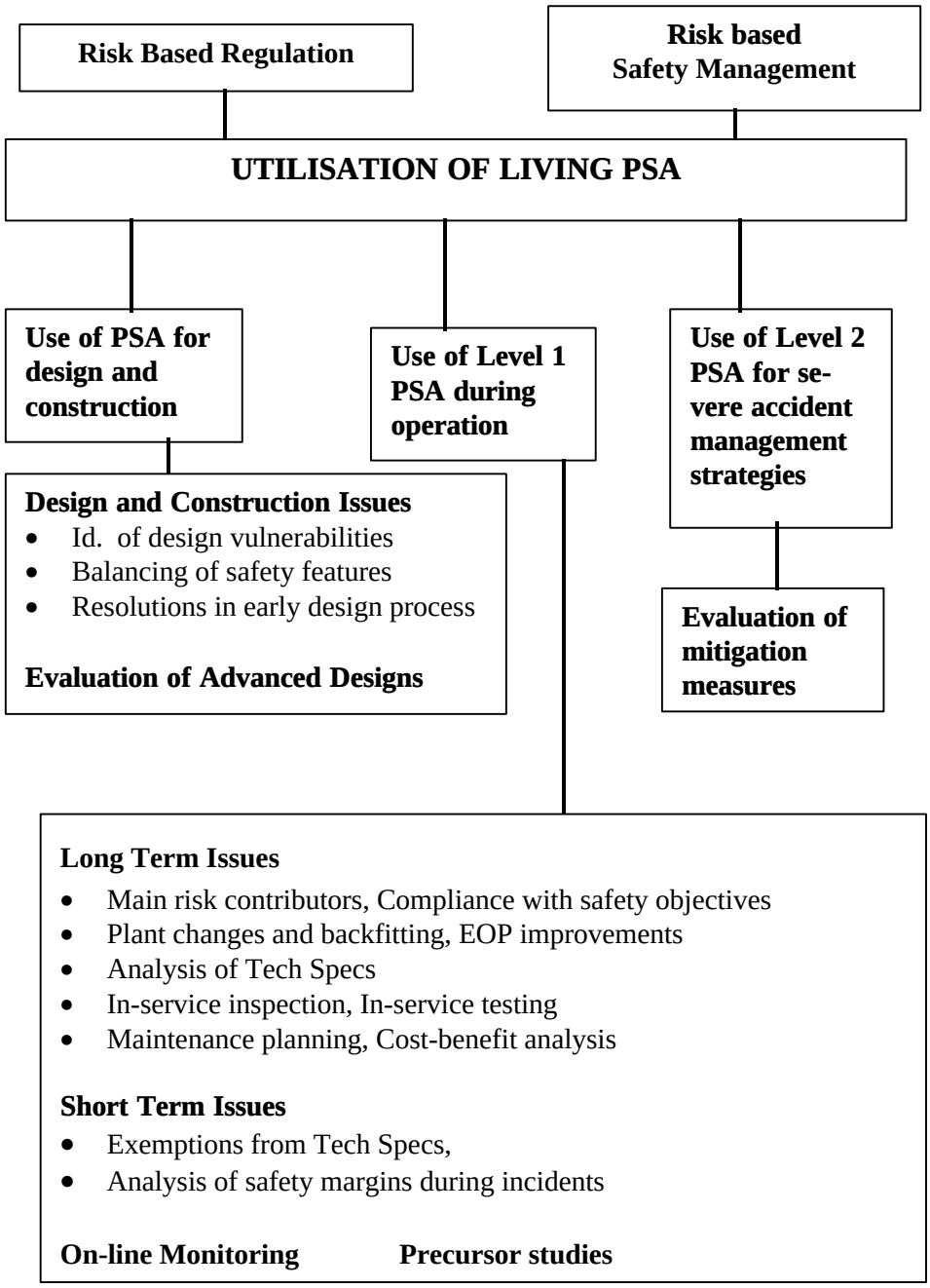


Figure 8.1 The STUK view of LPSA

In compliance with the requirements in Regulatory Guide YVL 2.8 the licensee has to use PSA in support of operational safety decisions as follows:

1. Plant changes and backfitting
2. Applications of Tech Specs
3. Case by case assessment of risks resulted from component failures
4. Training of plant personnel
5. Working out of the transient and emergency operating procedures
6. Risk follow-up of licensee events
7. Maintenance and surveillance programme planning

This list shows that LPSA is well established as use of PSA on a daily basis in the safety work both for planning and risk follow up purposes. However, risk monitoring is not yet in place.

The individual reactor plants, and often the individual reactor units, now take increasing responsibility for the PSA work, which is a prerequisite for a real Living PSA. It has been expressed by utilities that PSA analyses give a common platform for different parts of the organisation to assess safety issues. However, it also seems evident that the degree to which different personnel groups are involved in the PSA work varies substantially between the plants. The resources given to PSA also vary. It can be concluded that Living PSA requires a minimum size of a group that has the task to develop and maintain the model and to interact with different personnel groups.

Concerning the three application areas discussed in the previous section, Subproject 1 leads to a few observations, as follows.

Concerning the daily use of PSA for design and operational procedures

This is the original purpose of PSA, which by the LPSA concept is being used more and more as a day to day tool in the safety work. Generally there is a clear development toward using PSA as a tool for risk planning of operation, in-service testing, inspection etc. This means that different personnel groups become increasingly involved in PSA activities. The maintenance area, however, in general terms seems to be somewhat behind in this development although the situation varies between power plants. This may thus be an issue for consideration in the further development of maintenance strategies.

However, the use of PSA for design and development of operational procedures requires that the PSA models have a certain level of detail and realism. If the models are too conservative their use for optimising safety improvement may in fact lead to sub-optimisation. As pointed out in the SIK-1 report, this problem can only be solved by long-term improvement of the plant models. Today there seems to be a rather high variability between the individual reactor units with respect to the

status of the PSA models, and consequently to which degree they can be used for optimising safety improvements.

Concerning risk follow up of operation and incidents

This area of LPSA is rapidly developing and applications are already in use both on a routine basis, e.g. for each operational season, and when incidents have occurred.

Concerning risk monitoring

The concept of LPSA also includes on-line risk monitoring ultimately to be used in the control room for operational decision making. In some organisations this is also an outspoken goal for which, however, realisation seems to be relatively far into the future.

8.3 Contributions from NKS/RAK-1

The NKS/RAK-1 project may bee seen as having contributed in part to the development of PSA into a more living tool in addressing a number of safety issues where probabilistic approaches can support operation, maintenance and in-service inspection. One example is the development of probabilistic fracture mechanics in subproject 2. In fact the need to support risk based in service inspection with PFM and PSA was a major driving force behind this subproject.

Another example is the development of methods for integrated safety analysis, which has taken place within subproject 3. Here PSA is one of several integrated components that will support testing and eventually improving emergency operating procedures and operator training. A third example is the development of software for analysis and presentation of maintenance data that has been accomplished in subproject 4. Such software systems will be necessary tools for more interaction between maintenance personnel, databases and PSA.

9 Discussion and Recommendations

In this concluding chapter we first relate to some observations regarding the safety work that has emerged in subprojects 1 and 5. We then briefly summarise the achievements that have been made with respect to certain software developments (subprojects 1 and 5) initiating event frequencies (subproject 2), integrated sequence analysis (subproject 3) and maintenance (subproject 4). We conclude by emphasising the need for consolidating the results achieved in NKS/RAK-1 as well as in other programmes, and by indicating some areas where further research is recommended.

9.1 Some observations regarding the safety work

Subproject 1 has accomplished an overview of the safety work. The final report (Wahlström and Gunsell, 1997) is a broad and systematic description of the safety work in Finland and Sweden. Comparisons between the two countries are made. The description is based on extensive interview work done at utilities and authorities in Sweden and Finland. The report is descriptive rather than evaluating but leads to some important observations (examples are given below). Subproject 5 has explored how the needs for modernisation of the plants are dealt with. For a full overview the reader is referred to the reports (Wahlström and Gunsell, 1997) and (Hammar, Wahlström, and Simola, 1997). Here we only comment on a few observations.

The resource issue

The operation of nuclear power plants demands considerably more resources than was earlier expected. Despite efforts for increased efficiency both utilities and authorities seem to have a heavy workload due to a number of reasons, e.g.:

- Plant modernisation in response to ageing of the original design and enhanced safety requirements, reconstitution of FSAR
- Plant renovations due to ageing degradation
- A need for more integration between different groups of personnel

There are in principle three alternatives to overcome the situation: 1) higher efficiency, 2) less ambitious goal setting, and 3) more resources. Since the second alternative seems inappropriate, a combination of more resources and higher efficiency must be the way forward. One factor that needs to be taken into account in Sweden is the ongoing decentralisation of responsibilities from the utility headquarters to the reactor sites and the individual reactor units. Generally this is judged

as a positive development provided the individual units get the “critical mass” of competence and other resources for key functions.

The resources and the working efficiency on part of the authorities is also an important issue. There is e.g. a need to evaluate selective approaches for reviewing safety-related modifications. There is accordingly a need to consider possible approaches with regard to increasing the efficiency of inspections and safety reviews performed by the authorities. One important aspect concerns balancing properly the efforts aimed at ”doublechecking” the various technical matters and the efforts placed on assessing the relevant safety work processes at the utilities. One observation in this regard is that the Swedish regulatory authority SKI has relatively smaller technical staff than STUK (Wahlström, Nyman and Reiman, 1996). On the other hand, SKI has more personnel with knowledge in behavioural sciences than STUK.

Documentation

It is important to have documentation procedures in the daily work. Means and approaches for this need to be further developed. The utilities may e.g. consider applying formal modelling of the management and processing of plant modification and improved procedures for maintenance data systems, as illustrated in subprojects 4 and 5.

New developments

The RAK-1.5 report advises both the utilities and the safety authorities to actively follow the evolving safety standards for new reactors, e.g. the development of the European directives. This is irrespective whether new reactors may be planned or not since the new standards may have implications for assessing the safety of the existing reactors as well.

9.2 NKS/RAK-1 contributions

Software development for improved work procedures

The work in subprojects 1 and 5 has utilised techniques that could be considered by the utilities and the authorities in their evaluation of the safety work. In subproject 5 a formal modelling technique was used to describe the procedures involved in the modification process. The approach taken was largely in accordance with the so-called Structured Analysis and Design Technique.

In subproject 1 it was described how Object Modelling Technique eventually could be used to improve work routines in nuclear power plants. It aims at facilitating review of the process for completeness and consistency of applied procedures and allows them to be broken down in detail to account for all factors.

Protection against initiating events

The NKS/RAK-1 project has produced a model that calculates the probability that a given pipe weld will break due to IGSCC. In cases when IGSCC dominates the LOCA frequencies, which may well be the case especially for large LOCA, applications of the model has potential to produce PSA results that are not based on WASH 1400 values, but on actual conditions relating to inspection schemes, material properties, fracture mechanics and provisions for leak detection. Such applications will be quite resource demanding since they require a much more detailed modelling of the pipe systems than is usually done in PSA. Furthermore, data will be needed on material data and loading for individual welds. The effort, however, will not just give new PSA results but also data for decisions on risk based in-service inspection.

At the end of the project a joint seminar was held with the international SLAP project which has evaluated databases for pipe failures. The results from this project suggest that probabilistic fracture mechanics models only can take care of a limited part of the problem to estimate LOCA frequencies. Even so, the approach of probabilistic fracture mechanics needs to be further developed and, above all, applied in real PSA applications. Finally it must be emphasised that an increasing co-operation between PSA experts and fracture mechanics experts is of utmost importance for better estimations of LOCA frequencies.

Integrated sequence analysis

Development and application of methodologies for integrated sequence analysis has been a major effort in NKS/RAK-1. There were several reasons for this:

- Problems with the traditional PSA/HRA approach with respect to human performance
- The dynamic nature the evolution of disturbances with interaction between the technical and the human systems
- A need for feedback from the safety analysis to control room personnel and emergency operating procedures

The project started with three methodological surveys that gave a basis for the NKS work. Different methodologies were then tested on four sequences with much of human interaction. The work gave many results and experiences of value for future work in the area and the tested methods showed capability for important contributions, e.g.:

- Structured frameworks for integration between PSA and behavioural sciences
- Improved PSA for certain sequences
- “Control room PSA”
- Improved knowledge about cognitive factors related to procedures

- Feedback to operator training
- Increased understanding of risks associated with maintenance outages
- Use of simulators for event analysis

The event analyses also gave participants from different disciplines good opportunity for interaction that considerably enhanced mutual understanding.

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

Maintenance

Subproject 4 has contributed to the further development of maintenance programmes by:

- Exploring the status of maintenance strategies and mapping needs for development in Finland and Sweden
- Development of a maintenance data information system. The system was first installed at the Barsebäck plant
- Testing tools for decision analysis with respect to maintenance programmes.
- Bringing insights into the important issue of human errors in maintenance

It is believed that the NKS/RAK-1 contributions will be of value when the utilities develop their programmes for reliability centred maintenance.

Strengthening the feedback loops

One feature of the safety work, emphasised in RAK-1.1, is that all activities need goals, means and feedback in order to be effective. An activity that can not be described with such a loop needs improvement. Much of the work in RAK-1 subprojects 2, 3 and 4 had the purpose to establish interaction between data analysis, PSA and operation, thereby in fact strengthening feedback loops:

- Between risk based inspection and probabilistic fracture mechanics
- Between operation and integrated sequence analysis
- Between reliability centred maintenance and component reliability data bases

Since probabilistic fracture mechanics, integrated sequence analysis and component data bases all have direct links to PSA, the project has also contributed to the further development of Living PSA as established in the previous NKS/SIK-1 project.

9.3 Implementation and consolidation

The NKS/RAK-1 project has developed methods for safety analysis, documentation and evaluation in many areas. In several cases the development has taken place in direct co-operation with plant personnel involved in operation and maintenance. The installation of a maintenance software system in Barsebäck is an important example.

In other cases, however, time and resources have not allowed demonstration of the full potential of the methods. A probabilistic fracture model has e.g. been developed but not yet applied in a real plant model. The efforts to develop and test methods for integrated sequence analysis became more extensive than was originally foreseen and involved plant personnel to a great extent. On the other hand, time did not allow for cross-comparisons between methods to a desired extent. The methods used should also be more extensively tested on other sequences. There are also other methods and tools that should be subject for testing and implementation.

In summary, there are good reasons for the utilities and authorities to evaluate NKS/RAK-1 achievements in order to see how they can be implemented in the safety programmes. The active utility participation in the project as well as the organisation with a co-ordinating group with representatives from both utilities and authorities should give good prerequisites for this. However, in practice for reasons pointed out in subproject 1 there is still a risk that some of the achievements with potential good prospects may not be applied as would be desired. This is a general problem for the industry which needs to be addressed with special efforts. From the NKS point of view it would probably be valuable if such an effort of consolidation of achievements included also earlier NKS projects.

9.4 Some areas for further research

In addition to the implementation of NKS/RAK-1 results, the work has highlighted need for more research and development in a number of areas:

1. Evaluation of complicated programmes

As illustrated by the NKS/RAK-1.1 report, reactor safety is a complex area. The subproject used comparisons between different programmes and comparisons with a normative model as methods for evaluation. In addition different software systems were used as practical tools. Although the work resulted in certain observations regarding the safety work there should still be room for more development and testing of methodologies to evaluate complex systems.

2. Application of basic research in PSA

Reactor safety has many areas where integration between different disciplines is needed. This is not always a trivial task. One aspect is that PSA needs generalists with engineering background whereas basic sciences are characterised by research culture, and that the academic training still gives interdisciplinary efforts low priority.

In several areas has the NKS/RAK-1 project developed and used approaches to apply basic sciences (especially fracture mechanics and behavioural sciences) in PSA. The experiences are good but still there is need for developing structured approaches that can be met with confidence in all groups.

3. Evaluation of LOCA frequencies

It has already been emphasised that the probabilistic fracture mechanics model developed in the project needs to be applied. Subproject 2 also raises further needs for research. For instance there may be other mechanisms than IGSCC, especially for PWRs, that can be approached with the same type of method as has been done in NKS/RAK-1.2. Another issue is to develop a comprehensive methodological approach to the area of LOCA frequencies including modelling, use of databases and PSA.

4. Further development of methods and tools for integrated sequence analysis

Also this area is in a relatively early stage where much research and development still remains with the goal to get a comprehensive methodological package. More methods need to be tested on various types of sequences. Furthermore, there is a lack of software tools for dynamic and semidynamic approaches. Especially current PSA models need to be further developed for practical and illustrative use in this type of application. There are already early developments in this direction in areas such as accident management and PSA Level 2 that could be tested for this purpose.

5. Further development of maintenance strategies

The NKS/RAK-1.4 project has illustrated how maintenance strategies could be improved in a number of areas such as: development of intelligent condition diagnostics through integrated display systems, event reporting systems and databases for ageing, use of decision models for improved decision making. Also in this area there is a need for a comprehensive approach that integrates these and other topics. The concept of reliability centred maintenance is one suggested framework for such an approach.

Acknowledgements

The author thanks all the participants in the study: subproject leaders, report authors, researchers and all the representatives from regulatory bodies and utilities who engaged themselves so deeply in the work. I am grateful to NKS and SKI who supported me as project leader, and to all other organisations that supported the various parts of the project with national funding. The RAK-1 reference group, the NKS Secretariat in Risø and Torkel Bennerstedt supported me all the time with good advice. Finally, I also want to thank the other project leaders in the NKS programme for good co-operation and stimulating discussions. Is has really been a pleasure be part of the Nordic working environment.

References

Andersson, K., Johansson, G., Karnik, P., and Stokke, E., PSA as an integrated tool in nuclear safety work, NKS/RAK-1(97)R16

Andersson, K., and Pyy, P., NKS/RAK-1 Subproject 3. Integrated Sequence Analysis, Final Report, NKS/RAK-1(97)R11

Andersson, S.O. and 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

Ashby, W.R., An introduction to cybernetics, London: Methuen (1994)

Bergman, M., Brickstad, B. and Nilsson, F., A procedure for estimation of pipe break probabilities due to IGSCC, NKS/RAK-1(97)R9

Bush., S.H., Statistics of pressure vessel and piping failures, Journal. of Pressure Vessel Technology, **110** (1988) 225-233

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

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

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

Espejo, R., Schuhmann, W., Schwaninger M., and Bilello U., Organizational Transformation and Learning: A Cybernetic Approach to Management. Chichester: Wiley (1996)

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

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

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

Gunsell , L., Forss, A. and Andersson, S-O., The importance of piping reliability on the core damage frequency. Seminar proceedings: Piping reliability. Sigtuna, Sweden, SKI Report 97:32, October 1997

Gärdinge, M., Why is the OKG nuclear power plant interested in advanced pipe rupture models in their PSA studies? ISI and radiation doses to maintenance personnel. Piping reliability. Sigtuna, Sweden, SKI Report 97:32, October 1997

Hammar, L., Wahlström, B. & Simola, K,, Modernisation for maintaining and improving safety at Nordic nuclear power plants, NKS/RAK-1(97)R13

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

Hollnagel, E., CREAM - Cognitive Reliability and Error Analysis Method. Elsevier, Oxford. 1997.

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

Holmgren, P., Modellering av störd signalbild i kontrollrummet, pilotstudie, Relcon AB på uppdrag av OKG, NKS/RAK-1(96)R9

Holmgren, P. Jacobsson, P. and Sörman, J., Modellering av störd signalbild i kontrollrum, NKS/RAK-1(97)R17, and SKI Report

Jacobsson, P., 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. and Holmgren, P., Survey of methods for integrated sequence analysis with emphasis on man-machine interaction, Relcon, NKS/RAK-1(95)R2, May 1995.

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

Laakso, K., Safety evaluation by living probabilistic safety assessment and safety indicators, Tema Nord 1994:614

Laakso, K. Maintenance analysis and decision support for safety and availability of active systems, NKS/RAK-1(97)R12

Lydell, B., Strategies for reactor safety: Preventing loss of coolant accidents, NKS/RAK-1(97)R10

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

Nilsson, F., Brickstad, B. and Skånberg, L., Pipe break probabilities due to IGSCC, International Journal of Pressure Vessels and Piping, **43** (1990), 205-217

Nyman, R. et.al., Reliability of Piping System Components. Framework for Estimating Failure Parameters from Service Data, SKI Report 97:26, Swedish Nuclear Power Inspectorate, Stockholm, 1997

PISC-III Report no 33, Report on the evaluation of the inspection results of the wrought-to-wrought PISC III assemblies no 31, 32, 33, 34, 35 and 36, European Commission Joint Research Centre, 1995

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

Ross, D.T., Structured analysis (SA): A language for communicating ideas. IEEE transactions on software engineering, Vol. SE-3, pp. 16-34, Jan 1977

Seminar on Piping Reliability, Sigtuna-Sweden, September 30-October 1, 1997, SKI Report 97:32, October 1997

Simonen, F.A. and Woo, H.H., Analyses of the impact of inservice inspections using a pipe reliability model, NUREG/CR-3869, U.S.NRC, Washington D.C., 1984

Simola, K and Pulkkinen, U., Statistical models for reliability and management of ultrasonic inspection data, VTT Automation, KUNTO (96)10, NKS/RAK-1(97)R14

Strandell,Ch., Kärnkraftsäkerhetens begrepp och deras relationer; En analysmodell av säkerhetsarbetets komponenter och innehåll, NKS/RAK-1(97)R2

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

Wahlström, B. and Gunsell, L., Reaktorsäkerhet – En beskrivning och en värdering av säkerhetsarbetet i Norden, NKS/RAK-1(97)R8

Wahlström, B., Nyman, R.and Reiman, L., En jämförelse mellan myndighetsarbetet inom kärnsäkerheten i Finland och Sverige, NKS/RAK-1(96)R7

Zamali, J.H. , Lusby, M.D., Hubbard, F.R., Mosleh, A. and Waller, M.A., Evolutionary Enhancement of the SLIM-MAUD Method of Estimating Human Error Rates. Transactions of the American Nuclear Society. Volume: 65, 508-510.

Appendix 1

NKS/RAK-1 Participants

Project Leader

Kjell Andersson. Karinta-Konsult

Subproject Leaders

Subproject 1: Lars Gunsell, Vattenfall Energisystem
Björn Wahlström, VTT Automation (report editor)

Subproject 2: Björn Brickstad, SAQ Kontroll
Anders Enerholm, Relcon

Subproject 3: Kjell Andersson, NKS/RAK-1
Pekka Pyy, VTT Automation

Subproject 4: Kari Laakso, VTT Automation
Jette Paulsen, Risø Lab.

Subproject 5: Oddbjörn Sandervåg, SKI

Co-Ordinating Group (and steering committee for subproject 3)

Lennart Carlsson, SKI (Chairman)
Bo Liwång, SKI (Chairman)
Lars Gunsell, Vattenfall
Mauritz Gärdinge, OKG
Peter Jacobsson, Sydkraft
Markku Malinen, TVO
Pekka Pyy, VTT Automation
Lena Kecklund, SKI
Kjell Andersson, NKS/RAK-1 (Secr)

Subproject 1 Working Group

Lars Gunsell, Vattenfall Energisystem (sub-project leader, chair)
Björn Wahlström, VTT Automation (report editor)
Markku Friberg, TVO
Lennart Hammar, ES-Konsult
Ola Hernvall, Vattenfall/Ringhals
Bo Liwång, SKI

Lasse Reiman, STUK
Carl Rollenhagen, Vattenfall Energisystem
Göran Larsson, Sydkraft Konsult
Helge Smidt Olsen, IFE/Halden
Egil Stokke, IFE/Halden
Louise Dahlerup, Beredskabsstyrelsen
Kjell Andersson, NKS/RAK-1 (secr)

Subproject 2

Sub-Project leaders
Björn Brickstad, SAQ Kontroll
Anders Enerholm, Relcon

Steering committee
Lennart Carlsson, SKI (chairman)
Kostas Xanthopoulos, SKI (chairman)
Björn Brickstad, SAQ Kontroll
Anders Enerholm, Relcon
Fred Nilsson, KTH
Sven Olov Andersson, Vattenfall AB
Roger Axelsson, Sydkraftkoncernen
Rauli Keskinen, STUK
Bo Liwång, SKI
Kjell Andersson, NKS/RAK-1 (secr)

Report author
Bengt Lydell (RSA Technologies)

Subproject 3

Sub-Project leaders
Kjell Andersson, NKS/RAK-1
Pekka Pyy, VTT Automation

Steering committee: See co-ordinating group

Team leaders

Steam tube rupture sequence	:	Kjell Andersson, NKS/RAK-1
Cold over-pressurisation sequence	:	Pekka Pyy, VTT Automation
Shut-down LOCA sequence	:	Peter Jacobsson, Sydkraft Konsult
Disturbed signal view sequence	:	Per Holmgren, Relcon

Subproject 4 Working Group

Kari Laakso, VTT Automation (sub-project leader, chair.)
Jette Paulsen, Risø Lab. (sub-project leader)
Ralph Nyman, SKI
Per Olof Sandén , SKI
Lasse Pettersson, Vattenfall Energisystem
Sven Skagerman, Vattenfall Energisystem
Kecheng Shen, Studsvik EcoSafety AB
Pekka Skogberg, Sydkraft
Joan Dorrepaal, Risø
Kjell Andersson, NKS/RAK-1 (secr)

Subproject 5 Working Group

Oddbjörn Sandervåg, SKI (chairman)
Lasse Reiman, STUK
Lennart Hammar, ES-Konsult
Björn Wahlström, VTT Automation
Kaisa Simola, VTT Automation
Kjell Andersson, NKS/RAK-1 (secr)

Appendix 2

NKS/RAK-1 Reports

Final Report

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

Subproject Final Reports

Wahlström, B., Gunsell, L., Reaktorsäkerhet – En beskrivning och en värdering av säkerhetsarbetet i Norden, NKS/RAK-1(97)R8

Bergman, M., Brickstad, B. & Nilsson, F., A procedure for estimation of pipe break probabilities due to IGSCC, NKS/RAK-1(97)R9

Lydell, B., Strategies for reactor safety: Preventing loss of coolant accidents, NKS/RAK-1(97)R10

Andersson, K., & Pyy, P., NKS/RAK-1 Subproject 3 - Integrated Sequence Analysis, Final Report, NKS/RAK-1(97)R11

Laakso, K. et al , Maintenance analysis and decision support for safety and availability of active systems, NKS/RAK-1(97)R12

Hammar, L., Wahlström, B. & Simola, K,, Modernisation for maintaining and improving safety at Nordic nuclear power plants, NKS/RAK-1(97)R13

Subproject 1: Survey of safety work

Wahlström, B., Gunsell, L., Reaktorsäkerhet – En beskrivning och en värdering av säkerhetsarbetet i Norden, NKS/RAK-1(97)R8

Wahlström, B., Nyman, R., Reiman, L., En jämförelse mellan myndighetsarbetet inom kärnsäkerheten i Finland och Sverige, NKS/RAK-1(96)R7

Strandell,Ch., Kärnkraftsäkerhetens begrepp och deras relationer; En analysmodell av säkerhetsarbetets komponenter och innehåll, NKS/RAK-1(97)R2

Hammar, L., Seminarium om granskning för säkerhet och kvalitet - Strategi och praxis, NKS/RAK-1.1 och Kärntekniskt Centrum vid KTH, Esbo, Januari 1997, NKS/RAK-1(97)R3

Andersson, K., Johansson, G., Karnik, P., & Stokke, E., PSA as an integrated tool in nuclear safety work, NKS/RAK-1(97)R16

Subproject 2: LOCA frequencies

Lydell, B., Strategies for reactor safety: Preventing loss of coolant accidents, NKS/RAK-1(97)R10

Bergman, M., Brickstad, B. & Nilsson, F., A procedure for estimation of pipe break probabilities due to IGSCC, NKS/RAK-1(97)R9

Simola, K. & Koski, K. A survey of probabilistic methods for evaluation of structural component integrity, VTT Automation, KUNTO (95)7, NKS/RAK-1(97)R5

Simola, K & Pulkkinen, U., Statistical models for reliability and management of ultrasonic inspection data, VTT Automation, KUNTO (96)10, NKS/RAK-1(97)R14

Subproject 3: Integrated sequence analysis

Andersson, K., & Pyy, P., NKS/RAK-1 Subproject 3 - Integrated Sequence Analysis, Final Report, NKS/RAK-1(97)R11

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

Kahlbom, U. and Holmgren, P., Survey of methods for integrated sequence analysis with emphasis on man-machine interaction, Relcon , NKS/RAK-1(95)R2, May 1995.

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

Cold overpressurization sequence
Holmberg, J. et.al. Integrated sequence analysis - cold overpressurization accident sequence, May 1996, NKS/RAK-1(96)R5, VTT/TAU-6009/96

Shutdown LOCA sequence
Jacobsson, P., 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, NKS/RAK-1(96)R10, Sydkraft Konsult ES-9603m007

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

Disturbed signal view sequence
Holmgren, P., Modellering av störd signalbild i kontrollrummet, pilotstudie, Relcon AB på uppdrag av OKG, NKS/RAK-1(96)R9

Holmgren, P. Jacobsson, P. and Sörman, J., Modellering av störd signalbild i kontrollrum, NKS/RAK-1(97)R17

SGTR sequence
Josefsson, R., Tubbrott i Ringhals 3 - beräkningar med CENTS, Vattenfall Bränsle, Mars 1996, NKS/RAK(96)R1

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

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, Analys av tubbrott - Delrapport och utvärdering, NKS/RAK-1(96)R8

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

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

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

Subproject 4: Maintenance strategies

Laakso, K. et al, Maintenance analysis and decision support for safety and availability of active systems, NKS/RAK-1(97)R12

Dorrepaal, J.,Analysis tools for reliability databases, Risø National Laboratory, SKI Report 95:67, NKS/RAK-1(95)R3

Paulsen, J., Dorrepaal, J., Cooke, R., and Hokstadt, P., The design and use of reliability data base with analysis tools, NKS/RAK-1(96)R6, Risø, June 1996

Laakso, K., Pyy, P., Reiman, L., Human errors related to maintenance and modifications, STUK-YTO Technical Report, NKS/RAK-1(97)R15

Subproject 5: Plant modernisation

Hammar, L., Wahlström, B. & Simola, K,, Modernisation for maintaining and improving safety at Nordic nuclear power plants, NKS/RAK-1(97)R13

Appendix 3

List of abbreviations

ASAR	As operated Safety Analysis Report
BWR	Boiling Water Reactor
CAMS	Computerised Accident Management Support system
CCF	Common Cause Failure
CDF	Core Damage Frequency
CPC	Common Performance Conditions
EOP	Emergency Operating Procedure
EUR	European Utility Requirements
FSAR	Final Safety Analysis Report
HRA	Hunan Reliability Analysis
IAEA	International Atomic Energy Agency
ISA	Integrated Sequence Analysis
IGSCC	InterGranular Stress Corrosion Cracking
ISI	In-Service Inspection
LOCA	Loss Of Coolant Accident
MCP	Main Circulating Pump
MMI	Man-Machine Interaction
MPP	Marked Point Process
NKS	Nordic Nuclear Safety Research (Nordisk KerneSikkerhedsforskning)

OMT	Object Modelling Technique
PFM	Probabilistic Fracture Mechanics
PSA	Probabilistic Safety Analysis
PWR	Pressurised Water Reactor
QA	Quality Assurance
RCM	Reliability Centred Maintenance
RDBMS	Relational DataBase Management System
SADT	Structured Analysis and Design Technique
SGTR	Steam Generator
SGTR	Steam Generator Tube Rupture
SKI	Swedish Nuclear Power Inspectorate
SPSA	Shutdown PSA
STUK	Finnish Centre for Radiation and Nuclear Safety
Tech Specs	Technical Specifications
TUD	Availability, Maintenance and Operation (In Swedish: Tillförlitlighet Underhåll och Drift)