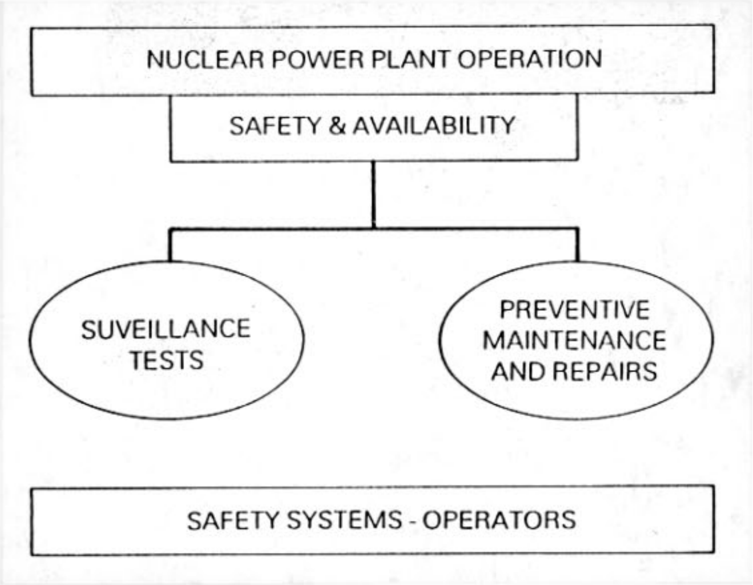
NORD
MAY 1990

OPTIMIZATION OF TECHNICAL SPECIFICATIONS BY USE OF PROBABILISTIC METHODS

A Nordic Perspective


NUCLEAR POWER PLANT OPERATION
SAFETY & AVAILABILITY
SUVEILLANCE TESTS
PREVENTIVE MAINTENANCE AND REPAIRS
SAFETY SYSTEMS - OPERATORS

nka

Nordic
liaison committee for
atomic energy

nka

Nordisk kontaktorgan for atomenergispørgsmål

Nordiska kontaktorganet för atomenergifrågor

Pohjoismainen atomienergia-yhdyselin

Nordic liaison committee for atomic energy

OPTIMIZATION OF TECHNICAL SPECIFICATIONS BY USE OF PROBABILISTIC METHODS

A NORDIC PERSPECTIVE

Final report of the NKA project RAS-450

Edited by
Kari Laakso
Technical Research Centre of Finland

This report was prepared
by a team consisting of:

Kari Laakso, Michael Knochenhauer,
Tuomas Mankamo and Kurt Pörn.

Participating organizations:

Technical Research Centre of Finland
Avaplan OY, Finland
ABB Atom AB, Sweden
Studsvik AB, Sweden
Swedish Nuclear Power Inspectorate
Swedish State Power Board
Teollisuuden Voima OY, Finland

MAY 1990

The present report is available on request from:

Technical Research Centre of Finland
Laboratory of El. and Autom. Engineering
SF-02150 ESPOO
Finland

ISBN 87 7303 422 3

NORD 1990:33

ABSTRACT

The Technical Specifications of a nuclear power plant specify the limits for plant operation from the safety point of view. These operational safety rules were originally defined on the basis of deterministic analyses and engineering judgement. As experience has accumulated, it has proved necessary to consider problems and make specific modifications in these rules.

Developments in probabilistic safety assessment have provided a new tool to analyse, present and compare the risk effects of proposed rule modifications. The main areas covered in the project are operational decisions in failure situations, preventive maintenance during power operation and surveillance tests of standby safety systems.

Key words

Safety - Reliability - Availability - Systems analysis- Probabilistic estimation - Risk assessment - Technical specifications - Repair - Maintenance - Testing - Nuclear power plants - Safety systems - Operation - Sweden- Finland.

This report is part of the safety programme 1985-89 sponsored by NKA, the Nordic Liaison Committee for Atomic Energy. The work has been financed in part by the Nordic Council of Ministers and in part by the participating Swedish and Finnish institutions, power companies and regulatory bodies.

SUMMARY

The Technical Specifications define the limits and conditions for safe plant operation. In the Nordic countries the Technical Specifications are prepared by the operating organizations and approved by the regulatory authority (the Swedish Nuclear Power Inspectorate in Sweden and the Finnish Centre for Radiation and Nuclear Safety in Finland). The ultimate goal of the Technical Specifications (TS) is to prevent radiological accidents in the plant, and thereby to protect the health and safety of the public and plant personnel. These operational safety rules have been defined with margins on the safe side, mainly on the basis of deterministic analyses prepared for the Final Safety Analysis Report (FSAR) of the nuclear power plant and on the basis of engineering judgement. At this time an extensive operating and design experience has accumulated and a number of problems have appeared which require specific modifications in the TS rules. The goal of the modifications is to further improve the nuclear safety and also to enhance the effectiveness and flexibility of plant operation, maintenance and testing.

Developments in probabilistic safety assessment (PSA) have facilitated an analysis of the risk effects of alternative requirements in the TS rules. This makes possible a relative comparison and balancing of the rules from the risk point of view, and a justification of modified rules. For example, temporary high risk situations in plant operation can be identified and evaluated in advance so that they can be prevented or controlled. Also, excessively stringent but not safety-significant requirements may be modified in order to improve the operational flexibility and plant economy. At the beginning of the project limiting conditions for operation and periodic testing were selected for evaluation by use of probabilistic methods.

The limiting conditions for operation shall assure that the safety systems are either ready for use or functioning on real demand, i.e. in the event of plant transients and accidents. The specifications require the plant to be brought into a safer operational state, usually cold shutdown, if the faulty equipment in a safety system cannot be restored within its allowed outage time. The surveillance requirements prescribe periodic tests and inspections for detection of faults and verification of operability of safety equipment. The active safety-related functions and systems were found suitable as case study objects. The practical part of the studies thus mainly concerned standby safety systems and functions.

PSAs have been completed for thirteen nuclear power plants in Sweden and Finland and are currently being performed for the remaining three plants. Therefore, another main objective was to test and develop the use of PSA plant safety models for analysis and verification of TS rules.

The main decision situations concerning TS are, whether one can justify and allow:

- proposed permanent modifications of TS rules
- temporary exemptions from TS rules.

An approximate guide for prompt decision making in specific failure and maintenance situations during plant operation can be provided by precalculating so-called risk importance measures. Risk increase factor is a useful measure for evaluation of the safety significance of a fault or an isolation of equipment due to maintenance.

As a result of method development and proposals for criteria in this project, and in probabilistic safety assessment in general, it is now possible to:

- make risk-based comparisons of alternative plant operating principles during failure situations in safety systems and search such operating modes that give minimum risk
- evaluate temporary risk increments caused by unavailable equipment, due to preventive maintenance in safety systems during power operation
- analyze the coverage and effectiveness of individual tests and quantify the effects of alternative test schemes of redundant equipment.

The case studies have produced useful results for specific Nordic nuclear power plants, for example:

- reconsideration of plant shutdown requirements in situations when multiple failures occur in specific safety systems
- justification of modified rules for preventive maintenance in high-redundant standby safety systems during power operation
- improvement of the effectiveness of surveillance test procedures and schemes of standby equipment.

The use of PSA methods through their systematic approach also enhances the understanding of complex operational situations where many factors affect the plant safety and availability. Thereby the readiness for prompt safety-related decisions on operational problems can be considerably improved.

SAMMANFATTNING

Ett kärnkraftverks säkerhetstekniska föreskrifter (STF) definierar villkor och begränsningar för anläggningens säkra drift. I Norden ligger ansvaret för utarbetandet av STF hos kraftbolagen, medan granskning och godkännande sker hos övervakande myndighet Statens Kärnkraftinspektion (SKI) i Sverige och Strålsäkerhetscentralen (STUK) i Finland.

Det grundläggande syftet med STF är att förebygga och minimera risken för radiologiska missöden, och att därigenom skydda såväl allmänhet som anläggningspersonal. Reglerna i STF formulerades ursprungligen konservativt baserat på deterministiska analyser ingående i FSAR (Final Safety Analysis Report) och ingenjörsmässiga bedömningar. I dagens läge, med stadigt ökande erfarenhet från konstruktion och drift av kärnkraftverk, har ett antal problemområden i STF identifierats. Det känns därför angeläget att utarbeta och pröva metoder för en mera systematisk utvärdering av specifika ändringar i STF i syfte att förbättra såväl anläggningssäkerheten som effektiviteten och flexibiliteten i anläggningens drift och underhåll.

Mot bakgrund av de senaste årens intensiva utveckling inom den probabilistiska säkerhetsanalysen (PSA) ter det sig idag naturligt att utnyttja probabilistiska metoder i utvärderingen av STF. En särskild styrka ligger i teknikens goda möjligheter till relativa jämförelser av utfallet av alternativa formuleringar av specifika STF-krav, och i de möjligheter som ges till sammanvägning av faktorer som till sin karaktär kan vara mycket olika. Detta kan utnyttjas för att skapa ur risksynpunkt jämnare STF. Således kan signifikanta tillfälliga riskökningar under specifika driftförhållanden (som följer av dagens STF) systematiskt identifieras, kvantifieras och elimineras. På samma sätt

kan överdrivet stränga bestämmelser, d.v.s. bestämmelser som inte är säkerhetsmässigt effektiva, modifieras i syfte att förbättra anläggningsekonomin och driftflexibiliteten. Inom NKA/RAS-450 har tyngdpunkten lagts på de delar av STF som berör periodisk testning och driftbegränsningar. De tillämpningsstudier som utförts som en del av projektet berör främst driftberedda aktiva säkerhetsrelaterade funktioner och system.

STF föreskriver intervall för och omfattning av periodisk provning och inspektion, som utförs i syfte att avslöja uppkomna fel och verifiera driftberedskapen hos säkerhetssystem.

STF:s driftbegränsningar skall garantera att säkerhetssystemen är insatsberedda i samband med plötsligt uppkommande behov, t.ex. vid ett yttre nätbortfall. I samband med fel i säkerhetssystem föreskriver reparationskriterierna att anläggningen skall föras till ett säkrare driftläge, vanligen kall avställning, om inte felet kan avhjälpas under den specificerade tillåtna hindertiden.

För närvarande har PSAer utförts för tretton av totalt sexton svenska och finska kärnkraftverk; för resterande tre är sådana analyser under utarbetning. Av denna anledning har inom projektet stor vikt lagts vid att utvärdera användbarheten av säkerhetsanalysernas system- och anläggningsmodeller för analys och verifiering av STF-regler. Arbetet har inkluderat såväl utvärdering som utveckling av nya och existerande metoder för riskbaserad optimering av STF. Som ett resultat av detta, och av dagens status inom PSA allmänt, är det möjligt att:

- göra riskbaserade jämförelser mellan olika alternativa driftvillkor i samband med fel i specifika säkerhetssystem, och söka efter lösningar som minimerar den då uppkomna tilläggsrisken,

- utvärdera den tillfälliga relativa riskökning som uppkommer som en följd av att förebyggande underhåll utförs på säkerhetsrelaterad utrustning under anläggningsdrift,
- utvärdera kvaliteten hos enskilda periodiska prov och kvantifiera alternativa provprogram för driftberedd utrustning med redundans.

Tillämpningsstudier utförda inom eller i anslutning till projektet har i vissa fall redan använts för att underbygga specifika förslag om ändring av STF. Som exempel på sådana förslag eller ändringar i Forsmark och TVO må nämnas:

- ändring av avställningsvillkor i samband med flerfaldiga fel i driftberedda säkerhetssystem med hög grad av redundans,
- ändring av regler och kriterier för förebyggande underhåll under effektdrift i system med hög grad av redundans,
- ändring av testintervall och -procedurer för redundant utrustning.

Det probabilistiska angreppssättet kan dessutom förbättra förståelsen av komplexa driftsituationer och kritiska ingrepp och därmed skapa ett bättre underlag för drift- och säkerhetsrelaterade beslut.

LIST OF CONTENTS

LIST OF CONTENTS con'd

1. INTRODUCTION

This project [1.1] is performed within the joint Nordic research program NKA/RAS: Risk Analysis and Safety Philosophy. NKA stands for the Nordic Liaison Committee for Atomic Energy. The NKA/RAS-450 project is part of the safety research program for the period 1985 - 1989.

During the preproject phase the opinions and experiences of Technical Specifications problems were surveyed among the Nordic nuclear power companies and regulatory authorities [1.2]. A survey of international method developments and planned research efforts in this area was also performed in 1985 [1.3]. The actual project was divided into three reporting phases and the results are summarized in this final report.

1.1 Introduction to technical specifications and probabilistic safety assessment

The Technical Specifications (TS) can be seen as a set of operational safety rules and criteria, which defines the allowed operational range for the nuclear power plant from the safety point of view. The TS in Sweden and Finland are prepared by the operating organizations and approved by the regulatory authority. These rules and criteria were originally formulated with margins on the safe side, mainly on the basis of:

- deterministic analyses prepared for the Final Safety Analysis Report (FSAR) of the nuclear power plant, and

- engineering judgement.

Developments in probabilistic safety assessment [1.4], and increasing operating experience, have made further analysis, balancing and justification of various requirements in the TS possible. Within the NKA/RAS-450 project, in-depth research, development and comparison for risk-based optimization of TS rules has been pursued.

A general overview of the structure and contents of the TS in the Nordic Boiling Water Reactor (BWR) plants follows in Table 1.1.

Table 1.1 General contents in Nordic BWR Technical Specifications for operation.

1. Introduction and definitions
2. Safety limits - concerning fuel cladding integrity - concerning primary circuit integrity
3. Limiting conditions for operation - operability requirements of equipment on system/component level for the operational states of hot shutdown, nuclear heating, hot standby and power operation - allowed outage times for equipment - action statements in failure situations
4. Surveillance testing - requirements and acceptance criteria on system/component level - test intervals
5. Administrative instructions and rules
6. Background for the conditions and limitations presented in the above Chapters 2 and 3
7. Conditions and limitations for cold shutdown and refuelling outage
8. Background for conditions and limitations in Chapter 7

At the beginning of the project, the problems concerning limiting conditions for operation (Chapter 3 in TS) and surveillance testing (Chapter 4 in TS) were selected as the main items to be evaluated using probabilistic methods. The limiting conditions for operation (LCO) shall assure that the safety systems are either ready for use or functioning on demand [1.5], e.g. at incidents involving loss of off-site power and at accidents. The action statements require the plant to be brought into a safer operational state, usually cold shutdown, if faulty equipment cannot be restored within its allowed outage time (AOT).

The surveillance requirements prescribe periodic tests for detection of faults and verification of operability of safety equipment.

Probabilistic Safety Assessments (PSA) have been completed, or are currently being performed, for all nuclear power plants in Sweden and Finland [1.6, 1.7]. The next development stage of these PSA studies is to use them within a Living PSA concept. Therefore, one of the main objectives of the NKA/RAS-450 project was to test the application and develop the use of the PSA plant safety models for verification of TS rules.

1.2 Objectives of the project

The objectives of the project have been to:

1. Look for areas of TS in which there is a potential for application of probabilistic methods in identification and evaluation of possible improvements.

2. Examine and develop probabilistic methodology, and plan experience data bases, to be used by utilities and authorities in their assessment of the implications of alternative requirements in Technical Specifications.

3. Develop the general philosophy and principles for further improvement and optimization of TS, taking into account both the safety and economical risks of the plant. Improve the understanding and application of these principles.

4. Perform practical case studies for specific nuclear power plants for testing and verification of the methods and principles developed.

The perceived needs and possibilities for a future development of Technical Specifications were found to differ considerably between different plants [1.2]. This fact, and the cumulative learning and experience achieved during the research project, have been taken into account in the gradual orientation of the above objectives and planning of the project work.

The Fig. 1.1 gives an overview of the items evaluated during the project.

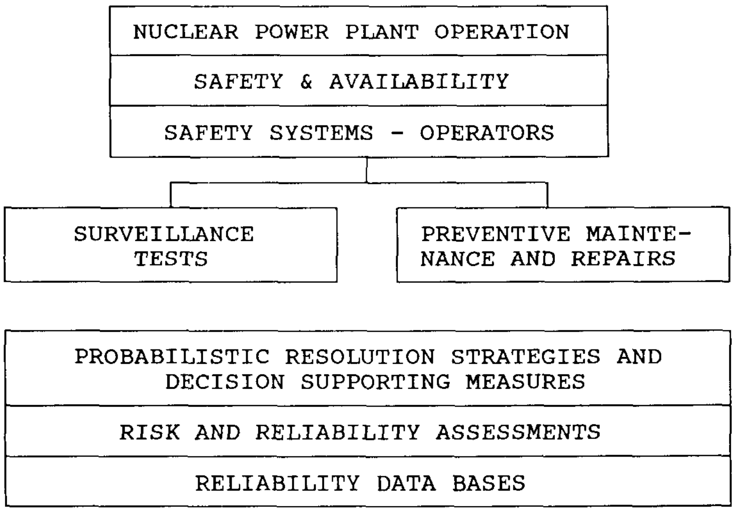

NUCLEAR POWER PLANT OPERATION
SAFETY & AVAILABILITY
SAFETY SYSTEMS - OPERATORS
SURVEILLANCE TESTS
PREVENTIVE MAINTENANCE AND REPAIRS
PROBABILISTIC RESOLUTION STRATEGIES AND DECISION SUPPORTING MEASURES
RISK AND RELIABILITY ASSESSMENTS
RELIABILITY DATA BASES

Figure 1.1 An overview of the items evaluated during the project.

The typical risk and reliability assessment cases are:

- evaluation of the impact of proposed permanent modifications of technical specifications (TS)
- evaluation of the safety significance of temporary exemptions from TS.

This project is, however, not proposing a total revision of the present Technical Specifications, which are now well established documents in the Nordic countries. Instead of that, a framework and reference is provided for utilities' and authorities' further identification, evaluation and justification of TS modifications needed.

1.3 The Nordic working group

The project work has been carried out by a Nordic working group, consisting of experts on Technical Specifications and PSA and reliability methods.

Representatives from utilities, regulatory authorities, research institutes, vendors and consultants have worked in this group. The group has communicated with the Nordic nuclear power utilities, authorities, the Technical Specifications Group of the Nordic Utilities and others interested in the subject. Several project seminars were arranged in Sweden and Finland.

The group has identified and selected TS requirements and rules, concerning active safety-related functions and systems, to be studied during the project. The practical case studies thus mainly concern standby safety systems and functions. The work in these pilot studies has contributed to proposal or approval of modified TS rules in the following areas for specific nuclear power plants:

- development of limiting conditions for operation in multiple failure situations of residual heat removal systems
- justification of introduction of preventive maintenance in selected standby safety systems during power operation
- test scheme rearrangement for diesel generators
- test procedure improvements of selected motor operated closing valves to better correspond with true demands.

International developments in this field have also been continuously surveyed and information exchanged with e.g.

the International Atomic Energy Agency, OECD Nuclear Energy Agency and the U.S. Nuclear Regulatory Commission and Electric Power Research Institute.

1.4 Plant and system types studied

The descriptions in this report of the background and criteria for the requirements in the Technical Specifications are mainly based on the Forsmark and TVO plants [1.8]. The Swedish plants are owned by the Swedish State Power Board and the Finnish plants by Teollisuuden Voima Oy.

The primary safety systems, which have active functions, are divided into four redundant subsystems in these BWR plants of ABB Atom design. The safety systems in Forsmark 1/2 and TVO I/II plants, designed for emergency cooling of the reactor core, are presented as an example in Fig. 1.2.

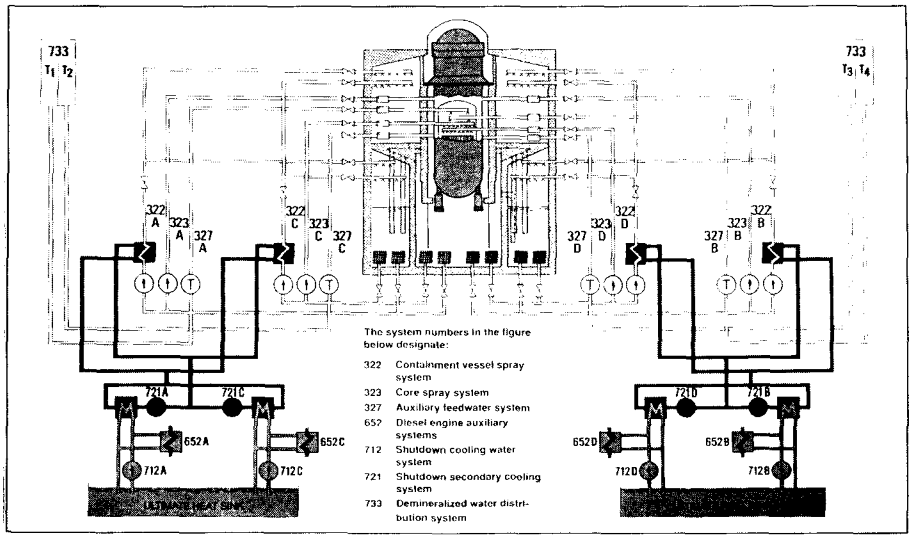

733
T1 T2
733
T3 T4
322 A
323 A
327 A
322 C
323 C
327 C
327 D
323 D
322 D
327 B
323 B
322 B
721A
721C
721D
721B
652A
652C
652D
652B
712A
712C
712D
712B
The system numbers in the figure below designate:
322 Containment vessel spray system
323 Core spray system
327 Auxiliary feedwater system
652 Diesel engine auxiliary systems
712 Shutdown cooling water system
721 Shutdown secondary cooling system
733 Demineralized water distribution system

Figure 1.2 A schematical presentation of emergency cooling systems in a BWR plant.

The subsystems are separated physically from each other and each subsystem has a separate electrical supply bus. The system capacities were originally dimensioned to be 4 x 50 % subsystems according to design criteria. This creates an excess margin to the single failure criterion, which makes it possible to justify power operation during a limited time with one subsystem unavailable due to planned maintenance actions or a repair of a fault. Furthermore, according to renewed and more realistic thermo-hydraulic calculations of Design Basis Accident events, the system capacities are in most cases 4 x 100 %.

1.5 Introduction to report chapters

The results of the work on methods and criteria development, mainly done in connection with the case studies, are summarized in this report as follows:

- In Chapter 2 a description is given of risk-based evaluation and optimization principles, methods and criteria tailored for treatment of operational safety problems.

- In Chapter 3 a summary of factors, influencing the effectiveness of periodic testing, and a description of related development of reliability evaluation methods are presented.

- In Chapter 4 an approach searching for the operational alternative with minimum risk, in specific failure and maintenance situations during power operation, is considered.

- In Chapter 5 specific data needs and data treatment methods, for risk and reliability analysis of TS problems, are described.

- In Chapter 6 systematic ways are introduced to treat complex operational safety problems by use of risk importance measures and probabilistic analyses, including presentation of uncertainties associated with a decision and analysis.

- In Chapter 7 the practical case studies performed, including experiences and benefits achieved, are briefly referred.

- The report ends with a concluding project summary in Chapter 8.

Several research reports and technical reports have been prepared within the project as listed in Chapter 9. Furthermore, the different work reports have been put together into an extensive technical documentation [1.1], which can be ordered from the working group members. The names and addresses are given on the last page of this report.

REFERENCES

1.1 Optimization of Technical Specifications by Use of Probabilistic Methods - A Nordic Perspective. Summary Work Documentation of the Project 1985-89. 420 pages. NKA/RAS-450(89)4. February 1990.

1.2 Ericsson, G. A Summary of Comments from Scandinavian Utilities and Authorities. Asea-Atom Technical Report KPA 85-111 (in Swedish). NKA/RAS-450(85)4. November 1985.

1.3 Mankamo, T. Optimization of Technical Specifications by use of PRA Methods. Preproject Survey-International Developments. VTT Research Report, NKA/RAS-450F(85)2. August 1985.

1.4 PRA Uses and Techniques. A Nordic Perspective. Summary report of the NKA project SÄK-1. Edited by Stephen Dinsmore, Studsvik Energiteknik. NORD Series. June 1985.

1.5 Safety Series No 75- INSAG-3. Basic Safety Principles for Nuclear Power Plants.International Atomic Energy Agency. Vienna, 1988.

1.6 Carlsson, L. Experiences of PSA Methods in Safety Review and Upgrading of Nuclear Reactors in Sweden. Proceedings of the SRE-Symposium 86. Scandinavian Chapter. October 1986. Espoo, Finland.

1.7 Virolainen, R. Probabilistic Safety Analysis in the Licensing and Regulation of Finnish Nuclear Power Plants. Proceedings of the SRE-Symposium 86. Scandinavian Chapter. October 1986. Espoo, Finland.

1.8 Brolin, S., Piirto, A., Laakso, K., Wahlström, B. Technical Specifications for Nordic BWRs. Structure, Experiences and Ongoing Programs. OECD/CSNI/Unipede Specialist Meeting on Improving Technical Specifications for Nuclear Power Plants. NKA/RAS-450(87)2, CSNI Report 151. Madrid, September 1987.

2. DESCRIPTION OF PRINCIPLES AND CRITERIA

2.1 Risk-based evaluation principles

Historically, Technical Specifications (TS) have to a large extent been based on deterministic criteria. The present project, and a number of related projects currently being performed worldwide, reflect an increasing interest in making use of probabilistic methods as a support for decisions in safety-related matters [2.1].

Methods for integrated probabilistic assessment of nuclear power plant safety have been in common use for about 15 years, i.e. since the performance of the Reactor Safety Study in 1974 [2.2]. During this period these methods have matured into a technique capable of handling in a satisfactory way many key issues in the evaluation of plant safety levels, such as the logical modelling of component activations and accident events as well as the interaction of these, the representation of human interactions, and the treatment and modelling of common cause failures (CCF).

Thus, there are two facts that have made the application of probabilistic methods to the evaluation and optimization of technical specifications especially promising:

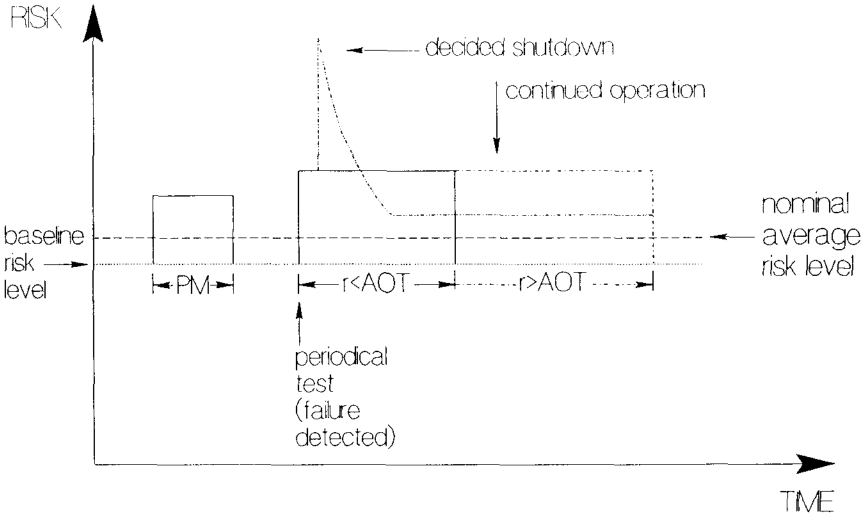
- the increasing maturity of PSA techniques,
- the possibility to handle complex interactions between influencing factors in a systematic and efficient manner.

The overall task of optimizing Technical Specifications with probabilistic methods circles around two main issues; the baseline risk of the plant and temporary risk increases.

Baseline risk of the plant
This is the risk level during power operation assuming no failures are detected and no subsystems are intentionally isolated for maintenance [2.3]. Obviously, the reliability of systems with safety tasks (operating and standby) is crucial. Various measures of reliability assurance are important to keep failure frequencies low and component unavailabilities short. One way to monitor this reliability, is by testing of components and of entire systems. Thus, a probabilistic approach must focus on the frequency and quality of periodic testing.

Temporary risk increases
Component outages in standby safety systems will temporarily increase the total plant risk above the baseline level. Such increases may be involuntary, e.g. due to component failures discovered at periodic testing. The increases may also be voluntary, e.g. due to performance of preventive maintenance during power operation (PM). The allowed outage time (AOT), given in the TS, specifies the deterministically stipulated maximum length of involuntary component outages during which the power operation is allowed. Temporary risk increases may also be due to sudden state changes, e.g. a planned or inadvertent plant shutdown. Probabilistic methods can be used to put these component and system level criteria into the broader perspective of overall plant safety.

The total risk as calculated in PSA is the average risk over the baseline and temporary risk increase states. These principles are illustrated in Fig. 2.1. The optimization of TS will involve controlling and evaluating the baseline risk as well as temporary risk increases. In addition it will be necessary to control a number of other safety aspects. Thus, within the NKA/RAS-450 project, a number of crucial areas requiring evaluation and/or method development have been addressed, as shown in Table 2.1.



<u>Abreviations</u>:

PM = Preventive maintenance during power operation
r = Repair time (corrective maintenance)
AOT = Maximum allowed outage time of safety-related equipment

Figure 2.1 Summary of risk definitions when considering the influence of failure and maintenance situations in safety systems.

Table 2.1 Crucial analysis areas within NKA/RAS-450.

PROBLEMS RELATED TO PERIODICAL TESTING	PROBLEMS RELATED TO OUTAGE LENGTH OF EQUIPMENT
- Frequency/Optimal test interval - Quality and coverage of testing - Alternative test staggering schemes	- AOT/Continued operation versus plant shutdown in AOT violating situations - Planning and evaluation of PM during power operation
GENERAL PROBLEM AREAS	
- Uncertainty and sensitivity in analysis results - Data bases, additional requirements for TS analyses - Presentation of results for decision making - Use of/demands on existing PSA models - Use of/demands on analysis software	

2.2 Important aspects of optimization

2.2.1 The task of optimization

The purpose of TS is to provide an envelope for the safe operation of the plant. The rules of TS concern both the baseline risk of the plant by specifying the frequency and contents of periodical testing, and expected temporary risk increases by specifying limiting conditions for operation. Thus, TS ultimately provide a controlled way of trading excessive safety margin for operational flexibility. Therefore, the word "optimization" in the context of optimizing TS has a twofold meaning:

1. Generally, to make optimal use of the available flexibility for TS as a set,
2. Specifically, to solve specific TS problems in an optimal manner, normally by minimizing the baseline risk.

The task of optimization involves a number of choices influencing the quality and interpretation of the final results:

- What do we intend to optimize?
- Optimization with respect to what?
- On what level shall we optimize?
- What optimization tools should we use?
- How do we recognize the optimum?
- Was the correct optimization criterion used?
- What assumptions and simplifications have been made?

In order to produce meaningful analysis results, all these questions must be addressed. Furthermore this information must be explicitely stated in the analysis report, as it gives the boundary conditions for the interpretation and understanding of the results.

The desired structuring of the analysis can be achieved by applying a pre-defined ordered approach to each TS problem to be analyzed. This may be done by using the Resolution Strategy defined in Chapter 3, Fig. 3.2. The proposed Resolution Strategy covers the whole spectrum of tasks involved in a TS evaluation, as shown in Table 2.2.

Table 2.2 An overview of tasks involved in a probabilistic TS evaluation.

- specification of the problem, with due regard to
  . technical constraints
  . economical constraints
  . operational constraints
  . regulatory constraints
- identification of solution alternatives
- choice of the appropriate analysis level
- concluding sensitivity/uncertainty analysis
- review of non-quantifiable influencing factors.
- recommendation of a practical and licensiable solution.

In Chapters 3 and 4 of this report, the Resolution Strategy will be applied to some of the case studies performed.

2.2.2 Levels of optimization

As mentioned above, one of the important initial questions in a TS analysis is on which level to perform the analysis. The levels that can be considered are:

- component level
- system level
- safety function level
- plant level
- society level.

The analyst will normally choose between one of the four former levels, while the last one usually will be present as a more or less qualitative boundary condition for the authority making the final decision about the TS issue.

A lower level of analysis usually means a simpler analysis requiring less resources. Therefore, an analysis should generally be performed on the lowest level which both allows the safety impact to be appropriately estimated, and illustrates the changes in parameters of concern. On the other hand, if an analysis has been performed on too low a level, the results may be misleading as the optimum will shift between the levels if the analysed system or component interacts strongly with other systems and components in the plant. This principle is illustrated in Fig. 2.2. It is also possible that some factors influence the risk level in conflicting ways (e.g. better system reliability at the cost of increased transient frequency); such interactions must be evaluated at plant level.

If a numerical acceptance criterion is to be applied to the results of an analysis, two possibilities exist, i.e. either to propagate the results arrived at on a lower level to the plant level by the use of risk importance measures, or to distribute the plant level criterion to lower levels - in both cases risk importance measures will have to be calculated for all analysis levels.

Component level

This level can be chosen if the analysis concerns individual components, and if the action being analysed neither influences the reliability of other components or systems nor increases the risk for plant transients. Examples are analyses concerning the contents of testing and preventive maintenance, and the resulting positive or negative influence on the reliability of the component.

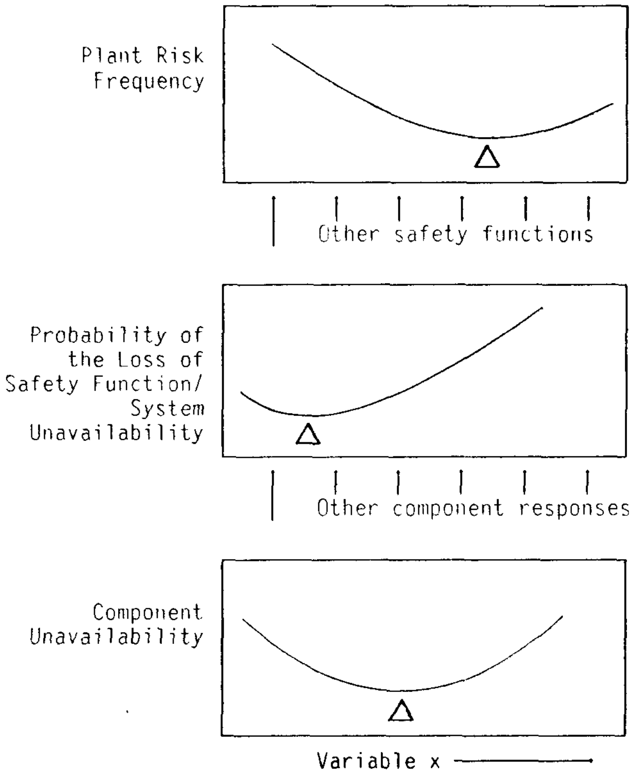


Figure 2.2 An illustration of the shift of optima when considering the influence of a specific variable x at different levels of system.

For these cases, the overall effects of changed component characteristics can be directly estimated on plant level through appropriate risk importance measures (i.e. the safety influence comes only via component basic events).

System level

An analysis can be confined to the system level if it concerns parameters influencing only the studied system, and if this system does not, directly or indirectly, influence the reliability of other systems; neither may the action being analysed increase the risk of plant transients. Examples are analyses of systems with redundant subsystems, where the overall layout of testing and preventive maintenance on component level always will influence the probability of a system failure due to common cause failures. Via risk importance measures on system level, the overall effect on plant level can be directly estimated (i.e. the safety influence comes only via system basic events).

Safety function level

In practice, a functional level analysis is the same as a plant level analysis. This means that it is prompted by the same kind of system interrelationships that are present in plant level analyses, but that these interrelationships are confined to one safety function (e.g. reactor shutdown).

Plant level

Analyses shall be performed on plant level if they concern *interacting* systems, especially support systems (e.g. electrical power supply, protection systems, and cooling systems). In addition, any analysis where the transient risk is directly or indirectly affected must be performed on plant level. Normally, the nominal risk level (average core melt frequency) as calculated in a Level 1 PSA is used as the reference risk; TS changes will be evaluated relative to this reference. If a higher level PSA is used the perspective will be widened accordingly. Three PSA levels can be distinguished as shown in Table 2.3 [2.4, 2.5].

Table 2.3 The levels of probabilistic safety assessment.

- **Level 1 PSA** comprises identification and quantification of accident sequences leading to core damage.
- **Level 2 PSA** includes analysis of core melt progression and containment response, which combined with Level 1 results leads to determination of the magnitude and frequency of radioactive releases.
- **Level 3 PSA** together with results of Level 2 covers environmental transport of radionuclides and assessment of radiation doses to the population. Hereby an estimate of the public risks is obtained.

The analysis must be brought to level 2 or 3 if TS for systems involved in accident mitigation are studied (e.g. systems dealing with containment integrity or with reduction of releases), or if the TS formulation will affect different accident sequences, with different release mechanisms, in different ways.

Society level

The society level is usually the authority perspective, based on information on one of the above levels, and completed with qualitative boundary conditions on plant and society level. Thus, considerations on this level will often involve parameters not connected to nuclear safety.

Usually, the optimization is performed in relative terms, i.e. results of the TS analysis are compared either to a reference level usually given by the plant PSA, or to a set of feasible alternative solutions to the TS problem. Thus, the criterion will depend on the level of analysis, but will usually be:

- Component level :	component unavailability
- System level :	system unavailability
- Functional level:	function unavailability
	core damage frequency
	loss of function frequency
- Plant level :	core damage frequency
	release category frequencies.

2.2.3 Optimization criteria

The question of what criteria to apply in decision making is complicated and controversial. It is complicated because it necessarily will involve the comparison and weighting together of highly disparate and sometimes conflicting influencing parameters. It is also made controversial simply by the fact that it involves the assessment and comparison of risks of potential disasters.

One of the main points in using probabilistic analysis for TS evaluations is to obtain a consistent treatment of a variety of TS issues. Therefore, the basis for the judgement of analysis results must be structured and flexible, meaning that consistent judgements must be used for a variety of issues evaluated in different ways, by different analysts using a variety of methods and boundary conditions. The most important of the criteria types that can be applied in the process of judging analysis results are described below and in Fig. 2.3. [2.6].

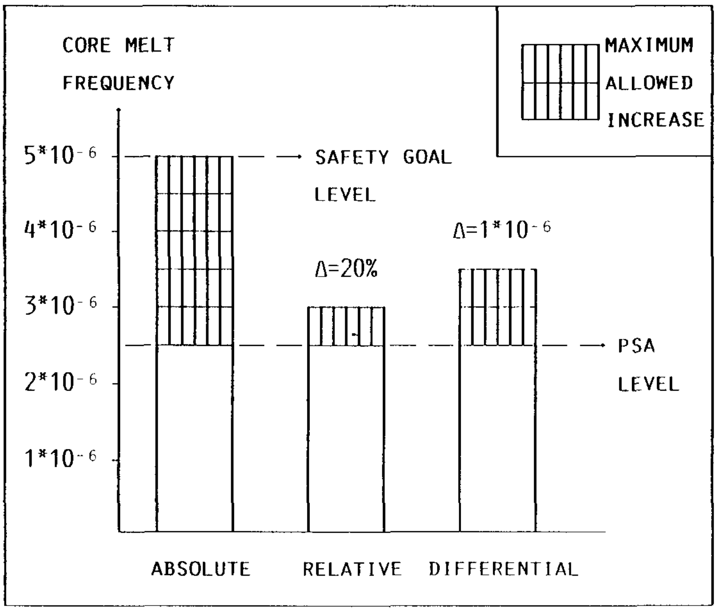


Figure 2.3 Characteristics of some decision criteria.

Within the NKA/RAS-450 project, the problem of decision criteria has been treated in detail in [2.7].

Absolute criteria

This type of criterion implies that TS and changes of TS are handled within a safety goal approach. Changes resulting from TS changes are expressed in absolute terms and judged against absolute acceptance criteria.

Relative criteria

Results from TS analyses are expressed in absolute terms, but judged in terms of relative changes, often with respect to a reference level given by a PSA, or as a comparison between two or more feasible alternatives.

Differential criteria

With this type of criterion, the interest is focused to the absolute size of the risk increase resulting from a TS change. A differential criterion states a maximal allowed risk increase, e.g. Δf(core melt) < 1.0E-07/year.

Trade-off criteria

This approach assumes a constant TS risk level, meaning that any changes resulting in additional risk must be wholly compensated by changes reducing the risk [2.8].

It should be noted that formal cost-benefit criteria are not addressed within the NKA/RAS-450 project, at least not the kind where benefits resulting from a decreased core melt frequency are weighted against safety improvement costs. This is due to the fact that this kind of approach has not been used in the Nordic countries, especially not in connection with TS related matters. However, some degree of cost-benefit considerations will obviously always be present implicitely, usually in the form of boundary conditions rather than as formal numerical decision criteria.

Generally, decision criteria can never be expressed entirely in quantitative terms. Therefore, it will always be necessary for authorities to define frames. A recommendable general procedure for making decisions based on probabilistic evidence is to proceed in two steps:

1. Quantitative demonstration of numerical acceptability, with or without the use of a formal criterion.
2. Case-by-case decision based on weighing of quantitative results against qualitative boundary conditions.

Decisions on TS problems are probably most often handled in this way today. As has already been mentioned, the purpose of TS is to provide an envelope for the safe operation of a nuclear power plant. As a result, TS as such do accept risk increases, and in defining an envelope actually define the acceptable extent of these increases. It is therefore an over-simplification to postulate, as is often done, that increases in absolute risk levels can never be considered or accepted. The extent of the flexibility in absolute terms can only be estimated by using probabilistic methods, while TS were originally formulated deterministically. For this reason, considerable interplant variations can be expected as to the size of the operational envelopes, and in the resulting extent of operational flexibility. Therefore, the relaxation of selected TS rules may be reasonable in some specific cases, and should not be judged out beforehand.

Ultimately, it may become necessary to establish criteria for judging the acceptability of existing TS rules for an individual plant on the basis of an estimate of the size of the operational envelope, expressed in terms of impact on total plant risk.

2.3 Use of PSA methods and results

Methods and models from probabilistic safety assessment (PSA) play an important role in TS optimization. The detailed PSA plant level model, covering all plant safety functions and including many of the interrelationships between systems and components, has proved to be a forceful tool for various kinds of safety-related analyses, including cases where the main focus is not primarily on plant core damage frequency.

It is the integration and coverage of the PSA models that make them especially useful for TS evaluation. This integration applies not only to the explicite modelling of hardware interaction, but to the inclusion of common cause failures (CCF) and human interactions as well. The main use of PSA is for relative comparison, usually between a set of alternative solutions to a TS problem, or for the consideration of a change relative to the reference level given by the PSA result.

For some classes of TS analyses, the PSA fault tree models will be used (directly or with modifications). This applies mainly to analyses on system or plant level, while component level analyses will be focused more on the analysis of the influence on the component performance from various performance shaping factors. In order to assess the impact on plant level from a TS change, risk importance measures for components and systems will be used as a link between lower level analysis results and the plant safety level.

Thus, PSA models and results are always used in one out of two ways, both aiming at estimating the plant level safety impact of a proposed TS change:

1. requantification of PSA fault trees in order to directly obtain the plant level impact, or
2. use of risk importance measures to propagate lower level influences to the plant level.

Risk importance measures are discussed in Chapter 6 of this report.

The problems encountered in using PSA models and results may be inherent to PSA as a technique, in which case they are a basic limitation in TS applications. However, they may also be due to attempting to use the PSA for something it was not originally intended for. If this is the case, it is important to state how and to what extent it might be possible to improve present and future PSAs.

Touching shortly on "inherent" PSA problems, it is unfortunately the fact that two of the factors playing the most important role in overall plant risk, viz. CCF and human interactions, are also among the hardest to treat. The inherently limited basis of experience data will not only result in major parameter uncertainties, but in substantial modelling uncertainties as well. Obviously, both CCF and human interactions are phenomena that are of great interest in connection to TS. However, from the TS evaluation point of view, the state of the art within these areas must be accepted as a starting point.

The remainder of this section will be devoted to the description of some of the problems arising when using a PSA for a purpose it was not originally intended for.

A PSA provides a snapshot of the plant risk level. It shows the average risk level and thereby defines a reference risk. Initiating events are assigned frequencies and thereafter postulated in order to analyse quantitatively and qualitatively the plant response. The kinds of information gained are relative mean measures of component and system importance to plant risk, identification of critical human interactions, weak links in design and procedures, etc. TS evaluations on the other hand, often have time-dependent phenomena in focus. Some of the typical problems resulting from this difference are:

- the PSA risk is usually based on mean unavailabilities of components, while many TS applications require information on the time-dependent behaviour of the components (e.g. standby failure and repair rate).
- the postulation of initiating events makes it hard to handle the possible inadvertent introduction of transients and to calculate margins to scram in different failure situations.

PSA fault tree models may sometimes be on too low a level of detail for a TS application. For hardware this is a minor problem, as it is a relatively straightforward task to increase or decrease the level of detail. A more complex problem is the modelling of operational interactions and recovery options which, if treated realistically, may not fit directly into the model structure of the existing PSA. Examples of less properly covered areas are [2.9]:

- DC supply,
- protection systems,
- external events,
- human interactions, and
- common cause initiators.

In many cases, the TS evaluation presupposes very detailed analysis of failure data, and subsequent requantification of PSA models. The problems encountered in these cases are more concerned with quality, coverage, consistency and interpretation of failure reporting, than with PSA modelling, and will be discussed in Chapter 5 of this report.

The reference risk as given in a plant PSA is not always an absolute entity - often specific boundary conditions of a TS application, or required changes in the PSA model, will make it necessary to define and calculate a new reference risk level.

In many cases of TS evaluations, affected parameters can only be partly expressed in quantitative terms. In consequence, numerical analysis results will have to be judged together with qualitative information. This should not be seen as a weakness of the PSA technique, but rather as something stressing the need for a thorough specification of boundary conditions and basic assumptions of any TS analysis.

Finally, some general recommendations aimed at increasing the applicability of PSAs to TS evaluations are:

- Include the "Living PSA" aspect in the planning stage of the PSA - this will make it possible to decide early on e.g. suitable levels of detail of system fault tree models.
- Use standby failure rates for components instead of mean unavailabilities.
- Calculate and present risk importance measures on component level, system sub level, and system level.

2.4 Relationships to other reliability assurance measures

Quite naturally, the project has concentrated on reliability assurance as it is handled in TS, i.e. through the specification of test and PM intervals as well as of the contents of periodical testing and preventive maintenance (PM).

In consequence, much of the method development has concerned the evaluation of test and PM schemes as they are specified in TS.

A connection between a particular scheme and the equipment reliability can be established by the use of various reliability assurance measures. These techniques all aim at increasing the knowledge about the plant, system, and component status, and will ultimately be an aid in prescribing adequate frequencies and contents of periodical testing and PM. Methods used include:

- Performance indicators
- Reliability centered maintenance
- Condition monitoring
- Data analysis and analysis of operating experience
- Plant status monitoring.

Performance indicators

The performance (or status) of a plant with respect to some crucial parameters, e.g. safety, availability, radiation doses, or economics, is reflected directly or indirectly in a number of indicators. A performance indicator (PI) system makes a systematic interpretation of the information obtained from operating experience, and presents the current status as well as trends for the parameters of main interest. Table 2.4 shows about 30 candidate indicators defined and chosen in a Finnish project [2.10]. The detailed indicators, included in this table, are primarily aimed at serving the power utility, particularly the plant's manager and other staff in detecting and preventing possible negative phenomena developing at the plant. A PI system will also provide information to authorities and the public and for international information exchange.

Table 2.4 Candidates for performance indicators [2.10].

Safety related events (Nb, yearly number of occurrences) Actuations of the safety systems (Nb) Equipment failures in the safety systems (Nb) Effectiveness of the surveillance programme (%)
Capacity factor (%) Energy availability factor (%) Forced outage time (days) Duration of the refuelling outage (days) Unplanned energy unavailability (%) Significant power reductions and outages (Nb) Reactor scrams (Nb) Turbine trips (Nb)
Proportion of preventive maintenance (%) Proportion of repair time to allowed outage time (%) Proportion of active repair time in unav. duration (%) Proportion of maintenance overtime (%)
Collective radiation exposure (manSv) Exceedences of regulatory radiation dose limits (Nb) Occupational lost-time accidents (Nb) Occupational lost-time accident rate (1/1000000 h)
Radiation exposures in environment (microSv/50 years) Liquid and gaseous releases (%)
Volume of radioactive wastes (m^3) Radioactivity of wastes (GBq)
Leakages in fuel elements (Nb)
Thermal performance (kJ/kWh)
Cost of electricity produced (FIM/MWh)

Reliability centered maintenance

The application of a reliability centered maintenance (RCM) program aims at increasing the efficiency of a PM program by systematically mapping functional failures and failure causes, and working them through a decision logic in order to decide on the necessity of applying a PM task. All PM tasks are based on safety, operational, or economical concerns. The implementation of RCM encompasses five basic steps [2.11]:

1. Collection of design/operating information

2. System identification and partitioning

3. Requirement analysis
   Functionally Significant Items (FSI) identified; an FSI is defined as an item which:
   . is a threat to safety at failure
   . remains undetected at failure
   . affects operating capability
   . results in unusually high repair costs
   . is affected favourably by scheduled PM
   Only the dominant failure modes are of interest [2.12].

4. Preventive maintenance (PM) task selection
   A decision logic is used in order to judge on the character of the failures of the FSI, and to identify efficient PM and testing measures.

5. Implementation
   A PM plan is established and translated into a procedure by which a PM program can be implemented.

Condition monitoring

Condition monitoring is used to detect degradations and faults in continuously running equipment before the degradations have developed into functional failures. Prediction of failures in rotating machines by wear particle analyses and vibration analyses are typical examples of condition monitoring. Condition monitoring can also be used to increase the possibility of detecting latent failures in standby safety systems. Periodic testing and preventive maintenance are two means of monitoring component condition; others may be the automatic surveillance of process parameters giving indication of component status.

Data analysis and analysis of operating experience

Achieving lower failure rates of components often influences the availability of safety systems more than can be achieved by reducing Allowed Outage Times in TS. Important components from the plants safety point of view should be analysed by use of trend analysis of failure modes [2.13]. Emphasis should be given to identification of recurring failures, common cause failures, and failures due to poor maintenance or other human errors. The means to achieve lower failure rates include design modifications or improvements in maintenance and testing procedures. On plant level, comparison of different unit's failure frequencies of important equipment, and their trends, is a means of identifying both problems and opportunities for improvements [2.14].

Plant status monitoring

The basic idea in a plant status monitoring system (PSM), is to computerize the control of the safety status of a plant, e.g. with respect to Technical Specifications. A pilot version of a PSM system for the control in real time of LCOs at Forsmark was implemented at the plant in experimental use in 1981 [2.15]. The system could also be used in a planning mode, i.e. the operator may suggest changes for maintenance or repair and check what consequences the actions will have with respect to LCO rules. Due to the low number of failures, the high level of redundancy and the strict separation in safety-related equipment, the PSM system was not implemented for commercial operation at the Forsmark plant.

Presently the U.S. Nuclear Regulatory Commission is considering the development of a computerized system to apply risk and reliability models, calculations and rules to advice the operator of allowed operating limits and conditions based on current plant configuration [2.16, 2.17]. Thus in combination with a living probabilistic safety assessment (PSA), a PSM system might be a useful tool for controlling the safety level of a plant.

2.5 Economical aspects of safety assurance

For several reasons, the introduction of elements of economical optimization into safety-related considerations is difficult and sometimes controversial. This is especially true for the nuclear industry. Part of the problem lies in the difficulty of finding an adequate risk measure; the risk picture is complicated by involving a number of different consequences (i.e. a multivariable situation). The usual approach when analysing the advantages of an action in economical terms, is to make a cost-benefit analysis. While the economical benefits of a suggested action (equipment redesign, procedure change, TS change etc.) can be quite easily defined and determined, the assessment of the associated risks and the expression of these in terms of costs is a formidable task. Accidents like Seveso, Three Mile Island, Bhopal, and Chernobyl have shown that the expression of the total losses in monetary values is not always possible, and that some effects can never be expressed.

Thus, some of the most important aspects that influence decision making in the nuclear industry are not technical but social. The technical assessment of risk typically models the impact of an event or of a human activity in terms of direct harms. It has become increasingly apparent that the consequences of risk events may extend far beyond direct harms to include significant indirect impacts (e.g.

liability, loss of confidence in institutions, alienation from community affairs, etc.).

In order to analyse economical aspects in safety assurance, three aspects must be covered:

Direct impact

Includes the direct costs resulting from severe accidents within the actual nuclear industry. These costs often are only a small proportion of the total economical consequences.

Indirect impact

Indirect impacts may contribute significantly to the total costs. Moreover, the effects are usually not confined to the operator and owner of the plant, but will affect the entire nuclear industry and society as a whole.

Public opinion

The public attitude towards risks has a much greater impact on decision makers than was the case before, and will have to be considered carefully.

What was described above may in some ways be on too high a level of consideration for day-to-day risk issues. Thus, for decisions concerning TS changes or plant modifications, we are often in a situation permitting relative comparison of risk changes. In these cases, the economical "optimization" may be the achievement of as favourable a result as possible within given economical limits. In practice this is often done by selecting one out of a number of predefined feasible alternatives.

REFERENCES

2.1 Vesely, W. E., Samantha P. K. & Boccio, J. L. White Paper Summarizing the Major Findings of the PETS Program on Risk Analysis of Technical Specifications. Brookhaven National Laboratory. Technical Report A-3230, September 9, 1987.

2.2 Reactor Safety Study, An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants. USNRC Report, WASH-1400, (Nureg-75/014).

2.3 Mankamo, T. Availability Analysis of Standby Safety Systems. Basic methodology for the optimization of the test and repair arrangements and limiting conditions of operation. Thesis Manuscript, 1986.

2.4 PRA Procedures Guide. NUREG/CR-2300. January 1983.

2.5 Bengtsson, G., (Editor). Risk Analysis and Safety Rationale. Final Report of a Joint Nordic Research Program in Nuclear Safety. Nord, December 1989:91.

2.6 Samantha, P. K., Vesely, W. E., Lofgren, E. V., Boccio, J. L. Risk Methodology Guide for AOT and STI Modifications. BNL Technical Report A-3230, February 1986.

2.7 Knochenhauer, M. Decision Situations and Criteria in Modification of Technical Specifications. ABB Atom Report RPC 89-46, NKA/RAS-450S(89)2. February 1990.

2.8 Sullivan, W. P., Ha, C., Pentzien, D. C., Visweswaran, R. S. Technical Specifications Improvement to Containment Heat Removal and Emergency Core Cooling Systems. EPRI NP-5904. General Electric Nuclear Energy. July 1988.

2.9 Hirschberg, S., (Editor). Dependencies, Human Interactions and Uncertainties in Probabilistic Safety Assessment. Final Report of the Nordic NKA-project Risk Analysis RAS-470. To be published in Nord Series in May 1990.

2.10 Lehtinen, E., Himanen, R., Viitasaari, O. Experiences from the Developing of Performance Indicators for the Finnish Nuclear Power Plants. Proceedings of the International Conference on Availability Improvements of Nuclear Power Plants, Madrid, Spain, April 10-14, 1989.

2.11 Krasnodebski, J., (editor, Ontario Hydro), Reliability Centered Maintenance, Draft standard document from IEC TC56 WG6, October 1989.

2.12 EPRI NP-6152. Demonstration of Reliability Centered Maintenance. Prepared by Electric Power Research Institute. California. January 1989.

2.13 Nyman, R., Carlsson, L., Andersson, L. How to Introduce Trend Analysis Using Probabilistic Methods. Procedures of the SRE'86, Society of Reliability Engineers Symposium 1986, Otaniemi, Finland, October 14-16, 1986.

2.14 Laakso, K. A Systematic Feedback of Plant Disturbance Experience in Nuclear Power Plants (in Swedish). Helsinki University of Technology, 1984.

2.15 Dahll, G., Dwortzak, F., Karlsen, B., Karlsson, B., Skjerve, G. The Computerized Safety Technical Specifications (CSTS) System for the Forsmark 1 Nuclear Power Plant. Halden Report HPR 284, November 1981.

2.16 International Atomic Energy Agency. Consultant's Report on the Use of Reliability Methods and Probabilistic Safety Assessment to Improve NPPs Operational Limits and Conditions. Wien. 4 - 8 December, 1989.

2.17 Atefi, B., Gallagher, D. W. & De Moss, G. M. Feasibility Assessment of a Risk-Based Approach to Technical Specifications. Prepared for U.S. Nuclear Regulatory Commission. Report SAIC-90/1033. March 1990.

3. SURVEILLANCE TESTING

Standby equipment are usually periodically tested in order to check their operability. By this means, the risk of latent faults, which accumulates during standby time, can be limited. Periodical tests also enhance the early detection of developing faults, which is especially important for the control of common cause failures.

3.1 Factors to be considered

Surveillance testing is a primary tool for the reliability assurance of standby equipment. Part of the tests are confined to checking the component or subsystem operation. In addition, testing of safety functions or plant functions is done in order to verify the interoperability of components and systems. Although the surveillance tests are aimed at simulating real demands as closely as possible, there still remain differences. The representativeness of tests is highly specific to components and systems, and depends on many factors.

Furthermore, the complexity of test arrangements as a TS issue is increased by the relationship to other measures of condition monitoring, which contribute in the detection of developing failure mechanisms or latent faults.

3.1.1 Variables for optimization

The many factors and relationships influencing the balanced choice of test arrangements include:

- test procedure and method
- relationship with other condition monitoring methods
- test interval
- test timing scheme in redundant subsystems
- test related disturbance risks
- relationship with LCO shutdown influences.

The test procedure and method determines the coverage of testing relative to the actual failure modes and demand conditions, and the negative side effects such as component degradation, introduced errors and risk of plant disturbances. The surveillance tests shall also be balanced in relation to component status monitoring, diagnostics and preventive maintenance, which provide other means for the detection of developing failure mechanisms.

The test interval is often the primary free variable which, however, has contradictionary influences as presented in Fig. 3.1. Balancing between these influences is a main optimization task.

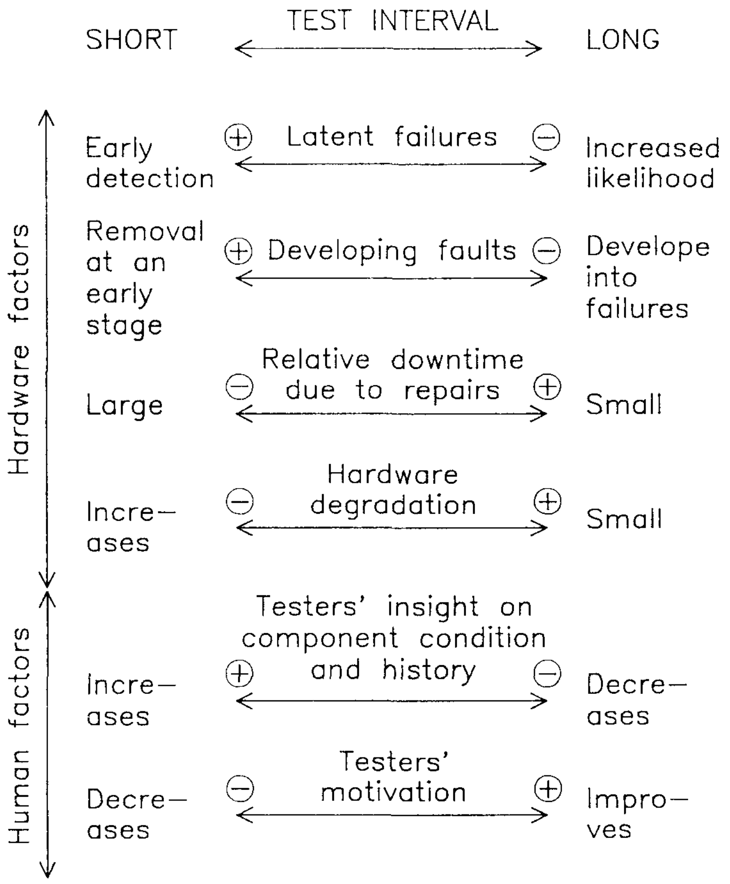


Figure 3.1 Test interval influences.

In systems with internal redundancy, the relative timing of tests of the redundant subsystems (so called test staggering) is also an important factor. It affects the detection of common cause failures, and the likelihood of introducing them by systematic errors.

The test procedure or actions can in certain cases include risk for disturbances to plant operation, especially if power generation needs to be reduced for the time of testing or if the test concerns equipment in the reactor protection system. The analysis scope needs to be appropriately extended in order to cover these connections in the optimization of test arrangements.

LCO criteria are likely to become crucial in connection with failures detected in surveillance tests. Hence, both allowed outage times (AOT) during plant operation and test arrangements need to be considered in such cases.

3.1.2 Other technical factors

The negative side effects of testing include in some cases component degradation. An example is the stress following from cold starts of diesel generators. On the other side, the periodic piecepart movement may also influence positively. For example, diesel motor roll-over prevents oil films dryout, and closing valve movement limits accumulation of corrosion products. These kinds of technical factors tend to be difficult to measure exactly, and need to be taken into account by engineering judgement in supplement to model considerations.

3.1.3 Organisational and economic factors

Many persons are involved in the chain of planning the tests, carrying them out, and in evaluation of test results. Proper communication is essential for the efficiency, coverage and correctness of the whole effort. The links in the chain need also to be continuosly updated to reflect plant modifications and new experience.

Surveillance tests impose personnel load. To a certain degree this may be desirable in order to maintain operational knowledge and readiness. The tests also mean costs, specially if power reduction is needed. These factors are secondary compared to safety optimization, but in practice they affect decisions about test arrangements, and they may have a determining role when the safety optimum is insensitive to the alternatives considered.

3.2 Level of consideration

The hierarchy of TS consideration levels was already discussed in section 2.2 of this report. Here they are illustrated for an analysis of test arrangements in the resolution flow diagram, Fig. 3.2. The marked parts show the applied resolution flow in the case study. As shown in Fig. 3.2 the resolution process is divided into a prestudy stage and a probabilistic study stage. The later stage in the resolution strategy will be brought into effect if the earlier evaluation shows that safety or cost benefits are likely to justify a deeper probabilistic study.

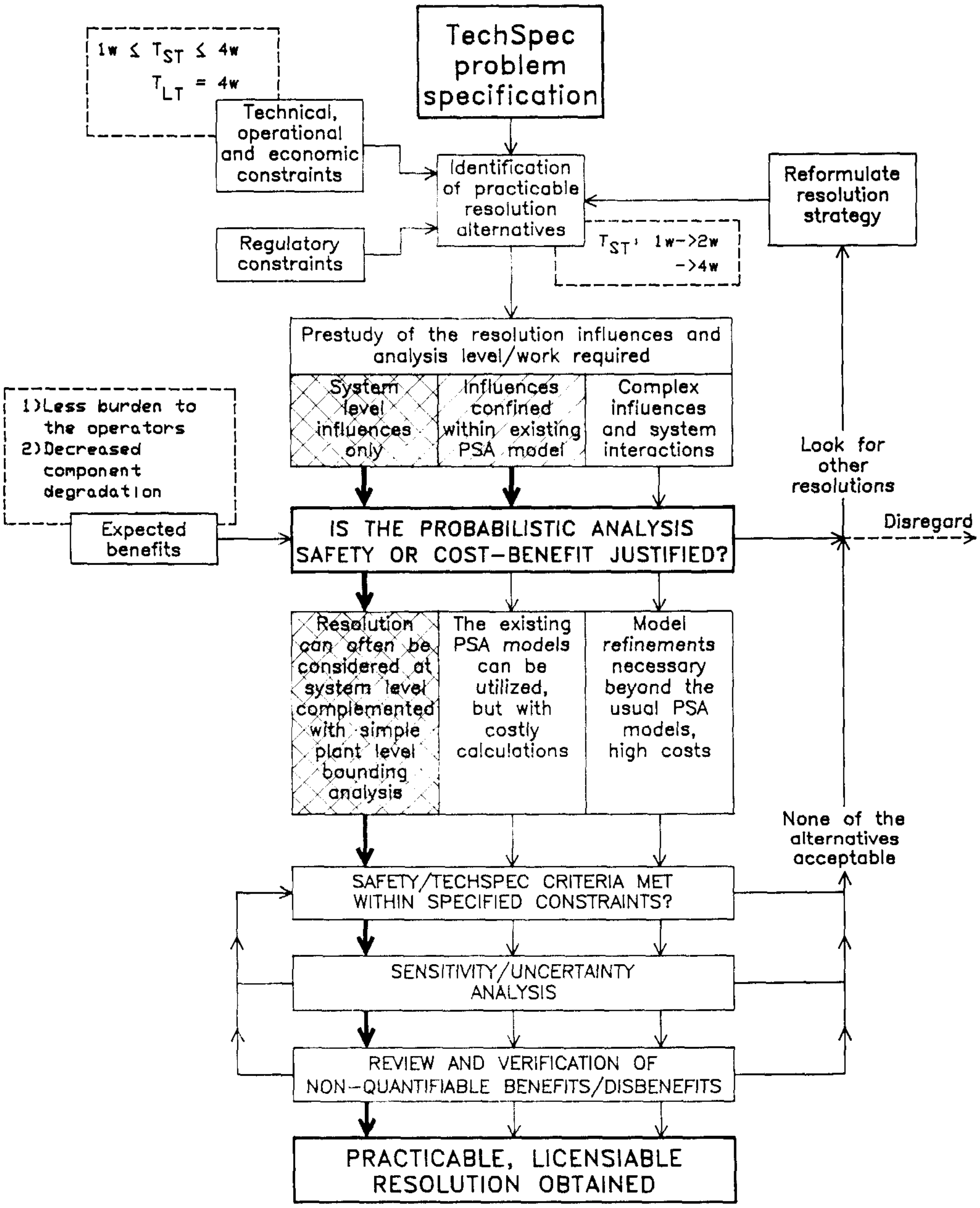

1w ≤ T_ST ≤ 4w
T_LT = 4w
TechSpec problem specification
Technical, operational and economic constraints
Identification of practicable resolution alternatives
Reformulate resolution strategy
Regulatory constraints
T_ST, 1w->2w ->4w
Prestudy of the resolution influences and analysis level/work required
System level influences only
Influences confined within existing PSA model
Complex influences and system interactions
1)Less burden to the operators
2)Decreased component degradation
Look for other resolutions
Expected benefits
IS THE PROBABILISTIC ANALYSIS SAFETY OR COST-BENEFIT JUSTIFIED?
Disregard
Resolution can often be considered at system level complemented with simple plant level bounding analysis
The existing PSA models can be utilized, but with costly calculations
Model refinements necessary beyond the usual PSA models, high costs
None of the alternatives acceptable
SAFETY/TECHSPEC CRITERIA MET WITHIN SPECIFIED CONSTRAINTS?
SENSITIVITY/UNCERTAINTY ANALYSIS
REVIEW AND VERIFICATION OF NON-QUANTIFIABLE BENEFITS/DISBENEFITS
PRACTICABLE, LICENSIABLE RESOLUTION OBTAINED

Figure 3.2 TS problem resolution strategy in the analysis of test scheme alternatives for diesel generators [3.1].

3.2.1 Component level factors

The test interval and test method, equipment specific factors such as piecepart movement or roll-over needs, and test caused degradation effects can often be optimized at the component level, assuming no significant influences for the reliability of other components, systems or plant operation. Practical examples will be presented in section 3.3.

3.2.2 System level factors

A system level consideration is necessitated if:

- test procedure affects the operability of redundant components or system configuration, and especially if
- test scheme alternatives are considered, because of CCF influences between subsystems.

Examples of the former type are the reactor protection system (RPS) tests, where the operational logic of the remaining channels is changed during the time of testing one channel.

Confining the analysis to system level presupposes that no significant connections exist with respect to the reliability of other systems or to plant operation.

3.2.3 Plant level factors

Plant level considerations become necessary, if the test arrangements affect several systems. This is usually the case for protection, electric power supply and other support systems. Such is also the case if one sub in each of several primary safety systems is simultaneously disconnected for testing. If containment isolation functions are affected, consideration at PSA Level 2 becomes necessary.

Also balancing with respect to test related transient risks can only be done at the plant level. Examples of such cases are:

- reactor protection system tests, where the test procedure directly, or the simulated partial (single channel) trips involve a specific transient risk
- main steam line isolation valve tests and turbine and bypass stop valve tests in BWRs, as these presuppose power reduction and configuration changes in main steam supply with associated disturbance risks.

3.2.4 Choice of the level

The significant factors to be taken into account, and hence the level of consideration, depends much on the proposed alternatives as well as on component, system and plant specific features. It is hence recommendable to map the influences at an early stage, in order to properly predict the appropriate analysis boundary, which then determines the data and model input needed, and work required. This mapping stage is included in the prestudy block of the resolution flow diagram in Fig. 3.2.

In some cases the detailled work can be confined to the system or component level, and the additional influences can be determined easily by the use of an existing plant PSA. The test scheme rearrangement study discussed in section 3.4 represents an example.

3.3 Testing standby components

3.3.1 Unavailability concept

The primary reliability measure of a standby component is the instantaneous unavailability u(t):

u(t) = Probability of the component being inoperable if challenged at time t

This is schematically illustrated in Fig. 3.3 for a periodically tested standby component. During the standby time the plant operator does not know about the presence of possible latent critical faults. He can only associate a probability with them. During the intervals between the tests, the instantaneous unavailability increases as the probability of latent faults accumulates. It decreases to a residual value, when the component is successfully tested, as the absence of latent faults is confirmed. In practice, the unavailability does not drop to zero after a successful test, because:

- the testing itself may cause faults that remain undetected until the next test
- some faults may not be detected at all in the test (and their contribution may again accumulate until more perfect test or actual demand)
- in addition, some faults may be inherently independent of the time from the preceeding challenge and they may result in failure with a non-zero probability also after a perfect test.

Examples of the last type, are failure mechanisms which progress only when the component is called upon to operate, but which are "frozen" while in the standby state.

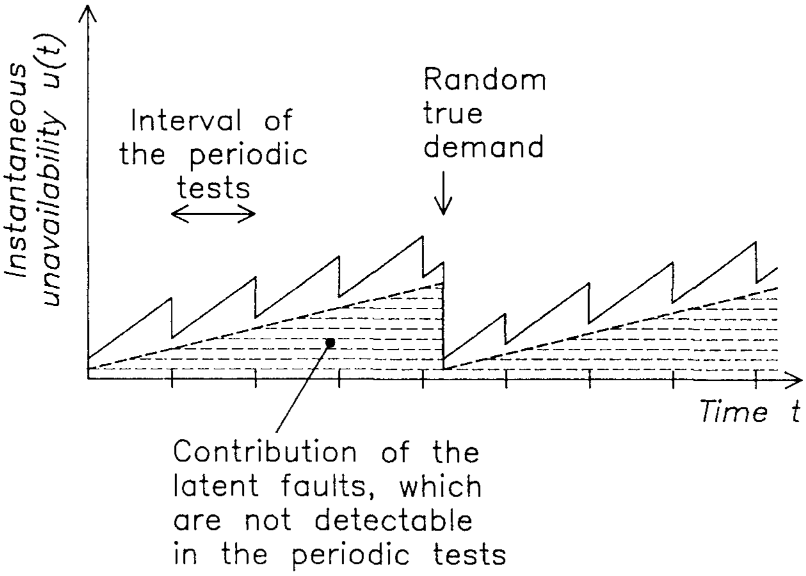


Figure 3.3 An extended unavailability model of standby component.

3.3.2 Simple q+λt model

A simple model of the instantaneous unavailability is given by [3.2]:

$$\begin{aligned} u(t) &= q + (1 - q)(1 - e^{-\lambda t}) \\ &\cong q + \lambda t, \text{ if } q, \lambda t << 1, \end{aligned}$$

where q = Time-independent contribution
λ = Standby failure rate
t = Time elapsed from the previous surveillance testing or operation on other demand.

This simple linear model often approximates the most important features of the standby component's unavailability reasonably well [3.2-5]. More developed models [3.6-7] are applied to investigate different test related failure mechanisms more closely [3.8, 3,9].

3.3.3 Failure modes covered by testing

The testing procedure influences which faults and failure modes are detected, i.e. it determines the effectiveness of testing with respect to latent faults. A usual classification of failure modes for standby components is presented in Table 3.1. Depending on the detection possibilities, the unavailability time may be quite different for the various failure modes, Fig. 3.4.

In many cases, surveillance tests only cover the failure mode for the main function while other failure modes may be less properly covered. Examples are failure modes specific to long operation times of standby pumps or diesel generators [3.1]. In other cases, the operating parameters (pressure, temperature, voltage level etc) may differ during tests considerably from the conditions encountered in some accident conditions [3.10], as will be discussed in more depth in section 5.1.1.

Table 3.1. Definition of functional failure modes, as used for standby diesel generators [3.2-3.4].

	FUNCTIONAL CONSEQUENCE	
OPERATIONAL PHASE	NONCRITICAL	CRITICAL
Component state at fault occurrence/ detection	Prevents operation only during active repair	Component inoperable directly
MONITORED IN STANDBY Detected via instrumentation, walkarounds, etc	MN Monitored noncritical	MC Monitored critical
LATENT IN STANDBY Detected at test or other start/demand	LN Latent noncritical	LC Latent critical
FAILURE DURING OPERATION Fault occurs after start	FN Fault during operation, noncritical	FC Failure to operate, critical

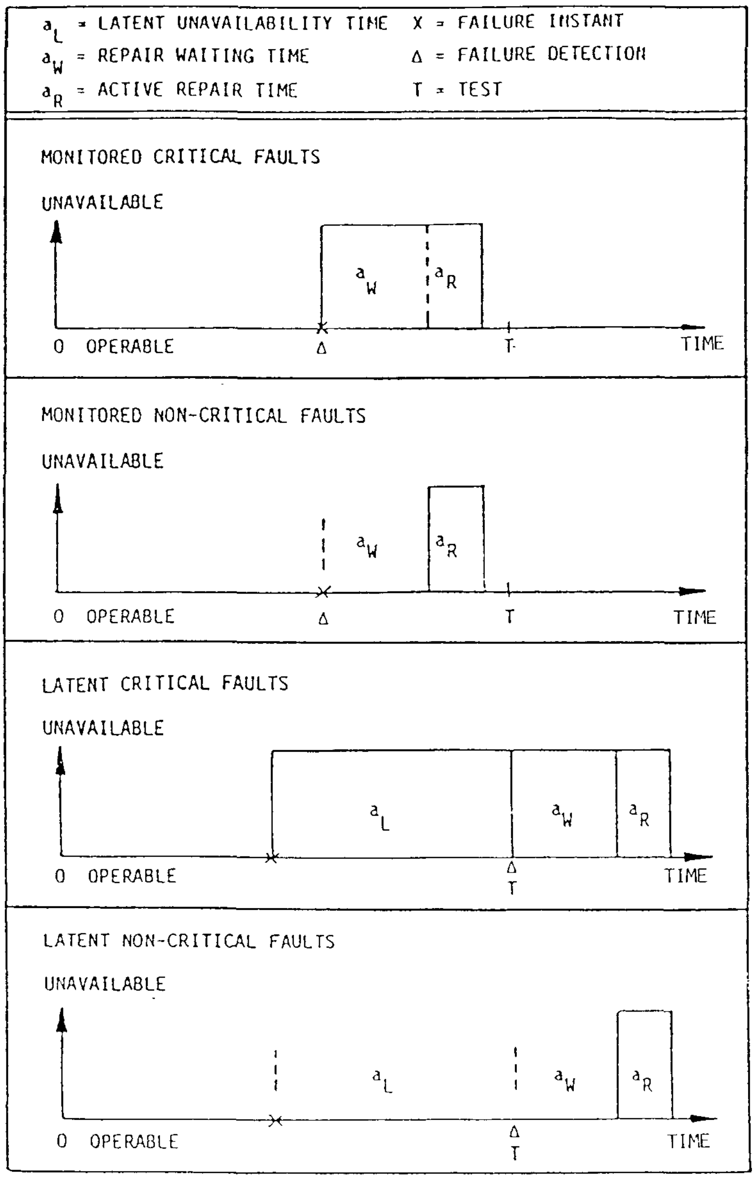


Figure 3.4 Unavailability times when considering effects of functional failure modes on standby component [3.2].

In practice, the surveillance tests during plant operation cannot be designed to be 100 % perfect. Principally, the only perfect test is a real demand situation, such as the occurrence of an (unplanned) plant transient or a real accident. By this we do not intend to say, that severe plant transients should be "simulated" more often, because they constitute a specific risk also, mostly outweighting the benefit of more efficient detection of latent faults in some equipment. A more balanced solution might be, for example, improvements of condition monitoring in association with overlapping periodic tests or overhaul maintenance.

After essential plant modifications, selected plant transient tests should be performed in order to test the interoperability of plant functions. For such cases, occurred plant transients could be credited as integral tests, if the associated event sequences, system responses and electric load sequences were analyzed systematically [3.11]. In specific cases, experienced transients can substitute periodic tests; if they are satisfactorily recorded.

3.3.4 Experiences and data

Obtaining relevant empirical data for the many factors associated with the test arrangement optimization is essential. Improvements in failure reporting and data bases is a necessary precondition for the development and verification of the models needed.

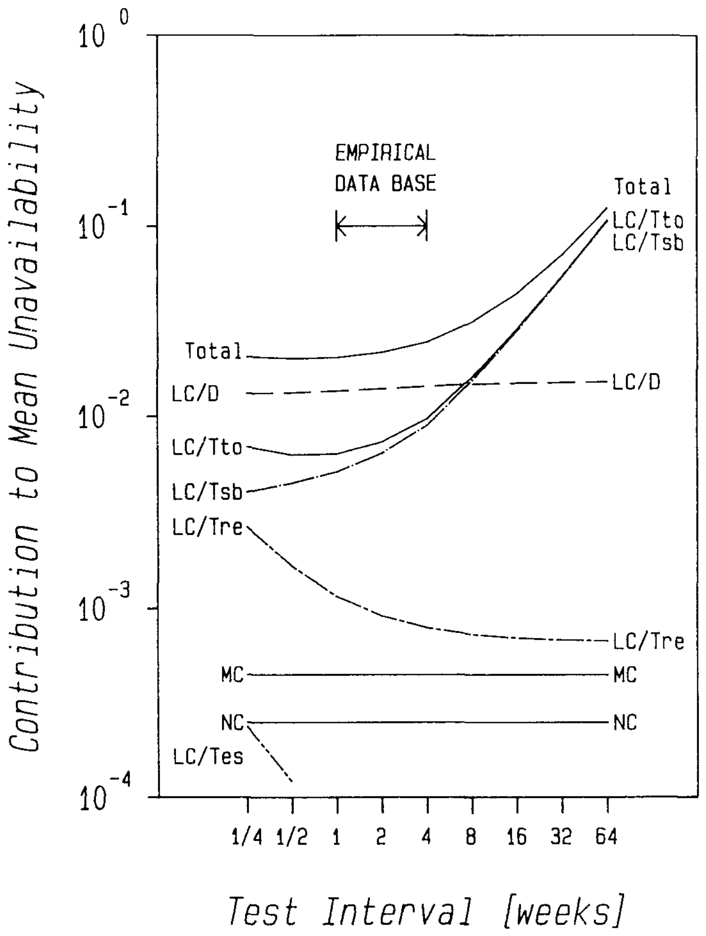
In the Nordic countries the following work has been done this far in order to collect adequate data for this purpose:

- Finnish-Swedish diesel generator study [3.4]
- TVO closing valve study [3.3]
- Finnish power plants/feedwater pumps study [3.2, 3.12]
- Forsmark 1/2 diesel generator study [3.1]
- Motor operated valves, data analysis [3.13-14].

Besides providing reasonable verification for the unavailability models, these data analyses have contributed to several recommendations for practical improvements. The data base problems will be further discussed in Chapter 5.

3.3.5 Practical applications

The probabilistic considerations (and data analyses) of test intervals and procedures have this far concentrated on diesel generators (DG) and motor operated valves (MOV), as listed above. For diesel generators, a typical outcome is presented in Fig. 3.5 [3.1]. In that case the total mean unavailability is rather insensitive within the range of usual test intervals 1...4 weeks. Thus, different technical and operational factors may be given the leading role when deciding the DG test interval. Similar studies for MOVs have shown a stronger sensitivity to test interval [3.13]. One of the most important results of the diesel



LC/D	Latent critical, detected only in annual test/demand
LC/Tsb	Latent critical, detected in ST/LT, standby period
LC/Tre	Latent critical, detected in ST/LT, repair period
LC/Tes	Latent critical, detected in ST/LT, test period
LC/Tto	Latent critical, detected in ST/LT, in total
MC	Monitored critical, repair period
NC	Noncritical, repair/disconnection period
ST	Start test
LT	Load test

Figure 3.5 Unavailability contributions for a diesel generator as the function of start/load test interval [3.1].

generator studies was the dominant contribution of "hidden latent" faults (LC/D), which are not deemed to be detected in the periodic start and load tests but only in actual demands or annual subsystem tests.

In a recent application, the coverage of surveillance tests was investigated for the auxiliary feedwater system (AFWS) in Forsmark 1/2 [3.8]. The coverage of the test of RPS signals is presented in Fig. 3.6. This test is performed annually, at the plant startup after the refuelling outage. The water is injected against low reactor pressure. The functional verification for some blocks was estimated to be close to 100 %, while for some other blocks it was small, owing to the differences between the test functions and the real demand situation. (More representative tests with injection against full reactor pressure are performed separately.)

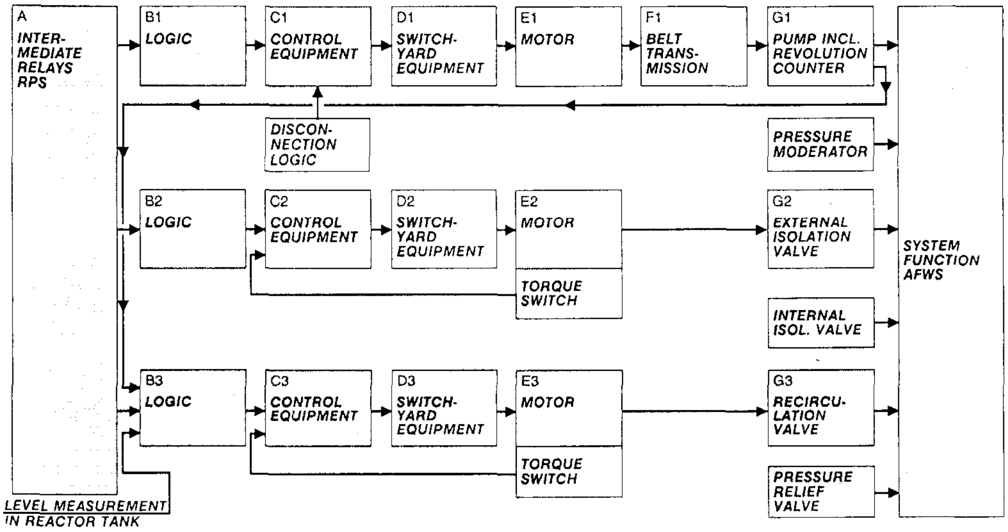


Figure 3.6 Test coverage chart for the test of RPS signals in the auxiliary feedwater system [3.9].

In another application for motor operated valves at Forsmark 1/2, considerable deviations for some valves were identified between test and real demands during anticipated accident conditions [3.10]. The crucial parameters were the differential and absolute pressure, and the temperature. The different types of valves (gate, globe and ball valves) were found to be affected differently by the deviations. The outcome is also significant for the PSA data issue, because the validity of the failure data mainly originating from surveillance tests (and only to a very limited extent from real demands and not at all from accident conditions) can be questioned. However the results indicate that the periodic tests are fairly representative for most transient situations.

3.4 Testing redundant subsystems and CCF influences

3.4.1 Test arrangements for systems

Full scale safety function tests may be excluded due to the transient risk imposed, or due to undesirable stresses imposed on equipment. In many cases they can be carried out under strict control, usually in cold shutdown or at low reactor power in connection to the refuelling outage. The function tests are supplemented with more frequent testing limited to subsystems or components. Examples are:

- pump line tests where water is recirculated but not injected into primary system
- isolation valve open/close movements
- RPS channel tests where the actuation of the front line safety system is blocked out.

Because of the limited extent, the question of coverage becomes important as discussed earlier. Subsystem/component tests are useful to a specific degree. With proper planning of overlapping and in combination with less frequent funtion tests, they provide an adequate coverage and control of both latent, developing failure mechanisms and functional interrelationships.

3.4.2 Test scheme and CCF issue

For periodic tests of redundant subsystems (called here subs), different time schemes are used. In Fig. 3.7, common schemes are presented for a four sub structure.

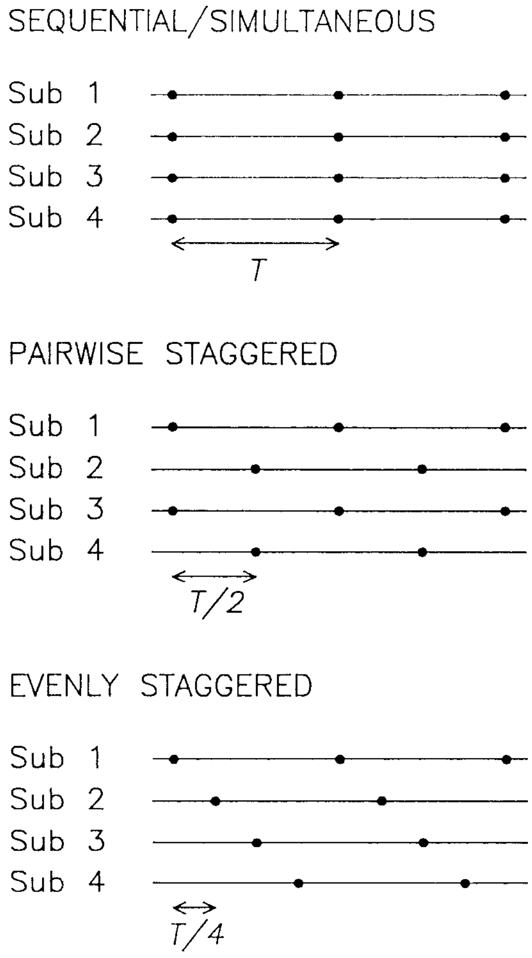


Figure 3.7 Basic test schemes in the case of four subsystems. The test interval, i.e. the cycle of the time scheme is denoted by T.

In the sequential test scheme the subs are tested in chain usually within one shift time. A variant of this is simultaneous testing, which, however, should be avoided due to the apparent risk of systematic errors (which may remain undetected or be impossible to recover directly). The sequential test scheme is also relatively prone to repeated errors, because then the test and possible associated maintenance actions are carried out by the same person(s) in sequence.

The staggered test schemes are used in order to distribute the test work more evenly along the time axis and between different shifts and persons. In addition to lower vulnerability to systematic errors, the staggering has apparent advantages with respect to discovering latent common cause failures and starting repair at least in one sub. On the other side, staggering imposes stricter demands on the communication between testers, and on the evaluation and synthesis of test results.

In contrast to fixed schemes, tests may be performed adaptively. For example, in a staggered scheme, an additional test may be performed on redundant components, if one subsystem is detected failed in a periodic test. Another example is the rule specifying a relationship between test interval and the number of observed failures in a given time period. This kind of rule should be applied sparingly. In case of recurring failures, the primary emphasis should be on the identification of the root causes and on their elimination.

3.4.3 Practical applications

Examples of system level studies are:

- different test arrangements for AFWS at TVO I/II [3.15]
- test scheme rearrangement for DGs at Forsmark 1/2 [3.1].

In both of these studies, the background was that the operating staff had begun to experience that the tests may be too frequent for AFWS pumps and DGs, respectively. Probabilistic studies supported the decision to change the sequential scheme with weekly tests to biweekly, with pairwise staggered scheme as an optimal resolution with respect to both calculational and practical considerations. A similar test arrangement study has been performed in the U.S.A. for an RPS/scram relay system [3.17].

3.5 Other means of condition monitoring

Periodic testing is only one method in parallel to component diagnostics, condition monitoring instrumentation, preventive maintenance, walk-arounds etc. These all in combination provide a possibility to identify faults early. Fig. 3.8 represents a simplified thinking model on these phenomena. In practice, the detection levels depend on the fault type and operating conditions.

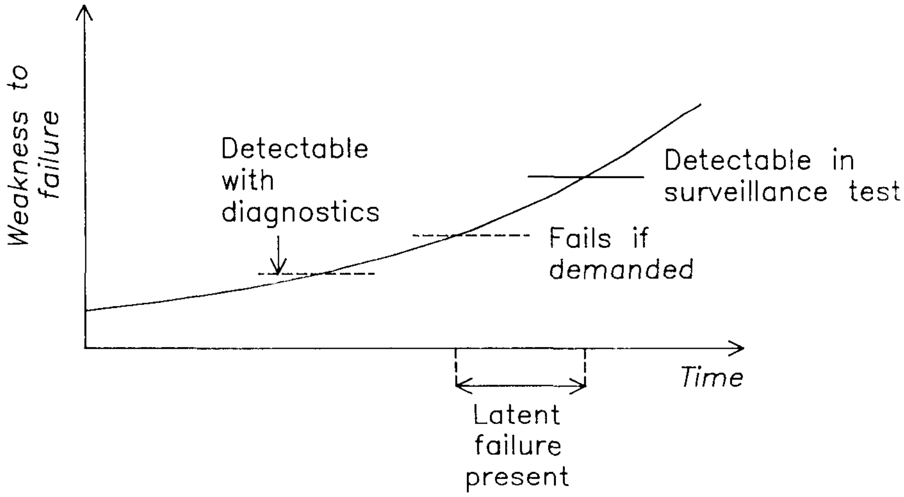


Figure 3.8 A schematic model of fault detection levels.

The Finnish-Swedish diesel generator study [3.4] gave apparent indications of the described phenomena, and this was further confirmed by the recent study for the diesel generators of Forsmark 1/2 /[3.1]. A few percent of the faults seem to be undetectable in periodic start and load tests. These faults may contribute significantly to the total mean unavailability due to their long latence time. Achieving more information on this aspect on other standby equipment would be highly valuable in future analysis of plant operating experience.

Plant transients also represent tests, as already discussed. There may exist design and tuning deficiencies in equipment, or functional interrelationships, which are by no other means tested completely. Systematic in-depth analyses of experienced plant transients could provide valuable information for the coverage of such gray areas [3.11].

3.6 Man-machine interface

Operator-system interface may influence significantly via the test arrangements. In fact, the testing can be considered as a chain of actions and information flow between:

- test planning with input from suppliers
- test procedures and preparations
- actual testing with associated maintenance
- evaluation, reporting, synthesis and acceptance of test results.

As there are different persons involved, and because of modifications in test practices are done quite frequently, the communication of, for example test objectives in one direction and test results into the other direction, is of central importance [3.18]. E.g. lacking understanding of test or maintenance objectives can lead to degradation in motivation and human performance. Consequently, restoring of equipment into on-line operability after test or maintenance may in some cases be omitted.

At the best, when surveillance tests are done by the same, well trained and motivated persons, there are good possibilities to detect developing faults through their early symptons, which enhance prevention of common cause and other functional failures.

If, however, the tests are done more or less randomly by different persons, the communication needs become pronounced in order to guarantee proper synthesis from diverse test outcomes.

These kinds of human influences are difficult to model, not to say anything about quantification. Systematic identification methods have been applied with good experiences [3.19]. The model calculations should always be supplemented by engineering considerations to check the implications of the human factors.

3.7 Summing up all factors

Planning of test arrangements means balancing between many component and system specific technical factors, human and organisational factors, as well as operational and economical factors. In cases where the test arrangement alternatives include many connections and contradictory influences, systematic qualitative and probabilistic analyses can be expected to provide a structured treatment as a support for decision making. To some extent the influences are usually not exactly known. Hence, the analyses need to be combined with technical valuation which still has the primary role.

Due to the lack of knowledge on many contributors, the analysis of operating experiences must be emphasized. Test arrangements should be updated according to the gradually increasing knowledge and technical modifications.

Unnecessary or useless tests should be withdrawn or modified, while effort should be laid down on problem areas or uncertain areas. Most importantly, tests should properly reflect actual demand situations. Information on these accumulates also via PSA studies.

REFERENCES

3.1 Engqvist, A. & Mankamo, T. Test scheme rearrangement for diesel generators at Forsmark 1/2. PSA'89 International Topical Meeting on Probability, Reliability and Safety Assessment, Pittsburgh, NKA/RAS-450(89)3. April 2-7, 1989.

3.2 Mankamo, T. & Pulkkinen, U. Test interval optimization of standby equipment, Technical Research Centre of Finland, Research notes 892, NKA/RAS-450F(86)2. September 1988.

3.3 Mankamo, T. & Pulkkinen, U. Dependent failures of diesel generators. Nuclear Safety, 23(1982), No. 1, pp 32-40.

3.4 Pulkkinen, U., Huovinen, T., Mankamo, T., Norros, L. & Vanhala, J. Reliability of diesel generators in the Finnish and Swedish nuclear power plants. Technical Research Centre of Finland. Research Notes 1070. NKA/RAS-450F(89)5. October 1989.

3.5 Lehtinen, E., Mankamo, T. & Pulkkinen, U. Optimum test interval of closing valves. Nucl. Eng. and Design 81(1984) pp 99-104.

3.6 Ginzburg, T. & Powers, J.T. Frantic III - A computer code for time-dependent reliability analysis. BNL, U.S.A. August 1989.

3.7 Vaurio, J. K. Unavailability of redundant systems with common mode and undetected failures. Nucl. Eng. and Design 58(1980)415-424.

3.8 Karlsson, C. & Knochenhauer, M. Mapping of the influence of periodical testing and preventive maintenance on the auxiliary feedwater system in Forsmark 1 and 2 (in Swedish), Report NKA/RAS-450 S(87)5, ABB Atom RPC87-45, June 1986.

3.9 Knochenhauer, M. Verification of system reliability by analysis of failure data and testing. PSA'89 International topical meeting on probability, reliability and safety assessment, Pittsburgh, April 2-7, 1989.

3.10 Eriksen, L. & Knochenhauer, M. Impact of differences testing conditions and anticipated real conditions on reliability data for motor operated valves. ABB Atom RPC 88-44. Report NKA/RAS-450S(88)2. June 1988.

3.11 Laakso K. A Systematic Feedback of Plant Disturbance Experience in Nuclear Power Plants. (In Swedish, summary in English). Helsinki University of Technology. 1984.

3.12 Pulkkinen, U. & Rämö, J. Availability of feedwater pumps and redundant pump systems. Presented in SRE Symposium '84. October 16-17 1984. Växjö, Sweden.

3.13 Knochenhauer, M. Pilot project on valve data analysis. ABB Atom Report RPC 88-59, NKA/RAS-450S(88)3. June 1988.

3.14 Knochenhauer, M. & Tuvesson, L. Development of a time-dependent failure model for motor operated valves based on analysis of failure data and testing. ABB Atom Report RPC 89-69, NKA/RAS-450S(89)3. September 1989.

3.15 Kosonen, M., Piirto, A., Vanhala, J. Mankamo, T. & Pulkkinen, U. Experiences of the use of PSA methods at the TVO power plant. Teollisuuden Voima Oy, NKA/RAS-450F(86)6. June 1986.

3.16 NUREG/CR-4810, Evaluation of diesel unavailability and risk effective surveillance test intervals. Prepared by Vesely, W.E., DeMoss, G.M., Lofgren, E. V., Ginzburg, T., Samantha, P. & Boccio, J. BNL, May 1987.

3.17 Samantha, P., Ginzburg, T. & Vesely, W. Consideration of test strategy in defining surveillance test intervals. NUREG/CR-5267, BNL/SAIC October 1987.

3.18 Hultqvist, G. Influence of human interface in test arrangements. SV Report PK-16/87, NKA/RAS-450. February 1987.

3.19 Pyy, P. & Saarenpää, T. A method for identification of human - originated test and maintenance failures. IEEE 4th conference on human factors and power plants. Monterey, California. NKA/RAS-450F(88)2. June 1988.

4. REPAIRS AND MAINTENANCE

During the unavailability time due to repairs or preventive maintenance, the risk level is increased, especially when the plant is in power operation state. In order to control the risk, the time allowed to continue operation in such a state is usually limited. For this purpose, the rules for Allowed Outage Times (AOT) have been established. The TS rules covering AOTs are included in the Limiting Conditions for Operation (LCO), and they principally differ depending on whether the event concerned is:

- random failure occurence
- possible CCF event
- repair need of a functionally non-critical fault or
- intentional isolation of equipment for preventive maintenance (PM).

The AOTs depend especially on the system's design criteria, degree of redundancy and safety importance. One of the determining factors in AOT criteria is fullfillment of the single failure criterion. It should be noted that the term AOT is associated to allowed unavailability periods of a component or a system part, when the plant is operated in different states, e.g. power operation.

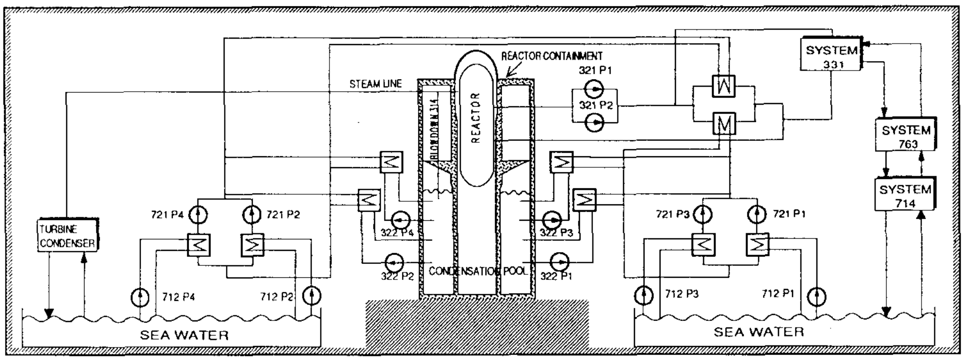
4.1 Introduction to TVO/RHRS case

The TVO I/II plant has two identical ABB Atom BWR units and is operated by Teollisuuden Voima Oy (TVO). The units are located in Olkiluoto, Finland. The AOT rules are illustrated here in a case of four redundant residual heat removal (RHR) systems 721/712, Fig. 4.1 [4.1]. This case will be used throughout this chapter as a practical example. The current rules, which are representative for other new Nordic BWRs as well, state that:

- with one out of four subsystems inoperable, power operation may continue 30 days without restrictions

- with two out of four subsystems inoperable, power operation may continue 3 days without restrictions

- with three or four subsystems inoperable, cold shutdown has to be reached within 24 hours.



Systems

314	=	Steam relief system
316	=	Condensation pool
321	=	Shutdown cooling system
322	=	Containment vessel spray system
331	=	Reactor water clean-up system
712	=	Shutdown service water system
714	=	Normal operation service water system (non-diesel backed)
721	=	Shutdown secondary cooling system
763	=	Heating system

RHR paths

321-721-712	=	Normal shutdown cooling path
(314-316-)322-721-712	=	Pool cooling path
321-331-763-714	=	Water clean-up path (back-up route)

Figure 4.1 Residual heat removal (RHR) systems of the TVO I/II units [4.1].

During the AOTs (single and double failure cases), the power operation is allowed to be continued, but if the repair is impossible, or the AOT is or will be exceeded, the operational conditions have to be changed to a safer state. In the 721/712 system failure cases (as in most other cases) this rule requires cold shutdown of the reactor.

The 30 days' AOT is also applied in the case of isolation of equipment for repair of a random noncritical fault (concerns one subsystem at a time). It should be noted, that according to operating experience, the mean repair times for both critical and noncritical faults are less than one day in these systems at TVO.

Preventive maintenance (PM) is allowed to be performed during power operation within an annual total unavailability time of three days per subsystem [4.2].

4.2 Outline of probabilistic approach

4.2.1 Basic operational alternatives in a failure situation

If a failure or a combination of failures is detected in safety systems during plant operation, the risk level known by the operator is increased above the baseline as illustrated schematically in Fig. 4.2. The operator faces alternative paths to proceed (compare also to Fig. 4.3). The main decision to be made is, whether to:

1) continue plant operation over the repair time of the fault, or to

2) shut down the plant, or proceed to some other operational state where the faulted component's inoperability has a smaller influence.

As illustrated in Fig. 4.2 (curves 2a and 2b), the change of the operational state usually involves a risk peak arising from the:

- unreliability of the systems which are needed during the plant state change or, which must be started up (for example shutdown cooling systems)
- vulnerability to plant transients initiated by the operational change itself (for example, spurious isolation of main heat transfer system, loss of external grid etc.)

In Fig. 4.2, curve 1 represents the case of continued power operation over the repair time. The risk increase associated with this alternative is the area below curve 1 and above the baseline.

The operational state change is principally justified only if the resulting expected total risk then becomes smaller than the risk of continued power operation over the expected repair time. For faults having short repair times, the change of the plant state is not justified.

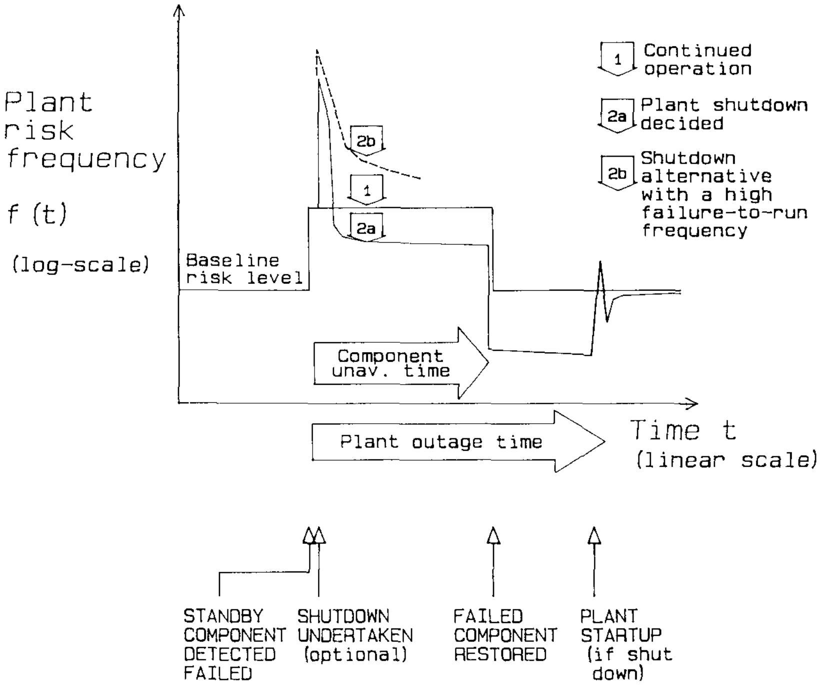

Plant risk frequency
f (t)
(log-scale)
Baseline risk level
1 Continued operation
2a Plant shutdown decided
2b Shutdown alternative with a high failure-to-run frequency
2b
1
2a
Component unav. time
Plant outage time
Time t (linear scale)
STANDBY COMPONENT DETECTED FAILED
SHUTDOWN UNDERTAKEN (optional)
FAILED COMPONENT RESTORED
PLANT STARTUP (if shut down)

Figure 4.2 Risk frequency in failure situation, conditioned by the operational decision of plant shutdown versus continued operation [4.3].

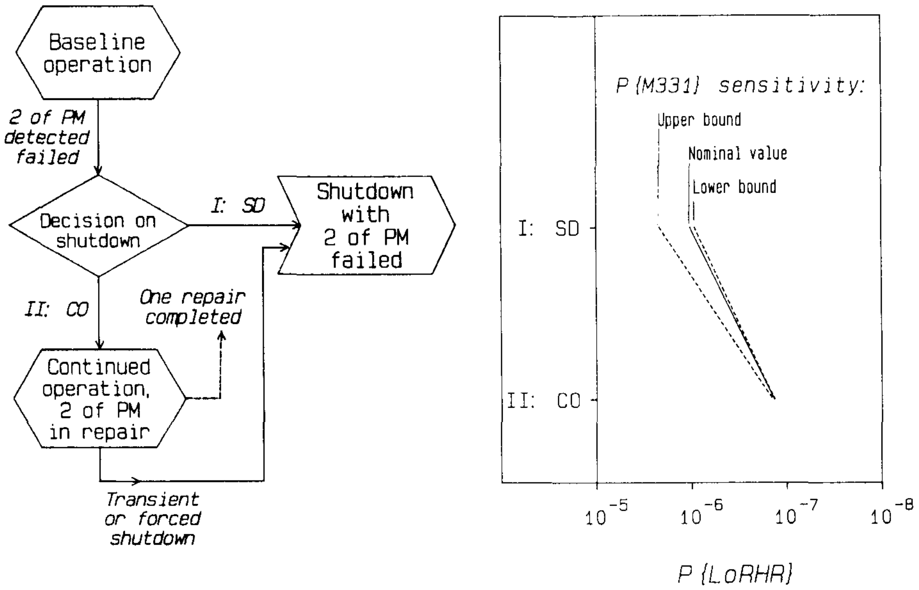


Figure 4.3 Decision example in the situation of two lines of system 712 (PM) detected failed. The expected RHR loss risks (P(LoRHR)) of the principal alternatives are presented on the right hand side. A sensitivity analysis is made with respect to the non-successful capacity increase of system 331 back-up RHR path (the basic event probability is varied by a factor of 10 around the nominal values) [4.1].

In the case of shutdown, the frequency of residual heat removal (RHR) loss often decreases after the state change peak (curve 2a in Fig. 4.2), as the decay heat power decreases. The decay heat decrease leads to lower capacity requirements on safety systems and longer available time for restoration in the case a critical safety function is lost.

Achieving a lower risk level after plant shutdown, as compared to the alternative of continued power operation, is the necessary precondition to justify a decision to shut down. In some cases a lower relative risk level may not be achievable. For example, if a part of the residual heat removal systems is inoperable, the probability that the operable part fails to run during the shutdown outage may be so high, that the situation of curve 2b in Fig. 4.2 exists after shutdown. The extreme example is the situation where the residual heat removal systems are detected totally unavailable, in which case it is trivial to conclude that continued power operation with minimized disturbances is the safest state, at least until some minimum residual heat removal capacity is restored.

4.2.2 Further alternatives of risk control

In addition to the principal decision of continued power operation versus plant shutdown, the operator has opportunities such as:

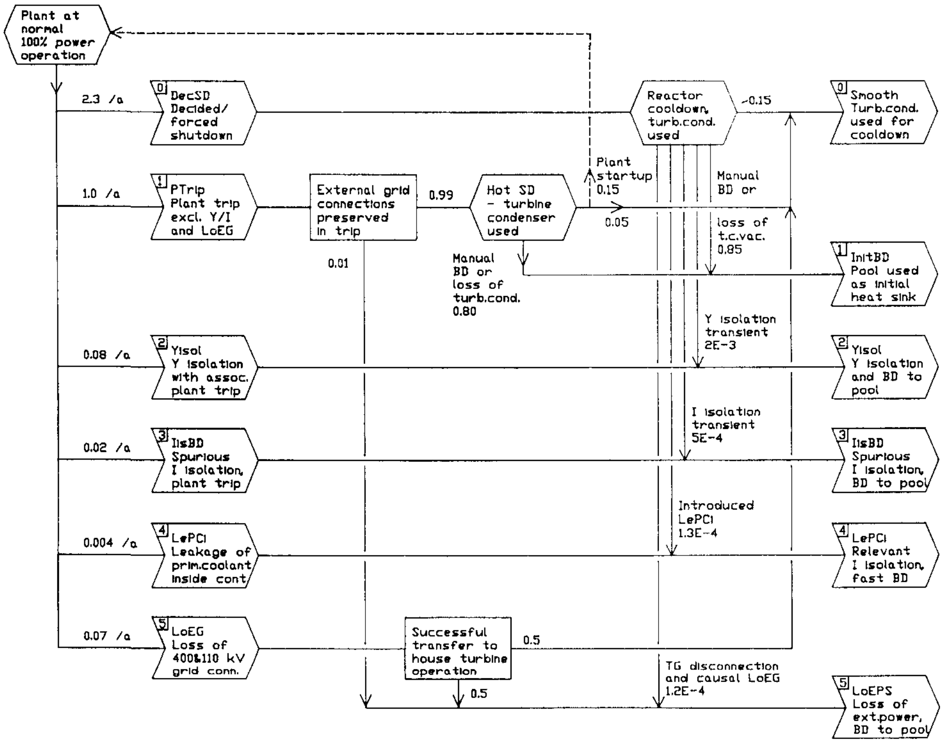
- checking or testing the operability of the redundant equipment to the failed one, prior to deciding upon further actions [4.4]
- arranging additional backup: for example, if diesel generators are failed, the starting readiness of a nearby gas turbine or another power plant could be increased
- calling upon personnel reinforcements.

Most of these opportunities for measures can be used to increase the safety of both the continued power operation and the shutdown alternative.

All in all, the treatment of the AOT issue is much concerned with the analysis of decision alternatives, and the comparison of their safety impact, as well as with parallel consideration of operational and economic aspects.

4.2.3 Models and data base needs

Risk comparison of operational alternatives as described above, necessitates the use of advanced modeling of event sequences (see shutdown transients in Fig. 4.4 for an example), phased missions and restoration options, with the associated need to obtain relevant data [4.5]. As these needs go beyond usual PSAs, the rightmost path in the resolution flow diagram applies, Fig. 4.5. However, an existing PSA greatly helps, as it provides a model and a data frame to build upon.



Plant functions

SD = Plant shutdown
BD = Blowdown (steam relief from the primary system to the condensation pool)
SC = Shutdown cooling (synonym to RHR)

Figure 4.4 Shutdown event sequence diagram describing the principal paths from the normal power operation state to different types of RHR initiation states [4.1].

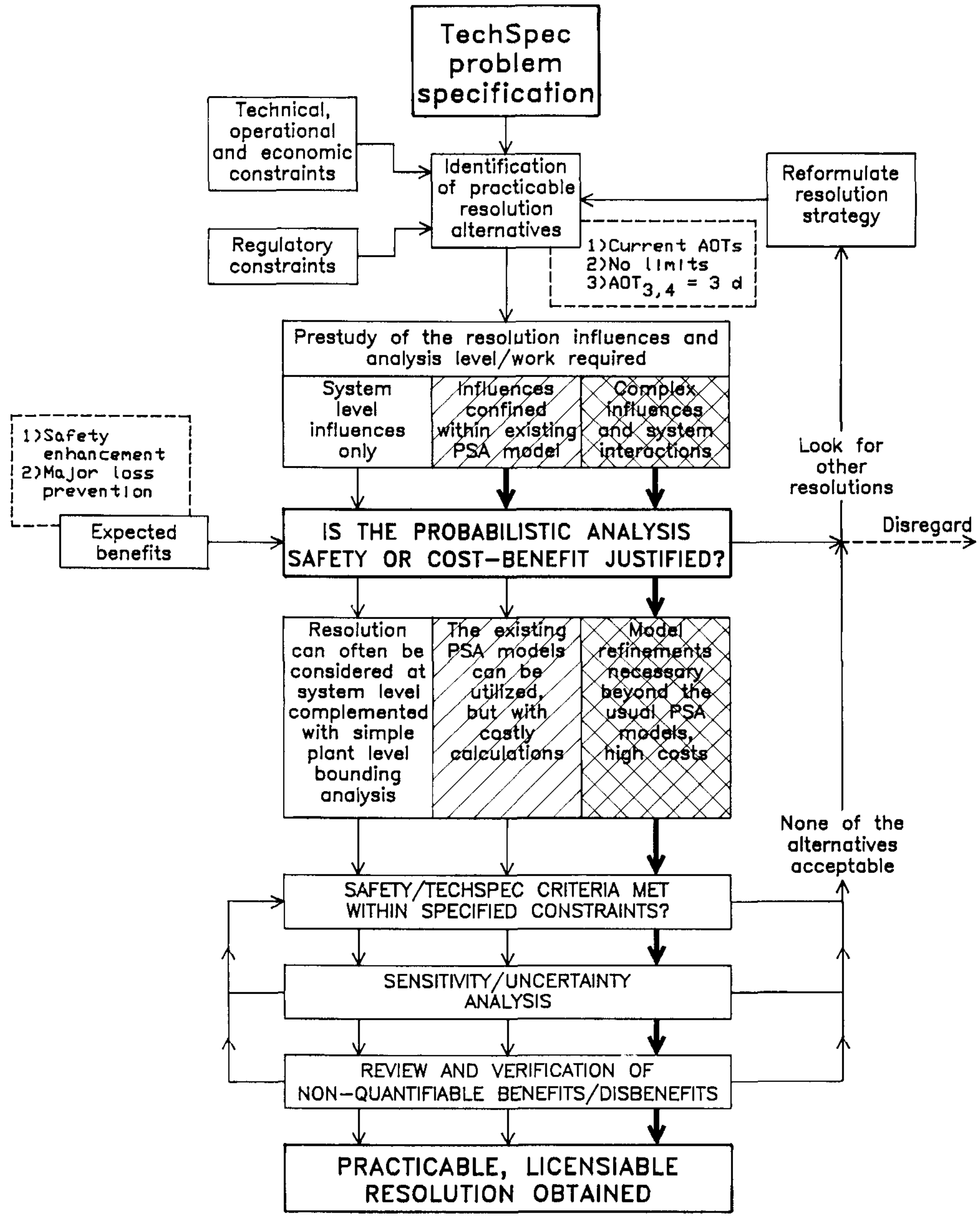

TechSpec problem specification
Technical, operational and economic constraints
Regulatory constraints
Identification of practicable resolution alternatives
1)Current AOTs
2)No limits
3)AOT$_{3,4}$ = 3 d
Reformulate resolution strategy
Prestudy of the resolution influences and analysis level/work required
System level influences only
Influences confined within existing PSA model
Complex influences and system interactions
1)Safety enhancement
2)Major loss prevention
Expected benefits
IS THE PROBABILISTIC ANALYSIS SAFETY OR COST-BENEFIT JUSTIFIED?
Look for other resolutions
Disregard
Resolution can often be considered at system level complemented with simple plant level bounding analysis
The existing PSA models can be utilized, but with costly calculations
Model refinements necessary beyond the usual PSA models, high costs
None of the alternatives acceptable
SAFETY/TECHSPEC CRITERIA MET WITHIN SPECIFIED CONSTRAINTS?
SENSITIVITY/UNCERTAINTY ANALYSIS
REVIEW AND VERIFICATION OF NON-QUANTIFIABLE BENEFITS/DISBENEFITS
PRACTICABLE, LICENSIABLE RESOLUTION OBTAINED

Figure 4.5 TS problem resolution strategy in the analysis of an Allowed Outage Time issue in the TVO/RHRS case [4.7].

Improvements in failure reporting and data bases is a necessary precondition for the further development and verification of the models. For the time being, a substantial part of the data must be assessed by engineering judgement with little or indirect empirical evidence available. Although in many cases the uncertainties can be handled by sensitivity analyses, such as shown in Fig. 4.3 and later in Fig. 4.7, it would be highly preferrable to obtain a firmer empirical data base. Examples of experience data especially desired are:

- conditional probabilities of plant transients in case of changes of the operational state (collection and analysis of transient data is developed in [4.6])
- restoration times, and associated probability distributions, of failed equipment and functions in transient situations; here the operator-system interactions also play a primary role.

4.2.4 Level of consideration

This issue was discussed generally in section 2.2. The complex operational interactions need to be considered especially in the decided shutdown alternative (compare to the DecSD branch in Fig. 4.4). The influences of the repair arrangements of critical faults can usually be considered at the plant level only.

The influences of preventive maintenance may be considered at system level. Relatively simple calculations of plant level influences can be performed by use of PSA information (mainly importance measures) - with the precondition that the subsystems that are simultaneously disconnected, are functionally in series. The risk importance measures cannot be directly used, if functionally redundant subsystems are simultaneously disconnected. The existing PSA models can still be utilized with proper modifications [4.8]. More extensive model completions are needed, if the preventive maintenance presupposes a functional rearrangement of systems, and especially if the rearrangements involve significant risk to human errors. Even in these more complex cases, the PSA models can usually be utilized to a large extent.

4.3 Risk variables and concepts

The basic concepts are defined here in order to serve the discussion of risk based AOT criteria, and the presentation of the practical case study of TVO/RHRS. The mathematical details are presented in more detail in [4.3].

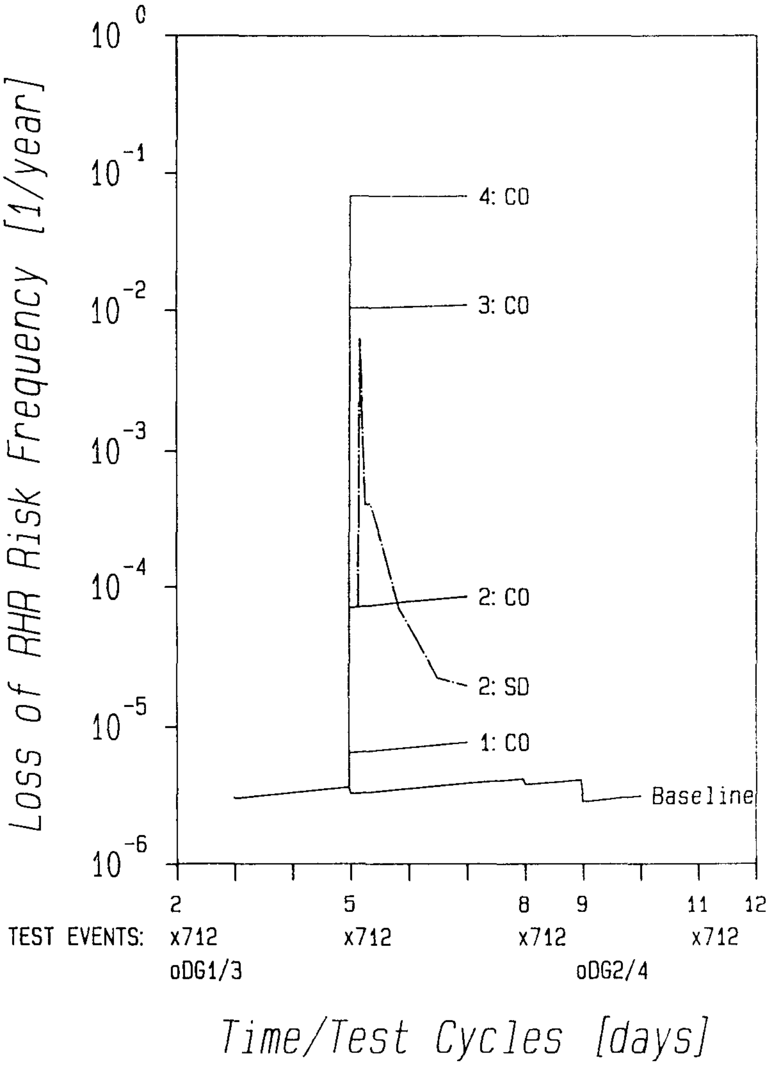
4.3.1 Risk frequency

The risk frequency is the basic concept. It is associated with the probability of the reactor core damage (a plant level risk variable), or loss of some important safety function (function or system level variable) per unit of time. The risk frequency is thus strongly coupled to the level of consideration. In the TVO/RHRS case the risk frequency is associated with the loss of the residual heat removal function (LoRHR):

f_{LoRHR} = Expected number of LoRHR events per unit of time

The risk frequency is usually given in units [1/year]. In the context of PSAs, the averaged risk over various component and system states is derived. In the context of LCO analysis, the actual dependence on time, component and system states, and operational scenarios are of interest, i.e. we are concerned with the "instantaneous" risk frequency. This concept and its meaning was schematically illustrated in Fig. 4.2, while Fig. 4.6 shows how f_{LoRHR} behaves in the various failure states of the TVO/RHR system 712 [4.1].

In some standards on terminology, the entity of risk frequency type is named "intensity". The term frequency is preferred here as it is in practice more commonly used for describing the likelihood of events when expressed per unit of time.



Syntax of N:XX and abbreviations:

N:	= Number of failed subs
XX	= CO = Continued operation of the plant
SD	= Decided shutdown of the plant
RHR	= Residual heat removal
x712	= Shutdown service water system
oDG1/3	= Diesel generators

Figure 4.6 Expected frequency of loss of RHR in different failure states of system 712 lines in the TVO/RHRS case [4.1].

4.3.2 Baseline risk

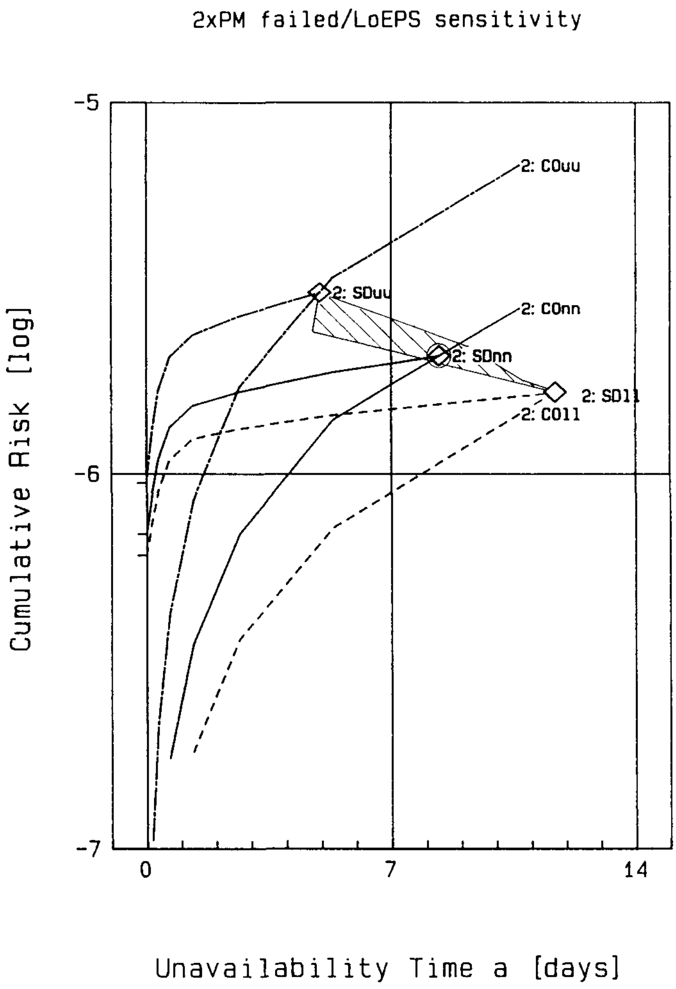
The baseline risk (compare to Fig. 4.2 and 4.6) will be used in the continuation to refer to the nominal risk level in case the safety systems are in their nominal state. Usually the nominal state is standby without any components known to be inoperable. Isolations for testing or maintenance, and detection of critical faults in surveillance testing etc., are deviations from the baseline state. The long term risk is composed of the integrated baseline risk plus the expected value of the increments due to all kinds of such deviations.

4.3.3 Cumulative risk over predicted repair time

Integrating the risk frequency over a given time yields the cumulative risk during this period. The cumulative risk over, and as the function of, the predicted (or actual) repair time a is derived as:

$$c_{ALT}(a|X) = \int_{t=t_0}^{t_0+a} f_{LoRHR|ALT}(t|X(t_0))\cdot dt,$$

where ALT stands for the operational alternative, and X for the failure situation considered, detected at the time instant t_0. This is illustrated in Fig. 4.7 for the TVO/RHRS case for X = double failures (and ALT = CO for the continued power operation and ALT = SD for decided shutdown respectively).



<u>Sensitivity analysis range of the external power supply reliability</u>

Two parameters are varied: Frequency of loss of external power grid during power operation, and probability of loss of external grid in a shutdown transient.

uu = 3 x nominal values	CO = continued power operation
nn = nominal values	SD = shutdown
ll = 1/3 x nominal values	2: = double failure state

Figure 4.7 Cumulative risk of the continued operation versus plant shutdown as the function of predicted repair time in a one-time case of failures in two system 712 lines [4.1].

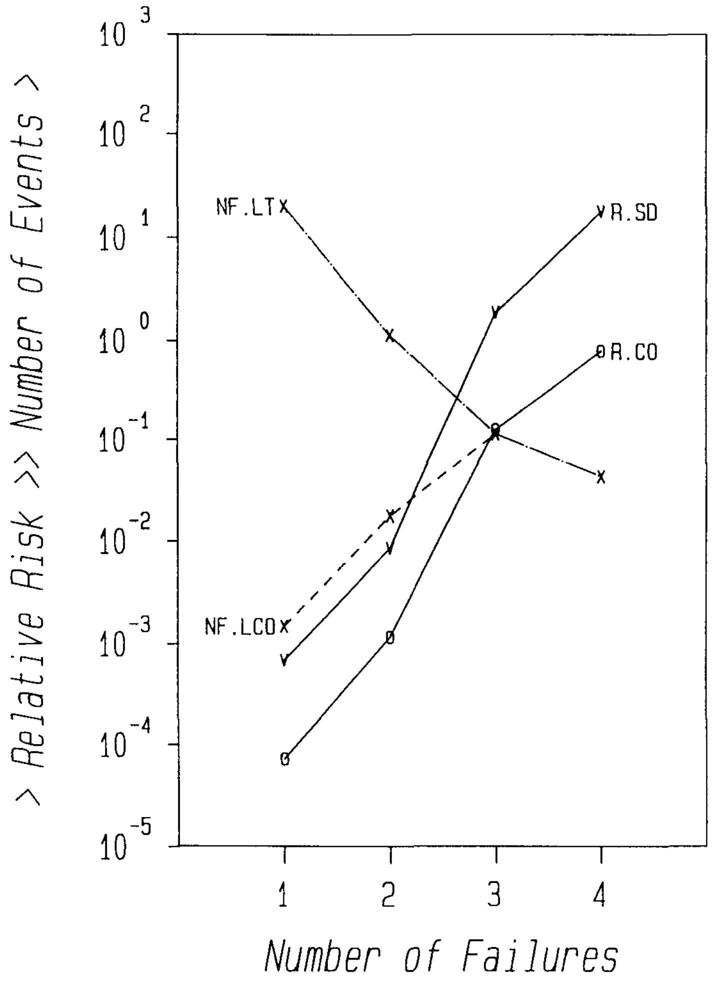
4.3.4 Expected risk over failure situation

Next, the expected risk over the failure situation X, for an operational alternative ALT, is the integral of the risk frequency:

$$R_{ALT}(X) = \int_{t=t_0}^{\infty} \bar{F}_X(t-t_0) \cdot f_{LoRHR|ALT}(t|X(t_0)) \cdot dt,$$

where $\bar{F}_X(a)$ is the complement $1-F_X(a)$ of the repair time distribution $F_X(a)$ for the failure state X. Here the risk frequency is the expected frequency of loss of residual heat removal function (f_{LoRHR}). As compared to the cumulative risk $C_{ALT}(a|X)$ over a given repair time a, the expected risk is the statistical average over the stochastically distributed repair time. This expected risk is thus the mean risk per one repair.

For the TVO/RHRS case, the expected risks per failure event are illustrated in Fig. 4.8. They are calculated from the risk frequencies of Fig. 4.6 using the repair time distributions derived from operating experience. The results are presented relative to the risk accumulating in the baseline state over the plant lifetime (40 years). In this way the results are easier to present and interpret and become less sensitive to a part of the input data.



Syntax of curve labels

NF.LT = Expected number of single or multiple failure situations during plant lifetime

NF.LCO = Expected number of LCO shutdowns during plant lifetime, with current AOT rules

R.CO = Increase in LoRHR risk due to one failure situation assuming continued plant operation, normalized by the baseline risk over plant lifetime

R.SD = Increase in LoRHR risk due to one failure situation assuming plant shutdown, normalized by the baseline risk over plant lifetime

Figure 4.8 Expected risk of loss of RHR over repair times of failures with different multiplicity in system 712 lines [4.1].

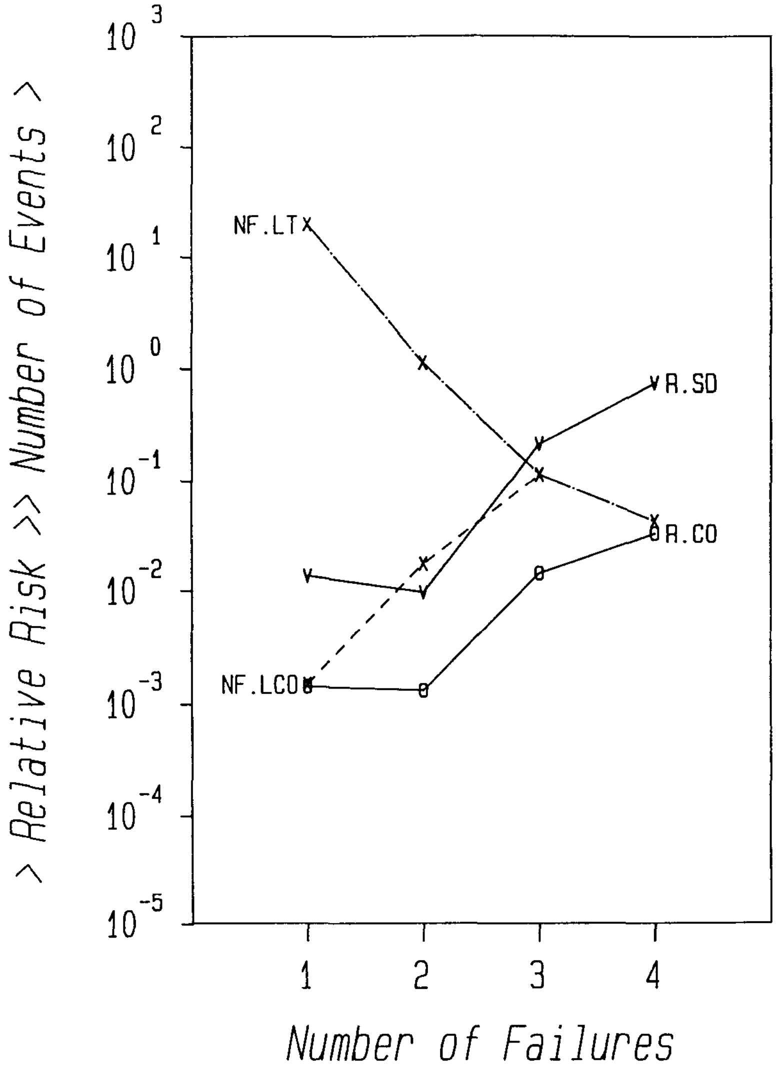
4.3.5 Addition in lifetime risk

The expected number of system failure situations NF_X (compare to Fig. 4.8) is also more meaningful to be presented in the perspective of the whole lifetime, as the likelihood of multiple failures per test cycle, and even per year, is small.

The expected contribution of different system failure situations to the lifetime risk is obtained as the product

$$dR_{ALT}(X) = NF_X \cdot R_{ALT}(X).$$

For the TVO/RHRS case these variables are presented in Fig. 4.9, again normalized and compared to the lifetime baseline risk.



Syntax of curve labels

R.CO = Risk increase in LoRHR due to expected failure situations assuming continued plant operation, normalized by the baseline risk over plant lifetime

R.SD = Risk increase in LoRHR due to expected failure situations assuming plant shutdown, normalized by the baseline risk over plant lifetime

Figure 4.9 Lifetime risk increases in LoRHR from repair times of failures with different multiplicity in system 712 lines [4.1].

4.3.6 Risk due to isolations for preventive maintenance

The intentional, planned isolation of a subsystem for regular PM differs from critical failure states due to the lack of randomness in the nature of occurrence and of unavailability time. The risk frequency during a PM isolation corresponds to a single independent failure state. The expected risk over the PM period is simply the product of the risk frequency increase and PM time (usually constant). The addition in lifetime risk (or in annual risk) is obtained again through multiplying one-time risk by the number of PM isolations during the plant lifetime. Usually, the PM influence is described by the increase of the average total risk frequency, in units [1/year] as calculated in PSAs.

4.4 Criteria for repairs during plant operation

4.4.1 Three variable approach

The safety influence of failures in standby safety systems can be considered from the point of view of:

1) Instantaneous risk frequency
2) Expected risk over failure situation
3) Contribution to the total risk over plant lifetime.

In the TVO/RHR case the three entities are presented in the Figs. 4.6, 4.8 and 4.9 respectively. The last alternative is equivalent to considering the contribution of the failure situations to the total averaged risk, usually expressed in units [1/year].

The three entities listed above present each a specific aspect of safety influence. Hence, they all need to be considered when criteria for repairs and action statements are defined. The approach presented here is rather similar to recent criteria developments in the U.S.A [4.9-10].

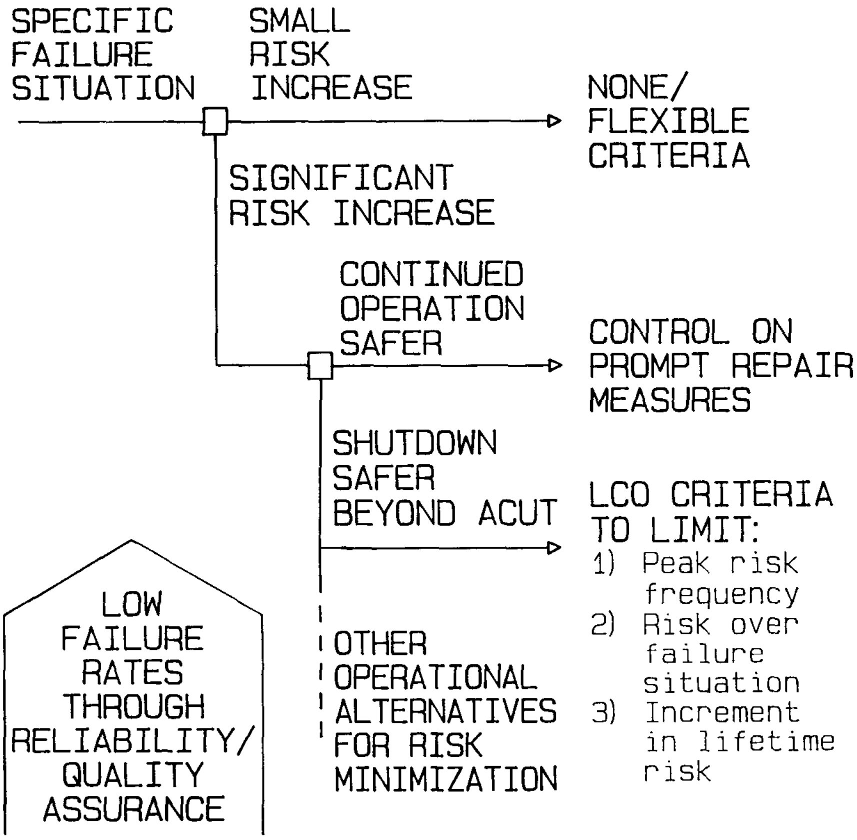

SPECIFIC FAILURE SITUATION
SMALL RISK INCREASE
NONE/ FLEXIBLE CRITERIA
SIGNIFICANT RISK INCREASE
CONTINUED OPERATION SAFER
CONTROL ON PROMPT REPAIR MEASURES
SHUTDOWN SAFER BEYOND ACUT
LCO CRITERIA TO LIMIT:
1) Peak risk frequency
2) Risk over failure situation
3) Increment in lifetime risk
LOW FAILURE RATES THROUGH RELIABILITY/ QUALITY ASSURANCE
OTHER OPERATIONAL ALTERNATIVES FOR RISK MINIMIZATION

Figure 4.10 Decision tree presentation for the proposed criteria on allowed outage time (AOT) during power operation in the case of critical failures detected in safety systems.

The criteria approach is structured by a decision tree in Fig. 4.10. Naturally, if the failure situation influences the safety negligibly, no or only flexible restrictions are justified. In practice, this could mean that in less important system parts, repairs and maintenance could be undertaken relatively freely - but still in a controlled way. The single failure situations in the TVO/RHR systems 712/721 can be considered to be of this type.

Next, if the failure situation implies a significant increase in the risk level, it is necessary to consider whether there are some other, safer plant states (or other safety-significant arrangements). If continued plant operation is shown to be the safest state, then emphasis should be on prompt repair measures in parallel to avoiding disturbances in plant operation.

The third principal type of failure situation means a significant risk increase and that a safer plant state is available. Usually this situation is connected with relatively long repair time needs so that the additional risk of the plant state change is expected to become compensated. The appropriateness of the state change needs to be assessed from the point of view of the three variables specified above:

- The instantaneous risk frequency is usually less determining.
- In highly critical failure situations, such as failures in three of four subsystems in the TVO/RHR case, the expected risk over the repair time is usually most determining. In these rather unlikely situations - given they occur - it is of primary importance to choose the operational alternative of the minimum risk.
- For frequent failure situations, which usually do not contribute significantly as single events, the contribution in the long term becomes determining. This variable also takes the frequency of the failures into account. In the TVO/RHR case, the single and double failures can be considered to be of this frequent type.

When deciding upon the acceptable AOT length, the cumulative risk as a function of repair time (compare to Fig. 4.7) needs to be considered in parallel with the expected risks following from "average" repairs. Also maintainability aspects and other practical factors shall be considered.

4.4.2 Budget criteria

The AOT criteria could be specified also with respect to cumulative unavailability time over some operating period - usually over a moving year - instead of single events. The main advantage of the risk budget criteria is, that they include also control of failure frequency. They also allow more operational flexibility, especially because repairs and preventive maintenance (PM) could be handled in principle on an equal basis. But looking more deeply into the practical implementation, severe disadvantages are identified [4.11, section 5.3.3]. These become pronounced in the case of infrequent, highly critical failure situations. Such an event, given it occurs, would exhaust the AOT budget for several years. Shutting down the plant for a long time afterwards is, however, unlogical if the affected systems are repaired promptly in a reasonably short time, which is the most likely outcome, meaning that the actual risk was successfully passed. Due to these inherent problems, the budget criteria have been applied almost exclusively on PM periods and on planned repairs of noncritical faults, but seldom on random critical failure situations.

4.4.3 Relationships to test arrangements

Especially in many TS cases handled in the U.S.A, trade-off between AOT and surveillance test intervals (STI) has been recommended. It has been treated mainly in such a way that by shortening of STI in some system, the AOT could be increased [4.12]. This treatment can be criticized, as the influence of shortening of STI appears to be overestimated, and because only one risk entity, the contribution to the total average risk is taken into consideration [4.11, section 5.3.4]. This kind of trade-off, applicable in principle also more broadly among other kinds of safety improvement measures, should be used with a great care, because all contributing factors shall be taken into account realistically.

4.5 Criteria for preventive maintenance during operation

4.5.1 Acceptable risk increment

In the newest Nordic BWR plants with four redundant safety systems, PM during power operation is currently allowed in one subsystem at a time with a budget criterion. The calculated annual average risk increase is a few percent [4.2, 4.8]. The temporary risk increase has been minimized by grouping PM into functionally linked subsystems, and by excluding simultaneous isolation of subsystems in redundant safety systems. The small contribution is partly explained by the fact that, in the 4 x 50 % or 4 x 100 % subsystems the isolation of one subsystem affects little, and the CCFs dominate the failure probability, Fig. 4.11.

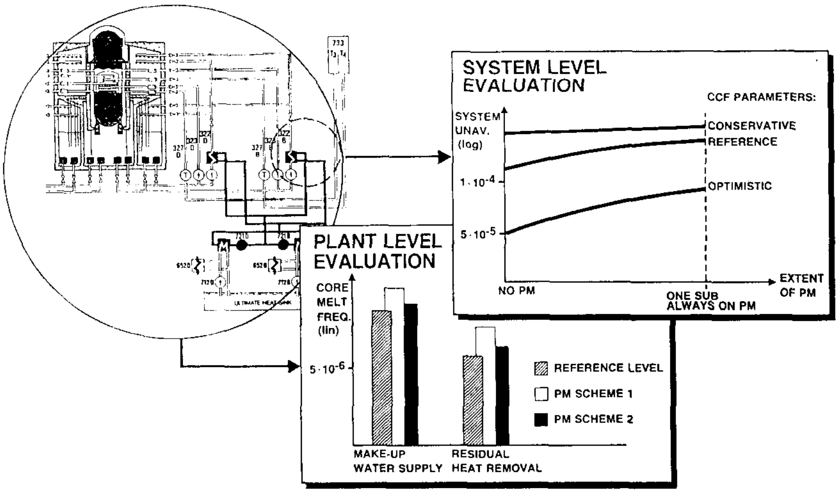


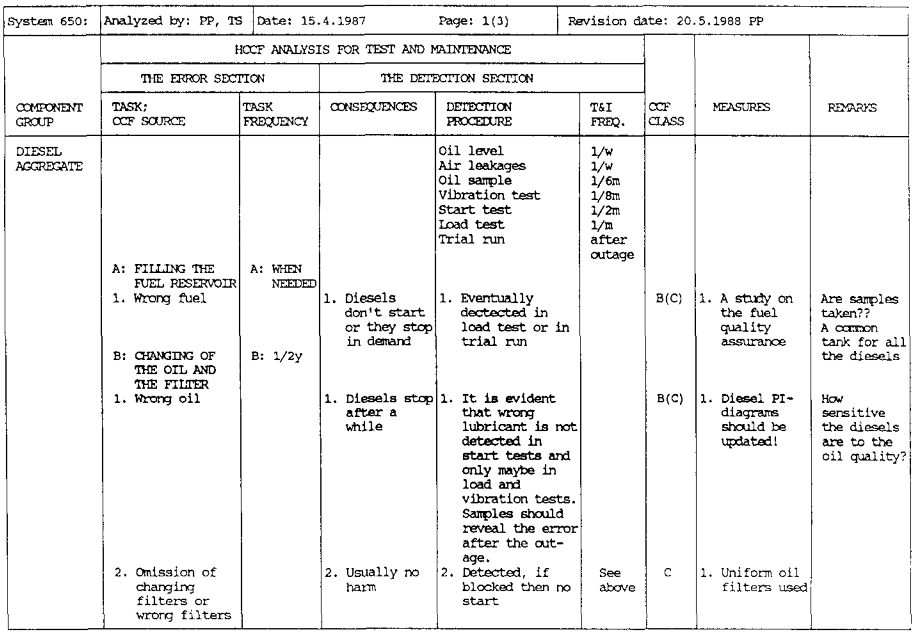
Figure 4.11 Analyses at system level and plant level of preventive maintenance during power operation at Forsmark 2.

4.5.2 Qualitative benefits

Performing PM during the operation period has many advantages compared to the refuelling outage which is loaded with a large number of tasks and a tight time schedule. During the operation period, PM work can be done more carefully, in a more orderly planned and supervised manner, and with less time schedule stress. It is possible to use the company's own maintenance personnel having special training. Quality assurance of the work can also be more effectively performed, and experts from the suppliers can be more easily engaged when needed. With one subsystem affected at a time, it is easier to control possible TS violations.

These many qualitative benefits are not readily expressed in quantitative terms, but by improving the equipment reliability they can counterbalance, at least partially, the few percent's unavailability contribution from the PM periods. (It should be noted, that in safety systems with four redundant subsystems, the designed excess margin to the single failure criterion also makes it possible to justify the power operation during a limited time with one subsystem unvailable for PM.) An important reservation must be made on the risk of systematic maintenance errors. Although their likelihood should be smaller when PM is performed during power operation in a more orderly way, the benefit of the efficient plant startup tests will be absent. Especially the risk of simultaneously disconnection of several subsystems is a potential problem [4.13], and not so readily detected during the power operation state (as compared to the startup tests following the refuelling outage). This observation has also contributed to an interest in developing new methods for configuration control of safety systems in the U.S.A. [4.14].

By careful planning, the risk of systematic PM errors can also be reduced. Recently, CCF analysis methods towards this aim are developed, an example of a qualitative analysis is shown in Fig. 4.12 [4.15].



System 650:	Analyzed by: PP, TS	Date: 15.4.1987		Page: 1(3)	Revision date: 20.5.1988 PP			
	HCCF ANALYSIS FOR TEST AND MAINTENANCE							
	THE ERROR SECTION		THE DETECTION SECTION					
COMPONENT GROUP	TASK; CCF SOURCE	TASK FREQUENCY	CONSEQUENCES	DETECTION PROCEDURE	T&I FREQ.	CCF CLASS	MEASURES	REMARKS
DIESEL AGGREGATE				Oil level Air leakages Oil sample Vibration test Start test Load test Trial run	1/w 1/w 1/6m 1/8m 1/2m 1/m after outage			
	A: FILLING THE FUEL RESERVOIR 1. Wrong fuel	A: WHEN NEEDED	1. Diesels don't start or they stop in demand	1. Eventually dectected in load test or in trial run		B(C)	1. A study on the fuel quality assurance	Are samples taken?? A common tank for all the diesels
	B: CHANGING OF THE OIL AND THE FILTER 1. Wrong oil	B: 1/2y	1. Diesels stop after a while	1. It is evident that wrong lubricant is not detected in start tests and only maybe in load and vibration tests. Samples should reveal the error after the outage.		B(C)	1. Diesel PI-diagrams should be updated!	How sensitive the diesels are to the oil quality?
	2. Omission of changing filters or wrong filters		2. Usually no harm	2. Detected, if blocked then no start	See above	C	1. Uniform oil filters used	

Figure 4.12 Example of a human CCF analysis related to PM of diesel generators [4.15].

4.6 Overall balancing

Usually, the total average risk can be affected relatively little by the optimal choice of AOTs of safety-related equipment, often only in the range of 1...10 % share. However, in the rare cases of multiple failures, an order of magnitude differences may exist between the expected risk over the failure situation, depending on the operational alternative selected.

The total average risk is much more sensitive to the reliability of equipment and operations, i.e. to the frequency of failures and disturbances. These also determine the likelihood of entering into rare multiple failure situations. Hence, we want to strongly emphasize the importance and primary role of the reliability assurance measures in order to limit the number of failure and disturbances - as noted also in Fig. 4.10.

The central AOT issue, i.e. the consideration of repairs allowed during continued power operation versus plant shutdown for repairs, has also significant economic influences because of the high cost of replacement energy. Furthermore, the state changes of the plant will also lead to thermally and dynamically induced stresses that may contribute to damage and leakage in equipment. The systematic setup of AOTs means balancing between different factors influencing safety, operational flexibility and economy. The example case study was concerned with all these factors, but mainly searching for an operational alternative leading to minimum risk from the safety point of view.

REFERENCES

4.1 Kosonen. M., Piirto, A., Saarenpää & Mankamo, T. Continued operation versus shutdown in failure situations of residual heat removal systems - Application of risk analysis methods for the evaluation and balancing of Limiting Conditions of Operation. Teollisuuden Voima Oy, NKA/RAS-450F(88)1. April 1988.

4.2 Heinonen, R. & Piirto, A. Preventive maintenance of safety systems during normal power operation of TVOs nuclear power plant. IAEA International Symposium on Advances in NPP Availability, Maintainability and Operation, Munich, 20-23 May 1985.

4.3 Mankamo, T. Availability analysis of standby safety systems. Basic methodology for the optimization of the test and repair arrangements and limiting conditions of operation. Thesis manuscript, 1986.

4.4 Mankamo, T. Is it beneficial to test/startup the remaining parts of standby safety systems in a failure situation? Proc. ENS/ANS/SNS Int. Meeting on Probabilistic Safety Assessment and Risk Management (PSA 87), Zürich, Aug 31 - Sep 4, 1987, pp. 765-770. NKA/RAS-450F(87)2.

4.5 Mankamo, T. Phased operations and recovery options - advances in event sequence quantification. PSA'89, Pittsburgh, April 2-7, 1989. NKA/RAS-450F(89)4.

4.6 Laakso, K. Systematic Feedback of Plant Disturbance Experience in Nuclear Power Plants. (In Swedish). Helsinki University of Technology, 1984.

4.7 Mankamo, T., Engqvist, A. & Kosonen, M. Resolution Strategy of TS problems, NKA/RAS-450. Draft 12 June 1989.

4.8 Knochenhauer, M. Plant-level probabilistic evaluation of preventive maintenance during power operation in Forsmark 2. ABB Atom Report RPC 87-61, NKA/RAS-450F(87)4. August 1987.

4.9 Mankamo, T. Optimization of Technical Specifications by Use of PRA Methods. Preproject Survey-International Developments. VTT Research Report, NKA/RAS-450F(85)2. August 1985.

4.10 Samantha, P. K., Vesely, W., Lofgren, E. V. & Boccio, J. L. Risk Methodology Guide for AOT and STI Modifications. Technical Report A-3230 12-02-86, BNL & SAIC December 1986.

4.11 NKA/RAS-450(88)4, Project Phase 2 Report, Optimization of technical specifications by use of probabilistic methods - a Nordic perspective. Ed. K. Laakso, Technical Research Centre of Finland, August 1988.

4.12 EPRI NP-5238, Risk-based evaluation of Technical Specification problems at the La Salle County Nuclear Station. Prepared by Bizzak, D. J., Trainer, J. E. & McClymont, A. S., Delian Corporation, June 1987.

4.13 Samantha, P. K. & Kim, I. S. Multiple Train and Component Outages Based on Plant-Specific Data. Preliminary Draft, BNL February 1989.

4.14 Work Plan for Phase I of the Pilot Program for Implementation of a Real Time Risk-based Configuration Control Approach to Technical Specifications. SAIC-88/1813, March 6, 1989.

4.15 Pyy, P., Saarenpää, T. A method for identification of human originated test and maintenance failures. 4th IEEE Conference on Human Factors and Power Plants, Monterey, California. NKA/RAS-450F(88)2. 5 - 9 June, 1988.

5. REQUIREMENTS ON DATA

Much of this chapter is concerned with evaluating the quality and usefulness of existing Nordic data collection systems. It should be stated at first, that in such a process it is quite natural that a major portion of these comments will concern problems encountered. Therefore, the formulation of criticism is not only inevitable but even necessary. Especially as the various data analyses performed have, among other objectives, aimed at coming up with suggestions for improvement of existing data collection systems. However, in this context it should be noted that the Nordic situation with respect to failure data collection is exceptionally good. Internationally, there are few (if any) data collection systems that can match the homogeneity and coverage of the ATV Reliability Data System. In addition the Swedish RO (safety-related occurrence) reporting system exists providing a more detailed description of a number of safety-related occurrences and their causes. These data systems, in turn should be seen as a good starting point for trying to achieve something even better.

The models applied in the evaluation of TS differ from those applied in usual PSAs. Since the optimization of limiting conditions of operation and test arrangements requires time dependent component and system failure models, the parameters of these models should be estimated realistically on the basis of accumulated operating experience. Further, knowledge concerning repair or unavailability time distributions is essential. Other important parameters include the effectiveness of testing and the reliability of components in abnormal operating conditions.

5.1 Specific data needs in optimization of Technical Specifications

In this chapter the data situation will be reviewed, especially in view of the specific data needed for TS analyses. The word "specific" should be understood as extra requirements in additions to what is needed in normal level 1 PSA analyses.

As the project proceeded, it became increasingly obvious that the task could not be limited to the "extra" data needed, but must deal with standard data as well. This was due to several facts:

- standard data are used extensively also in TS related analyses,
- significant problems with the quality of standard data were encountered,
- the task of TS optimization is an integral part of any living PSA approach, and therefore the specific data needs cannot be viewed in separation.

In consequence, although the focus will remain on TS related data, much of the contents of this chapter refers to general rather than to specific needs for data base improvements.

5.1.1 Problem overview

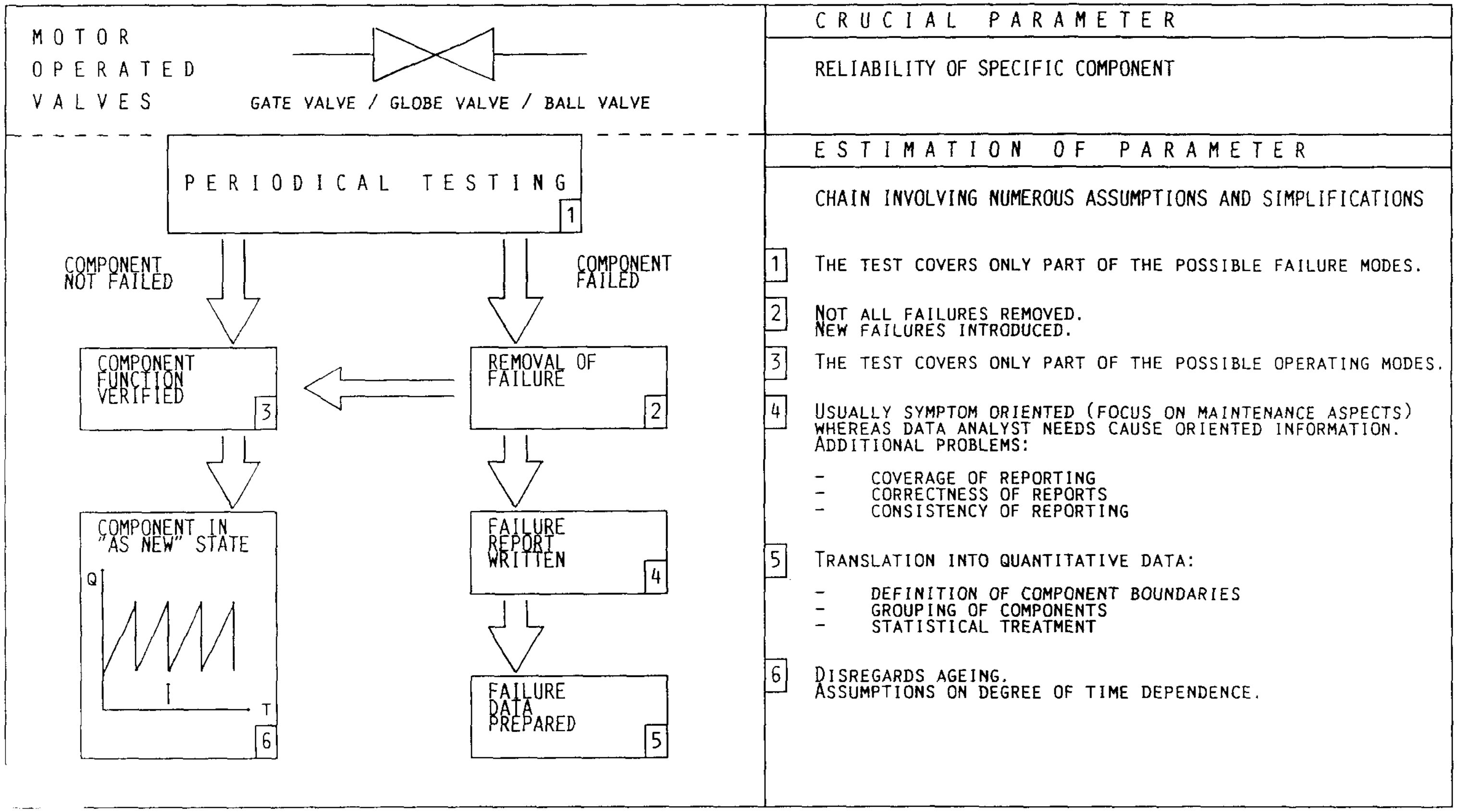
Most of the analyses performed within the NKA/RAS-450 project have highlighted problems involved in preparing and using component failure data of safety systems [5.1].

When modelling a system and quantifying the model, it is a fact - and a problem - that the model and the quantitative input to it will necessarily be based on idealized assumptions. The main link to reality is established by using relevant experience data on component and system failure modes, failure mechanisms, and event frequencies and unavailability times, preferably plant specific data.

However, the interpretation of this experience is almost without exception based on the assumption that periodic testing simulates reality correctly. In spite of the fact that an overwhelming majority of all component failures have not manifested themselves at real demands, but rather at periodic testing or inspection, failures from periodic tests will still be the most important foundation for analyses and conclusions involving component and system reliability in disturbance and accident situations. Within the NKA/RAS-450 project it has therefore been seen as a very important task to investigate the applicability of test-based failure data to real demand situations [5.2].

The component failure data used in e.g. a PSA, are the end product of a long chain of assumptions and simplifications, introduced in the process of data preparation as well as when the data is used. Many of the problems are by no means obvious to the final user of the reliability data. The problems are summarized and illustrated in Fig. 5.1. The most important simplifications are:

- periodic testing is assumed to cover all relevant failure mechanisms of the component, i.e. all latent failures are assumed to be discovered [5.3],
- periodic testing is assumed to cover all relevant operating and failure modes of the component,
- failures discovered in periodic testing are assumed to be efficiently eliminated by corrective actions,
- failures introduced at periodic testing are assumed to be adequately covered by data available
- the failure reporting is assumed to be adequate, i.e. all failures are reported, all reports are correct, and all test occasions are recorded,
- the failure reporting is assumed to be consistent, i.e. inter-plant differences in reporting practices and in coverage of reporting are disregarded,
- the failure reporting is usually symptom and action oriented, i.e. aimed at providing the information required by the maintenance organization, whereas the data analyst would be better helped by reporting focusing on e.g. failure modes, criticality, latency, and CCF occurrence,
- quantitative failure data are usually generic, which decreases statistical data uncertainty, but may introduce major systematic errors when the data is used in certain specific applications,



CRUCIAL PARAMETER

RELIABILITY OF SPECIFIC COMPONENT

ESTIMATION OF PARAMETER

CHAIN INVOLVING NUMEROUS ASSUMPTIONS AND SIMPLIFICATIONS

1 THE TEST COVERS ONLY PART OF THE POSSIBLE FAILURE MODES.

2 NOT ALL FAILURES REMOVED.
NEW FAILURES INTRODUCED.

3 THE TEST COVERS ONLY PART OF THE POSSIBLE OPERATING MODES.

4 USUALLY SYMPTOM ORIENTED (FOCUS ON MAINTENANCE ASPECTS) WHEREAS DATA ANALYST NEEDS CAUSE ORIENTED INFORMATION.
ADDITIONAL PROBLEMS:

- COVERAGE OF REPORTING
- CORRECTNESS OF REPORTS
- CONSISTENCY OF REPORTING

5 TRANSLATION INTO QUANTITATIVE DATA:

- DEFINITION OF COMPONENT BOUNDARIES
- GROUPING OF COMPONENTS
- STATISTICAL TREATMENT

6 DISREGARDS AGEING.
ASSUMPTIONS ON DEGREE OF TIME DEPENDENCE.

Figure 5.1 Approximations involved in estimation of component reliability. Motor operated closing valves are used as an example [5.1].

- in order to achieve reasonable population sizes, components having different designs are often combined into groups, which will sometimes introduce errors,
- various mathematical model assumptions, possibly in contradiction with other assumptions, are applied in statistical treatment.

There is also the general problem of the scarceness of these data. For several reasons this is a problem that can never be completely solved - even with perfect coverage. The demands on data will almost by definition remain higher than what can be supplied from existing experience. There are several reasons for this:

- An existing set of component failure data will seldom be up to date with todays status. This is due partly to the fact that equipment is modified, creating new operating conditions for components, partly to experience feedback resulting in the elimination of the causes of recurring failures. However, failure frequencies are often rather constant, at least when it comes to long-term trends.
- In order to get data of optimal quality, they should be as specific as possible, preferably plant or component specific. However, this will often cause the basis for data assessment to shrink to an extent that may make further quantitative analysis pointless.
- High reliability demands on a component will automatically make it difficult to find failure data of a quality that matches the demands.

It is a common attitude and excuse to attribute vagueness in conclusions, or difficulties in making proper use of developed analysis models, to scarce data. Although the excuse is sometimes relevant, it often indicates a flaw in the analysis as such - if data is scarce, additional measures must be taken to put conclusions in the proper perspective. Such measures might be statistical uncertainty analyses or systematic sensitivity analyses.

In conclusion, it can be stated that, when viewing todays failure data situation, the main problem lies not in the amount of data available, but in the information contents and analysis of these data. In the future more will be gained by caring about the quality of data, which can be improved significantly, than by complaining about the inherent scarceness of available data.

5.1.2 Summary of data requirements in TS analysis

This section will summarize the data needs expressed in the preceeding sections. The data required can be roughly divided into three groups:

A. Standard PSA input data; (usually generic)
A1 Failure rate in operation (λ_o)
A2 Standby failure rate (λ_s)
A3 Failure on demand (time independent) (q)
A4 Active mean time to repair (MTTR) for corrective maintenance
A5 Repair time distributions (including waiting times)

In many data compilations, a mean failure probability on demand value is given instead of λ_s and q. As the total unavailability of standby components is often dominated by time-dependent failures, this simplification may give rise to major discrepancies.

The distinction between A4 and A5 above concerns two aspects of closely related experience data. The choice of which parameter to use is situation specific. For the calculation of the mean system unavailability, A5 should be used. This time is usually considerably longer than the active repair time (A4), which is appropriate to be used in recovery situations of single critical failures.

B. Boundary conditions of testing; (plant specific)
B1 Test and preventive maintenance (PM) intervals
B2 Test and PM durations
B3 Test and PM schemes

These parameters are by definition totally plant specific, and can usually be easily defined.

C. Test quality parameters; (usually generic)

C1 Measure of test or PM effectiveness

C2 Measure of failure introduced at test or PM

C3 Test override unavailability, i.e. probability of a real demand overriding an ongoing test

C4 Hardware degradation due to testing

C5 Measure of probability of test-introduced plant transients.

These extremely crucial data are unfortunately next to impossible to extract from todays failure reporting systems. Some of the problems encountered will be touched upon in the final section. In some cases, they can be extracted from analysis of field data, by comparing the frequencies and spectrums of failures of the same kind of equipment under differing test/PM conditions.

5.1.3 Existing data sources

In Sweden and Finland, there are four main sources of information on component failures and plant disturbances; they will be shortly described below. The first three of them have been used extensively within the project.

ATV Reliability Data System

The ATV system [5.4], a formalized failure reporting system for component failures in Swedish and Finnish nuclear power plants (except Finnish PWRs) has been in existence for more than a decade. Both critical and non-critical component failures are reported on special failure reporting form, including information on failure type, failure manifestation, and corrective actions taken. This information is given both explicitely and in coding.

Based on ATV data, the T-book [5.5], a reliability data handbook for safety-related equipment in Swedish BWRs and PWRs is produced. The T-book is updated at a fairly regular interval of about three to five years. The components covered include mechanical as well as electrical equipment. The next version, which will appear in 1990, will also include the Finnish TVO plants (BWR). The parameters presented include:

- failure rate for running equipment,
- failure per demand for standby equipment,
- active mean time to repair, and
- uncertainty distribution characteristics.

Some of the main problems encountered in the evaluation of ATV data are described in section 5.1.4.

RO/ Safety Related Occurrences

The RO reports (Rapportervärd omständighet, roughly equivalent to Licensee Event Reports, LER, in the USA), are by far the most exhaustive information sources of safety-related failure events, including an analysis of failure causes and corrective actions. They have also been used for some analyses within or in connection with the NKA/RAS-450 project [5.6, 5,7]. A Swedish RO report is prepared and checked subsequently at the plant prior to the reporting to the authority. These reports include information on:

- description of failure event
- TS rules applied
- consequences on component level
- consequences on system and plant level
- failure causes
- corrective actions taken
- cross references to related failures (generic problems).

However, ROs include only a fraction of the failures reported in the ATV system, as ROs handle only function critical safety related occurrences. RO reports will give a thorough picture of some of the reported component failures. Their main use is, therefore, in detailed analysis of failure causes, failure mechanisms, corrective actions, and the connection between test and maintenance quality and system performance. The Swedish RO system is presently being modified and will include more explicite information and less coding than earlier.

Work Order System

A work order system is usually a computerized system for the processing of work orders based on predefined planned testing and maintenance as well as on reporting of failures discovered during plant operation and outages. The work order systems will be plant specific as to lay-out, updating routines, and ways of processing information. They have, however, common tasks, viz.:

- Issuing of work orders based on:
  - . corrective maintenance requirements
  - . planned maintenance requirements
  - . regular testing requirements
  - . TS testing requirements

- Information retrieval on:
  - . fulfillment of TS testing requirements
  - . descriptions of corrective maintenance actions
  - . reporting to ATV reliability data base

In many cases, the work order system will contain valuable additional information that can be used along with the information reported to the ATV system. Problems in analysis can be foreseen due to inter-plant variations in reporting practices and information contents.

ERF/ Plant Disturbance and Scram Reporting

The ERF is a computerized information system covering data on plant disturbances and safety-related occurrences (RO). Reports are prepared by Swedish utilities and by TVO in Finland. The ERF system is operated by KSU, the Training and Safety Center of the Swedish Utilities. This information and communication network includes:

- Daily operating reports from all plants
- Plant operational statistics
- RO reports (described separately above)
- Scram reports
- Swedish incident reports
- International incident reports
- International disturbances.

5.1.4 Conclusions from ATV data analysis

In the data analyses performed, problems have been identified, that have great impact on the interpretation and use of failure reporting, and on the derivation of component failure parameters. Some of the main findings from the pilot project on valve data analysis [5.8] will be summarized below:

A. Detection circumstances
In the T-book it is assumed that all failures are detected at periodic tests. This is a simplification, as a closer analysis of the failure reports indicates that a significant proportion of the failures are discovered at other occasions (local inspections, central alarms, preventive maintenance, etc.)

B. Criticality of failures
There is a lack of consistency when it comes to judging the functional criticality of failures forming the basis for the T-book. In the referred analysis, about 31 % of the failure reports had to be reclassified (from non-critical to critical or v.v.).

C. Revision period contra operating year
The detection or other circumstances during normal plant operation seem to differ considerably from revision. The application of the proposed failure model results in dominant contributions from latent critical failures that are discovered only at tests during revision outages, compared to the contribution from failures discovered during the operating period.

D. Repair critical failures

A subject that has not been touched upon in the T-book, but which may have great impact on the availability of standby safety systems, is the treatment of non-critical failures causing unavailability during repair.

E. Fluctuations within reporting period

It is quite obvious from the analyses performed that two factors must be considered:

- bad coverage at the start of reporting from the plants,
- long delay time in reporting.

For this reason, it seems reasonable to exclude from the reliability analyses the first and latest operating year for each plant.

F. Presentation of results for individual plants

There are great differences among the plants with respect to volume of reporting, and thus also in resulting failure parameters. Although the differences may to some extent be attributed to "real" plant-to-plant variation, they will often be due to differing reporting practices, and degree of coverage. This is seen when comparing reporting from twin plants at the same sites (Barsebäck, Forsmark, and TVO). Therefore, it is concluded that the ATV data base, as it looks today, does probably not allow preparation of sufficiently credible plant specific failure data.

5.2 Specific data treatment methods

The application in which the data is used determines the way of data analysis. For basic calculations, the reliability data used in PSAs is often enough, and standard data analysis procedures are suitable. In modern PSAs the methods are those of Bayesian statistics, which makes the incorporation of engineering judgement possible. Classical methods (non-parametric methods, maximum likelihood estimations, classical parametric analyses including trend tests, etc.) may also be applied, but do not allow the flexible inclusion of engineering judgement.

If data is needed for specific modelling problems, we analyse the empirical data according to our modelling principles. Examples of this are the estimation of parameters in the linear standby failure rate model, the estimation of repair times, and ageing trend analysis.

If the models are based on several assumptions, the data analysis should reflect these assumptions simultaneously in order to avoid double counting and other types of incoherencies. An error sometimes encountered in data analysis is that the data is first analysed with respect to some aspect (e.g. ageing) and thereafter other assumptions are taken into account (e.g. time-dependent standby failure model) and both analyses are based on the same empirical data. This leads to double counting and to artificial extension of evidence. To avoid these kinds of errors qualitative data analysis methods are needed.

The aim of qualitative data analysis is to identify or reveal various failure modes and mechanisms which may have influence on the TS evaluations. Examples of such failure modes are failures which cannot be detected in normal surveillance testing, failures which occur more frequently in accident situations, dependent failures, and ageing. If these types of phenomena are identified in a qualitative way we may already at that stage draw conclusions or make decisions and corrective actions which may be concerned with TS.

Many of the important factors having effect on TS evaluations can hardly be evaluated directly on the basis of statistical analysis. As an example, the expected positive effects of preventive maintenance on component reliability may be mentioned. The evaluation of these factors must be based on engineering or expert judgement. Systematic ways to select experts, train them for probabilistic evaluation, eliciting the expert opinions, and mathematical modelling of the expert judgements should be further developed.

In TS evaluations, various sensitivity and uncertainty analysis principles are applied. However, many of the methods do not take into account the strength of the background statistical evidence. One of the most important aspects of data analysis is to make the evaluations more credible, in which task also the statistical methods and principles are of great importance.

Applications within the NKA/RAS-450 project include several analyses of specific features of the reliability of motor operated valves (MOV). In all the applications described, the failure data is the same as, or part of the data analysed in the pilot project on MOV data analysis [5.8].

5.2.1 Standby failure rate [5.9]

When performing a data analysis, two important characteristics of the data are the coverage and the homogeneity. Data from different test arrangements (e.g. leakage tests vs. motioning of valves) are not homogeneous, and should be treated separately. Often the data available is incomplete, which increases the uncertainty of the results. In the case study, the sensitivity of the linear standby failure model (see section 3.3.2) was studied with respect to three factors; coverage, homogeneity, and estimation method.

As for coverage, specifically concerning total number of activations during the periods concerned, the impact of possible underestimation of the number of activations is not clear. However, the effect on the estimation of q and λ parameters might be significant.

The data set of this example seemed to be rather inhomogeneous, especially concerning valves having 3 months test interval (all belonging to system 321, shutdown cooling system). This was probably due to systematic differences in operating conditions, and possibly also due to differing test acceptance requirements. Heterogeneity usually causes bias and will necessarily lead to greater uncertainties.

The effect of the choice of estimation method was noticeable. While the estimation of λ was rather insensitive, q was rather sensitive also in larger data sets. Generally, larger data sets mean smaller differences.

Bayesian analysis of standby components is possible but poses a rather difficult problem from the computational point of view. Due to the special sampling situation, the Bayesian estimations have till now only been successful in the case of minor data sets.

5.2.2 Repair time distributions [5.10]

Criteria for allowed outage times (AOT) for corrective maintenance of safety-related equipment are specified per failure event in the TS for Forsmark and TVO. When making probabilistic analyses of TS problems, it would be highly unrealistic to assume the entire AOT to be used up in each failure situation [5.11]. Instead, the average unavailability time, and the associated probability distribution should be determined.

The criticality definition of the faults is shown in Fig. 5.2.

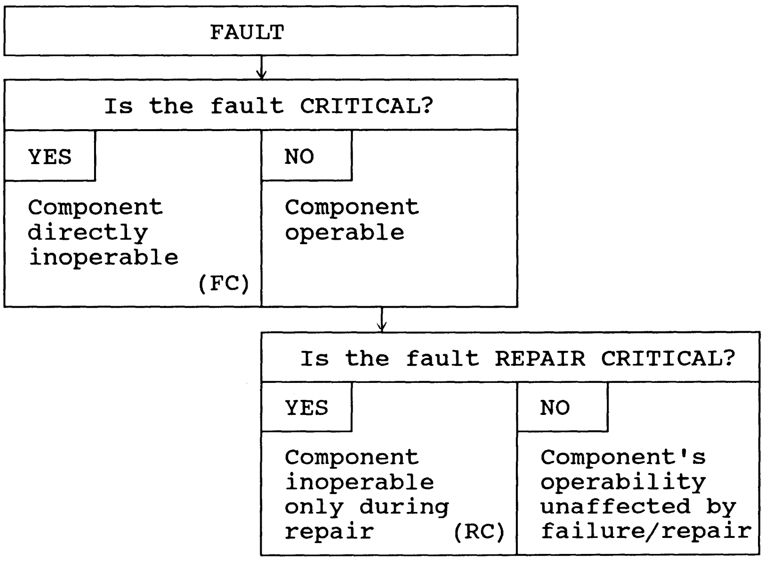

FAULT
Is the fault CRITICAL?
YES
NO
Component directly inoperable (FC)
Component operable
Is the fault REPAIR CRITICAL?
YES
NO
Component inoperable only during repair (RC)
Component's operability unaffected by failure/repair

Figure 5.2 Definition of fault effects on standby component.

The analysis described is concerned with FC (function critical) and RC (repair critical) type failures. A further division can be made on the basis of the detection method, i.e. latent or monitored.

The analysis was based on ATV reports for Forsmark and on failure data used within the TVO PRA. The period covered is 1981-86. The undetected unavailability time, preceding the corrective maintenance activities, was not included in the analysis. In order to estimate the parameters of the data observed, a number of statistical distributions were tried; the maximum likelihood method was then used for the estimation. The best fits were arrived at by using the 2-mixture exponential (TVO) and the Weibull distribution (Forsmark). The mean repair times that were thus arrived at are shown in Table 5.1.

Table 5.1 Average repair times for motor operated closing valves (hours).

	TVO I/II		Forsmark 1/2	
	Revision	Operation	Revision	Operation
Critical	26	36	58	31
Repair critical	44	41	50	46

It should be noted that the average repair times (25 - 60 hours) are far below the maximum allowed outage times (AOT) given in TS. The AOTs are 30 days for single failures. Only 15 % of the repair times of the MOVs exceeded 3 days which is the AOT limit for possible double failures.

Direct comparison of the repair waiting and active repair times between the plants is not possible due to differing reporting practices in the ATV and TVO PRA data bases.

The experience from these repair time analyses in general is that it would be beneficial to be able to present the following detailed steps contributing to the unavailability time of a safety-related equipment:

- undetected unavailability time
- repair waiting time
- active repair time
- post-repair unavailability time.

Such a subdivision would facilitate a more complete evaluation of the effects of technical failures and human errors on the unavailability of the equipment. The failure reports from the plants should therefore include an exact information of the start instant of the unavailability time of repair-critical faults and the return instant of the equipment to the on-line operability after repair of critical or repair-critical failures.

5.2.3 Ageing trends [5.12]

In an analysis covering the same critical failures for TVO I/II and Forsmark 1/2 as in the pilot project on MOV data analysis [5.8], it was investigated if any ageing trends can be identified for the plants or for selected valves. Non-critical and repair-critical failures were not included. The failures detected during revision periods were included. The internal leakages of valves were also included. A majority of the failures had appeared during revision outages.

Ageing trends were analysed by using a non-homogeneous Poisson process. The results were presented as β-values along with the associated probability of β being more than 1 (i.e. ageing). The results for different plants are shown in Table 5.2.

Table 5.2 Ageing trend analysis of motor operated valves.

Plant	β	$P(\beta>1)$
Forsmark 1	0.795	0.16
Forsmark 2	0.798	0.13
TVO I	0.875	0.18
TVO II	1.48	0.91

Thus, the results do not indicate any ageing tendencies, except possibly for TVO II (the underlying data for TVO II would have to be further studied in order to get a definite picture). The failure frequency of the shutdown cooling system (321) was much higher than in other systems. This may be due to differing operating conditions compared to the standby safety systems. Also, a difference in number of failures for the containment vessel spray system (322) and auxiliary feed water system (327) was observed between the plants. As mentioned in the previous sections of this chapter, this may well be due to differing reporting practices, resulting in differing coverage of the reporting.

5.3 Improvement suggestions for the ATV data base

Many of the case studies performed within the NKA/RAS-450 project involved the analysis of failure reporting, mainly for motor operated valves. These analyses utilized data from the ATV data base as well as from plant work order systems and from the RO system (safety related occurrences). As already indicated, a number of problems were encountered. Many problems are mainly concerned with the representativity of data, e.g. the kind of problems in use of ATV described in Fig. 5.1. However, some of the most important problems encountered concern the quality of the data base as such:

- completeness of failure reports,
- coverage of reporting (not all failures reported),
- homogeneity of failure reporting from different plants.

In this section, some specific recommendations will be given on actions that would help to improve the quality of data. These recommendations apply mainly to the ATV data base, as this is the main source of data for most PSA related work in Sweden and Finland. A more far-reaching proposal is given in [5.13], where the outlines of an entirely new data collection and information system are given, based on an integrated computer network and requiring major changes in current data collecting procedures. Here, only such recommendations are given that can be quite easily implemented, and that do not require any increases in the amount of data to be collected.

Thus, the following recommendations concerning the ATV Reliability Data System are given:

A. Modernization

The present ATV system was built up around 15 years ago. This means that it runs on a mainframe computer and utilizes the information processing techniques available at that time. The system is therefore somewhat outdated both from the hardware and the software point of view, and therefore has unnecessarily high operating costs. In view of this, the pay-off time for a modernization would probably not be very long. Data might still have to be stored on the mainframe computer, but the information processing could be made on a workstation or a PC. Major users should have the possibility to communicate with the data base online in a similar way as with the ERF information system. Online input of ATV data from the own and other similar plants would also probably affect the delay times favourably.

B. Presentation of Data

The options for data presentation should be updated in order both to make the system more easily accessed, and to make use of modern data processing, analysis and presentation techniques. This is a necessary step in order to make the system more attractive. Furthermore, with online users, e.g. in maintenance departments, this would be a necessary step.

C. Quality of Failure Reporting

The quality of the failure reporting in the sense mentioned above must be improved. This can only be achieved if reports are more strictly checked at the plant, before being submitted to the ATV data base. The persons responsible for the reporting should both check the completeness and correctness of the reports and guarantee the homogeneity of the reporting. This does obviously not work especially well today. Some kind of coordination of the reporting from different plants must also be made, as there are significant differences between plants with respect to all the quality parameters mentioned. This coordination must be the responsibility of the ATV staff.

D. Simplification

The information content of todays ATV data base should be better matched with the information needs of the ATV users. Today, only a fraction of the data stored is used, mainly for probabilistic analyses. Probably, there is a potential for simplification that might release resources. The simplifications may consist both in a reduction of the number of systems covered (e.g. focus on standby safety systems and safety-significant process systems), and in a reduction of the parameters to be stored. Thus, much of the information on failure causes and failure effects which is normally also found in the work order system, might be entered automatically from computerized work order systems. Additionally greater stress must be put on specifying the unavailability times involved in failure occurrence and repair.

E. Motivation

From the very beginning, the main problem with the ATV data base has been the lacking motivation of the personnel in maintenance departments. At many plants they do not use the data base, and will consequently not be very happy with the extra burden the reporting puts on them. To increase the motivation can never be an easy task and may even be impossible considering the very specific use of the data. However, it may be possible to do it indirectly if the data base is being used directly by the utility, which is not the case today. This presupposes that the plant personnel has online access to the ATV data base for feedback of component operating experience from own and other similar plants, as described in A. An even more feasible approach is to take advantage of the high motivation for the filling out of work orders. This will be achieved simply by including some extra information in the work order and by eliminating entirely the extra task of filling out an ATV reporting form.

F. Efficiency of Reporting

The approach outlined in E above is especially efficient if the work order system is computerized, in which case the selection and the transmission of the information to the ATV reliability data base can also be made automatically.

REFERENCES

5.1 Knochenhauer, M. Verification of System Reliability by Analysis of Failure Data and Testing, PSA'89 International Topical Meeting on Probability Reliability and Safety Assessment, Pittsburgh, Pennsylvania, April 2-7, 1989. ABB Atom Report RPC 88-153, NKA/RAS-450S(89)1.

5.2 Eriksen, L. and Knochenhauer, M. Impact of Differences in Testing Conditions and Anticipated Real Conditions on Reliability Data for Motor Operated Valves. ABB Atom Report RPC 88-44, NKA/RAS-450S(88)2.

5.3 Karlsson, C. and Knochenhauer, M. Mapping of the Influence of Periodical Testing and Preventive Maintenance on the Auxiliary Feedwater System in Forsmark 1 and 2 (in Swedish). ABB Atom Report RPC 87-45, NKA/RAS-450S(87)5.

5.4 Ekberg, K., Andersson, M. and Bento, J-P. The ATV System and its Use, PSA'85 International ANS/ENS Topical Meeting on Probabilistic Safety Methods and Applications, San Francisco, California, February 24 - March 1, 1985.

5.5 T-BOOK - Reliability Data for Mechanical And Electrical Components in Swedish Nuclear Power Plants, Second Edition 1985, RKS 85-05, prepared by ABB Atom AB and Studsviks Energiteknik AB for the Nuclear Safety Board of the Swedish Utilities and the Swedish Nuclear Power Inspectorate, May 1985.

5.6 Knochenhauer, M. and Tuvesson, L. Development of a Time-dependent Failure Model for Motor Operated Valves Based on Analysis of Failure Data and Testing, ABB Atom Report RPC 89-69, NKA/RAS-450-S(89)2.

5.7 Engqvist, A., Mankamo, T. Test Scheme Rearrangement for Diesel Generators at Forsmark 1/2. PSA'89 International Topical Meeting on Probability, Reliability and Safety Assessment, Pittsburg, April 2 - 7, 1989. NKA/RAS-450(89)1.

5.8 Knochenhauer, M. Pilot Project on Valve Data Analysis. ABB Atom Report RPC 88-59, NKA/RAS-450-S(88)3.

5.9 Simola, K. and Pulkkinen, U. Statistical Sensitivity Analysis of Linear Standby Failure Model - A Case Study on Motor Operated Valves at TVO and Forsmark Nuclear Power Plants. Work Report VTT/SÄH 10/89, NKA/RAS-450F(89)3.

5.10 Simola, K., Laakso, K. and Huovinen, T. Repair Time Distributions and Unavailability Time Definitions for Motor Operated Closing Valves at TVO and Forsmark NPP's. Work Report VTT/SÄH 5/90, NKA/RAS-450F(89)2.

5.11 Pulkkinen, U., Huovinen, T., Norros, L., Mankamo, T., Vanhala, J. Reliability of Diesel Generators in the Finnish and Swedish Nuclear Power Plants. VTT Research Notes 1070, Espoo 1989. NKA/RAS-450F(89)5.

5.12 Simola, K., Huovinen, T. and Laakso, K. Failure Trend Analysis of Motor Operated Valves in TVO and Forsmark Plants. Work Report VTT/SÄH 2/89, NKA/RAS-450F(89)1.

5.13 Lyytikäinen, A. Idea Plan for Improvement of Nordic Reliability Information Systems. Work Report in the Section 6.3 of Summary Work Documentation of the NKA/RAS-450 Project 1985-89. May 1990.

6. DECISION SUPPORTING MEASURES AND UNCERTAINTY

In this chapter we are concerned with the situations of decision making which are actualized by Technical Specification (TS) issues, and how the results of probabilistic safety analysis (PSA) could be presented in order to really support the decision maker. The first section describes the use of various risk importance measures, the second is devoted to treatment of uncertainties associated with each decision option, the third one discusses a theoretical framework for the presentation of probabilistic analyses including the uncertainty aspects in a decision situation. The fourth section discusses general demands on presentation of results to decision makers.

Some typical situations of decision making concerning TS have been treated in the previous chapters. As main categories [6.1] we may mention decisions whether one can allow temporary exemptions from or permanent modifications of TS. In the latter group we find the decision, treated in [6.2], of allowing continued power operation or initiating plant shutdown in case of a degraded safety system (Fig. 4.3).

It is easy to understand the documentation requirements the analyst must fulfil in order to support the decision maker, namely to clearly and systematically summarize the results achieved and to describe all presumptions, limitations and simplifications that have been made in the analysis. As regards the uncertainty aspects it is equally important to qualitatively identify all the uncertainty sources the analyst is aware of.

6.1 Definitions and use of risk importance measures

A quick, approximate guide for prompt decision making in specific situations is provided by precalculated risk importance measures, which have also been studied in the project. This section decribes how these measures can be used as a gross guidance to importance ranking with respect to different aspects, such as safety significance of a fault, safety impact of possible reliability improvements, or suitability of test arrangement changes.

Risk importance measures are means to present contributions to the absolute risk in the form of relative information, which often is more suitable than absolute numbers for making conclusions. Several types of importance measures are available, each describing some special aspect. For a broader treatment of the subject, the reader is referred to the excellent textbook presentation [6.5] and the technical reports [6.8, 6.9]. The importance measures which have been used and analysed most in this project are defined in the following, using risk frequency (f) as the basic risk variable.

<u>The fractional contribution</u> - originally introduced by Fussel and Vesely [6.6] - is the most commonly used importance measure in PSAs. Let f_n denote the nominal risk frequency (see also 4.3.2). If f_0 is the corresponding frequency when the system/component considered is assumed perfectly reliable ($f_0<f_n$), then the fractional contribution (C) is defined as [6.4]

$$C = (f_n-f_0)/f_n.$$

Thus this measure describes the fraction of the total risk frequency which is affected by the system/component considered. In many fault tree evaluation codes the fractional contribution is calculated according to its original definition, based on the concept of minimal cut set (MCS). In practical cases, where the rare event approximation can be used in MCS and sequence quantifications, the fractional contribution is equal to the <u>criticality importance</u>, which is often used as an alternative in PSA studies [6.7].

The risk increase factor, also called risk achievement worth or increased risk ratio (IRR), is defined as the relative increase of the risk frequency given the system/ component concerned is known to be failed or removed from the plant design. Thus if f_1 stands for the risk frequency of this degraded state ($f_1 > f_n$) the risk increase factor (A) is formally defined as

$$A = f_1/f_n.$$

An important use of the risk increase factor, as pointed out in [6.4], is that it classifies the systems and components according to the impact of their unavailabilities (caused by maintenance, repairs or tests, including erroneous isolations from the line). Furthermore, it helps to identify systems and equipment for which reliability assurance measures would be important.

Another measure, the risk decrease factor or risk reduction worth, is obtained when calculating the relative decrease in the risk frequency assuming that the system or component concerned is perfectly reliable (never fails). Thus the risk decrease factor (D) is formally defined as

$$D = f_n/f_0.$$

Sometimes the inverse of D is used, a measure called risk remainder or decreased risk ratio (DRR).

The practical interpretation of the risk decrease factor or its inverse value is that they describe the maximum improvement theoretically achievable by improving the reliability performance of the feature considered. Hence they serve as a tool for classification of potential improvement objects [6.4].

The definitions of the importance measures mentioned above as well as some analytic relationships between them and practical examples are presented in more detail in

[6.8]. A hierarchical procedure of calculation, based on the concept of conditional probability but approximated to MCS representation of system logics of a PSA, has been tentatively applied in [6.10] (see Figs. 6.1 and 6.2).

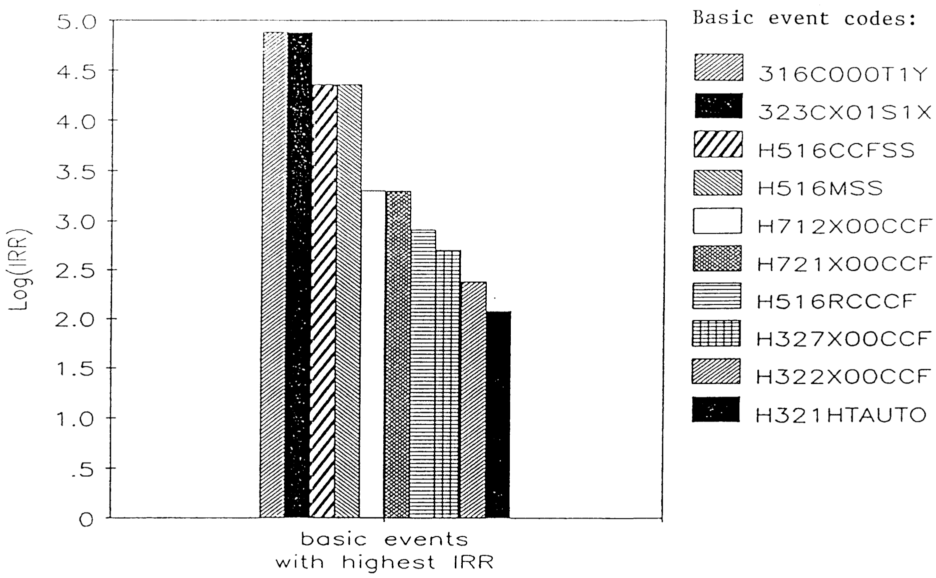


Figure 6.1 Increased risk ratio IRR (risk increase factor) with respect to the core damage frequency of two initiating events from the Forsmark 3 PSA study - a tentative application [6.10].

Some designations and explanations

316COOOT1Y = empty condensation pool
323CX01S1X = emergency core cooling strainer plugged
H516CCFSS = CCF in 3/4 channels of reactor protection system 516
H516MSS = independent failure in 3/4 channels of system 516
H712X00CCF = quadruple CCF in shutdown service water system 712
If log(IRR)= 5.0, then IRR = 100000
If log(IRR)= 2.0, then IRR = 100

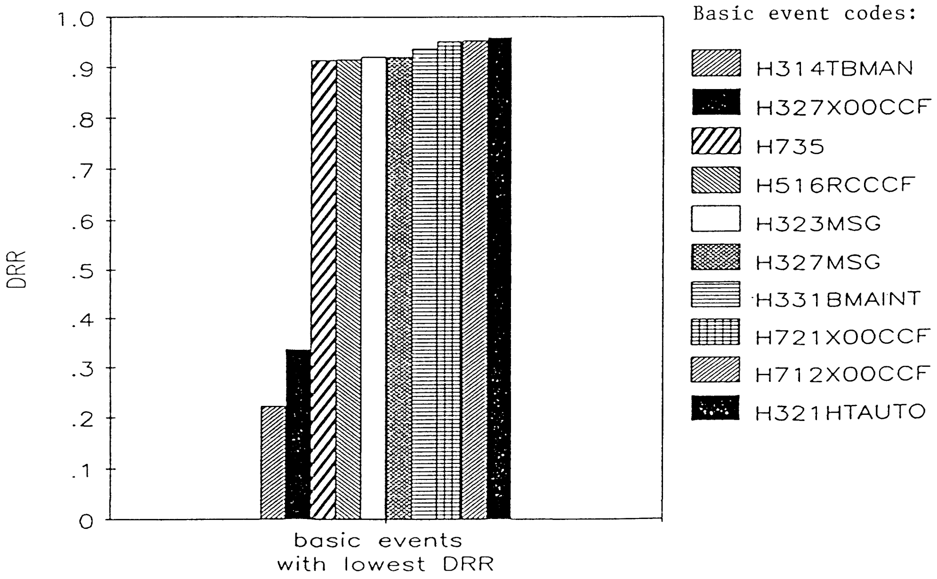


Figure 6.2 Decreased risk ratio DRR (risk remainder) with respect to the core damage frequency of two initiating events from the Forsmark 3 PSA study - a tentative application [6.10].

Some designations:
H314TBMAN = error in manual depressurization
H327X00CCF= quadruple CCF in auxiliary feedwater system 327.

As shown above importance measures are valuable tools for processing of PSA results into a form more suitable for drawing conclusions and making decisions.

6.2 Treatment of uncertainties

In each decision making situation one has to choose among a set of alternatives, $\{d_j\}$, the consequences of which having to be evaluated and mutually compared [6.3]. In case of permanent changes of TS, the decision maker may be faced with several possible solutions to the problem. When a temporary exemption from TS is being discussed, there are usually only two alternatives; to apply TS as they are or to allow a temporary exemption. To choose among alternative actions is, however, a decision under uncertainty. This uncertainty comes from the uncertain (random) events $\{E_j\}$, which are dependent on the decision taken but have not occurred or otherwise are unknown at the moment of decision. In the example mentioned in the introduction of this chapter such uncertain events may consist of potential transients occurring during the repair of the degraded system or initiated by the process of plant shutdown. Other events may be failure occurrences which make necessary safety systems unavailable.

As will be seen in the next section, to evaluate the various decision alternatives it is necessary to estimate the probability of the uncertain events, $P(E_j|d_i)$, conditioned by each alternative decision d_i. To estimate these probabilities for TS oriented decisions one needs at least PSA results, but probably also the results of an extended analysis related to the specific situation, as decision supporting information. Results including their uncertainty bounds from a PSA study are presented as an example in Fig. 6.3.

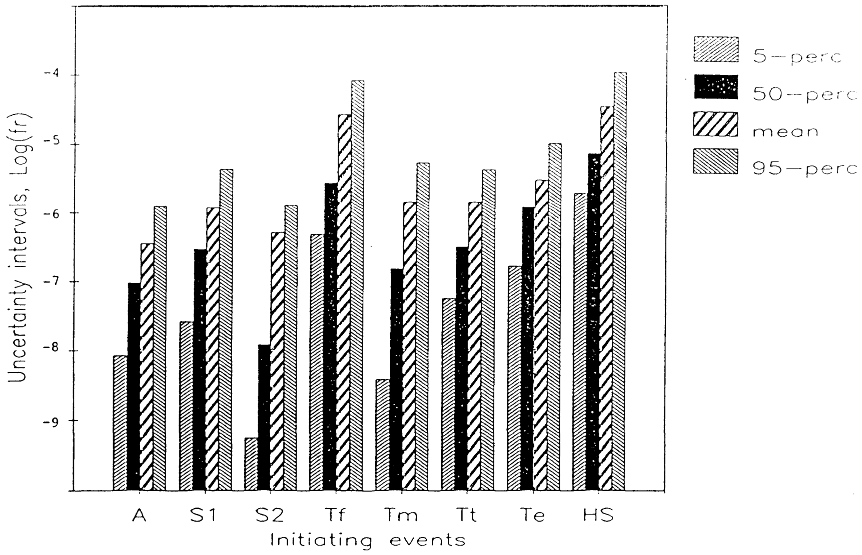


Figure 6.3 Uncertainty intervals of core melt frequency (fr) and its contributors corresponding to the different initiating events [6.12].

Some designations:
Tf = loss of feedwater supply
HS = total core melt frequency

The uncertainty considered in this section is related to the determination of the probabilities $\{P(E_j|d_i)\}$. The modelling of both the system structure and the unavailability of its components is uncertain because of the limitations of the analysis and the lack of knowledge about the complex relationships. Further, the probability models are usually based on parameters, $P(E_j|\theta,d_i)$, where the parameters θ are uncertain because of sparse input data.

Due to the relative complexity of phenomena and models, explicit and systematic treatment of uncertainties is absolutely necessary in TS considerations. The modelling and data uncertainty types that are most relevant in TS considerations, are summarized in Table 6.1. Both types can be described by probability distributions, although the modelling uncertainty has hitherto been assessed mostly by sensitivity analysis. In principle, however, the modelling uncertainty can also be treated probabilistically. This will hopefully become possible even in practice by the future development of the uncertainty analysis techniques.

As a general rule, the problems evaluated should always be decomposed and treated isolated when possible. This makes analyses simpler and enhances possibilities of managing uncertainties and achieving valid conclusions.

Table 6.1 Uncertainties of special importance in TS evaluation

Uncertainty	Type	Remarks
Time dependent unavailability models of components	D,M	Characteristic to specific components and plants; influenced by operating and maintenance conditions; operator/system interface also important
Repair/restoration time distributions	D	
Dependent failures	D,M	
Sequential thermohydraulic phenomena and dependences	M	Complex physical phenomena and little direct operating experience
Coverage of plant - protection functions instrumentation - automation - DC power supply systems	B	Amount of work needed or detailed treatment is tremendous, often inadvertently skipped assuming that these give only minor contribution
Operator response to disturbances, manual restoration possibilities	B,M,D	Influenced by many factors; difficult to construct realistic models/ obtain data for models
Quality of test and maintenance, and associated relationships	B,M,D	Treatment has mainly been confined to a qualitative analysis only, except in the simplest cases

D = Data lacking, difficulties in the interpretation of recorded events

M = Modelling problems, relationships not sufficiently known

B = Boundary limitation, difficulties in the identification of important contributions

How can we treat the uncertainties discussed above in the decision making process? Fortunately we can use a basic probability law, which in terms of notations that we have already presented, reads

$$p(E_j|d_i) = \int p(E_j|\theta,d_i)p(\theta|d_i)d\theta,$$

where we have included the model parameter θ and the (parametric) uncertainty distribution $p(\theta|d_i)$. The probability on the left hand side of the formula is a single number and has no uncertainty bounds around it. The probability itself expresses the total uncertainty concerning the occurrence of the event E_j, i.e. it incorporates the uncertainty on the values of the model parameters θ, too. Typical examples of θ are failure rates - time or demand related - on component level, CCF-parameters on system level and core melt frequency on plant level. The determination of the joint distribution $p(\theta|d_i)$ is the main objective of the uncertainty analysis. The difficulty in obtaining this objective depends, of course, strongly on the level of consideration and complexity of the decision variable to be used.

6.3 Decision making under uncertainty

In the previous section we presented the probabilities $\{P(E_j|d_i)\}$, where both d_i and E_j run through an exhaustive and exclusive list of decisions and uncertain events. In addition to these probabilities the decision maker has to evaluate the consequences $C[d_i,E_j]$ of each pair of decision and uncertain event. Because the consequences may be of quite different size and type the decision maker needs a yardstick by which the consequences can be measured and compared to each others [6.3]. Such a yardstick is the concept of utility.

Well established decision theoretic models [6.11] help us to combine these separate quantities in a logical and coherent way to finally reach a decision which maximizes the expected utility or minimizes the expected risk. Although the implementation of the neat, logical theory may be difficult in many practical cases, it would be worthwhile to aim at in the future development. Such a step should give a desirable structure both to the analysis work and to the decision process.

To translate our present efforts around TS to the decision theoretic vocabulary we have already mentioned examples on decision sets $\{d_i\}$. Similarly, much light can be thrown on the decision problem by the mere attempt to provide an exhaustive list of events $\{E_j\}$, the outcome of which will affect the consequences. As such uncertain events we may think of the occurrence of plant transients and of failures in appropriate safety systems during the time period considered. The task to identify a really complete list of events includes the same problem of completeness as we encounter in all PSA work. Much work in the form of normal PSA as well as specific TS related analysis today is devoted to the determination of the probabilities $\{P(E_j|d_i)\}$. As these are a measure of uncertainty they will also incorporate the uncertainty associated with the analysis itself, namely the parametric and modelling uncertainties. This requires that the latter types of uncertainty are described by probability distributions. Finally the analyst has to present the consequence $C[d_i,E_j]$ for each pair of the decision and uncertain event, in the range from no damage at all to the worst possible accident. Thereafter it is the decision maker's task to mutually rank these consequences and assign a utility-value to each of them. The different steps in this theoretical decision making framework including necessary supporting analyses are schematically illustrated in Fig. 6.4.

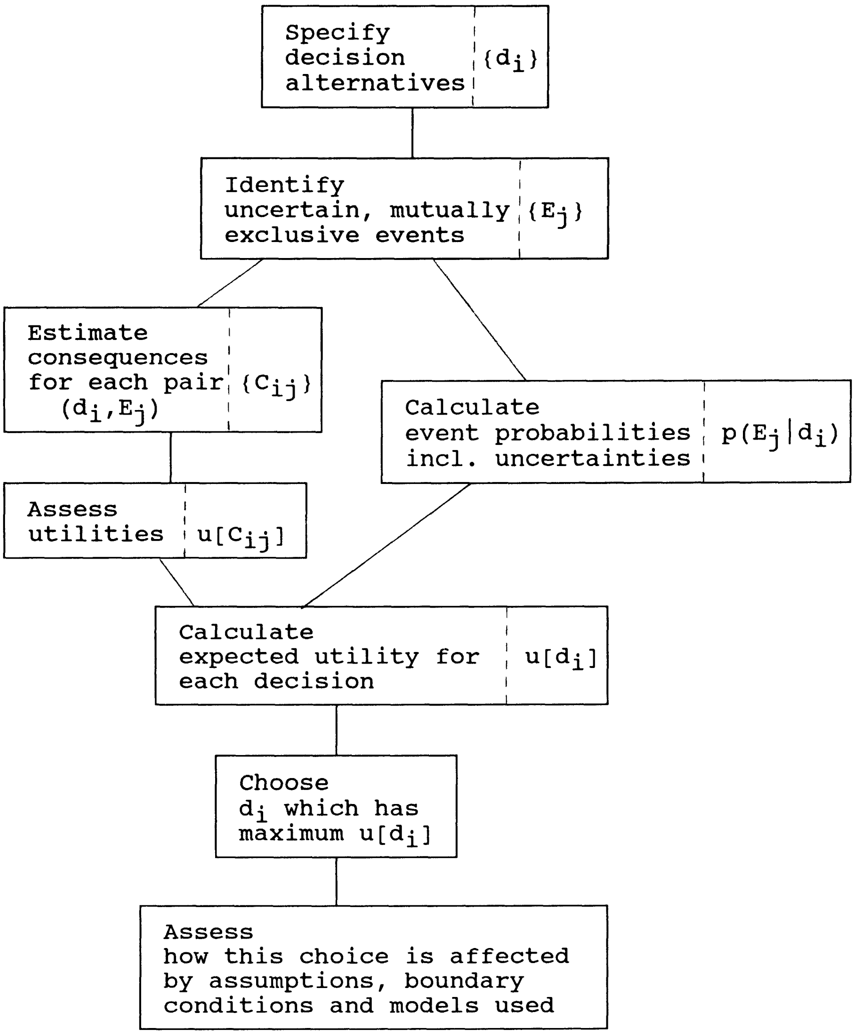

Specify decision alternatives
$\{d_i\}$
Identify uncertain, mutually exclusive events
$\{E_j\}$
Estimate consequences for each pair (d_i,E_j)
$\{C_{ij}\}$
Calculate event probabilities incl. uncertainties
$p(E_j|d_i)$
Assess utilities
$u[C_{ij}]$
Calculate expected utility for each decision
$u[d_i]$
Choose d_i which has maximum $u[d_i]$
Assess how this choice is affected by assumptions, boundary conditions and models used

Figure 6.4 Theoretical framework procedure for decision making.

It is encouraging to see that most of the items and thoughts presented in [6.1] can be given the decision theoretic framework discussed above. Thus the procedure is relatively clear as far as such decision influencing factors are concerned that can be quantified. Well aware of the fact that all analyses are incomplete in some respects it is very important that this incompleteness is highlighted by explicitely presenting the boundary conditions and simplifying assumptions. If the analyst has not been able to include the modelling uncertainty into probability measures, this uncertainty must be emphasized by presenting the results of traditional sensitivity analyses.

What has been said above is valid especially for decision making situations that can be anticipated (e.g. permanent changes of TS) and, therefore, can be supported by comprehensive, probabilistic analyses made in advance. Such analyses cannot be performed in situations when the decision has to be taken on very short notice (e.g. certain exemptions from TS). Then the decision has to be based, as far as possible, on already available analysis results. An important group of such initially available results are the various importance measures treated previously in chapter 6.1.

6.4 How to present results to decision makers

The previous section dealt with the more theoretical aspects of making decisions under uncertainty, and also presented an analysis procedure. This section will deal with more general demands on an analysis, demands that apply even if no formal uncertainty analysis is performed, and that must be fulfilled in order to assure that the results presented are adequate both with respect to contents and layout [6.1]. Thus the section ends up with a checklist concerning the main demands on how to present results for decision making.

6.4.1 What do we mean by results?

Usually, when utilizing the word "results", we refer to only a part of the outcome of an analysis, usually presented as a kind of summarizing numerical codification, which may or may not be supplemented with clarifying tables, graphs, or illustrations.

In the context of decision making, the term takes on a wider meaning, and includes all the information that is needed in order to understand and interpret the results of an analysis. Thus, the three main parts are:

1. Assumptions and boundary conditions
2. Models used
3. Final results.

It is usually necessary also to include negative information, meaning information on what has not been done, potentially relevant conditions that were not fulfilled, alternative models that were not used, etc.

6.4.2 Users of results

As a first step, the recipients of the results must be identified along with their expectations and demands on analysis results. It is an inherent dilemma that the analyst, while making the analyses and presenting the analysis results, is not the person who will make decisions based on the results and will not either be called up to act on the emerging decision.

Generally speaking, three levels of recipients of analysis results can be defined, with differing tasks:

1. <u>Technical level</u>

- executing.

2. Utility level (technical and economical level)
- planning
- decision making
- executing.

3. Authority level (society level)
- planning
- decision making.

When it comes to defining the information demands from these levels, it has to be taken into consideration that the number of qualitative boundary conditions will increase with the level. Some of the main demands put on the analysis results on the different levels are summarized in Table 6.2.

Table 6.2 Demands on analysis results from different user levels.

	Technical level
1a	Results should specify recommended or required actions and their technical consequences
1b	Results should provide basis for detailed planning
	Utility level
	In addition to all above mentioned requirements:
2a	Simplifying boundary conditions should not affect crucial parameters
2b	Must be possible to weigh results against crucial qualitative boundary conditions
	Authority level
	In addition to all above mentioned requirements:
3a	New non-quantifiable boundary conditions added; may be technically "irrelevant"
3b	Information should be "clean", i.e. it should give as clear a picture as possible of the purely technical situation
3c	Must be possible to combine with qualitative information on society level, e.g. power situation

The acceptance and usefulness of PSA results for decision making in TS related matters presupposes understanding of the assumptions and methods. The usefulness and understanding is greatly enhanced if the operating personnel and authorities are involved in the analysis process. Also the way, how the models and results are presented, plays an important role.

6.4.3 Summary of requirements

In view of the substantial uncertainties that are inherent in these types of decision making, strict demands must be put on the presentation of results. These general demands can be summarized as follows:

1. Basis for decision

- Boundary conditions and simplifications must be explicitely stated.
- Simplifications must be chosen in such a way that they do not infringe the applicability of results.
- Uncertainty analysis and sensitivity analysis should be systematically and extensively used.
- Conclusions which should lead to corrective actions in hardware or procedure should be presented.

2. Presentation of results

- Results should be expressed in terms of parameter(s) important to the decision (criteria).
- Results should show explicitely the influence of parameters that are either important or very uncertain.
- Results should show explicitely the influence of assumptions that are either important or very uncertain.

3. Models, assumptions and boundary conditions

- Qualitative boundary conditions
  - which are they?
  - how do they influence?
  - how have they been considered/ why have they not been considered?

- Quantitative boundary conditions
  - which are they?
  - how do they influence?
  - how have they been considered/ why have they not been considered?
  - uncertainty analysis/sensitivity analysis

- Choice of model
  - which models were used?
  - are there alternatives?
  - why were the alternatives not used?
  - might the alternatives lead to different conclusions?

REFERENCES

6.1 Knochenhauer, M. Decision Situations and Criteria in Modification of Technical Specifications, ABB Atom Report RPC 89-46, NKA/RAS-450S(89), 1990.

6.2 Kosonen, M., Piirto, A., Saarenpää, T., Mankamo, T. Continued Plant Operation Versus Shutdown in Failure Situations of Residual Heat Removal Systems, Teollisuuden Voima Oy. NKA/RAS-450F(88)1, April 1988.

6.3 Pulkkinen, U., Pörn, K. Uncertainty in Safety Analysis and Safety Related Decision Making. Proceedings of SRE-Symposium 89, Stavanger, Elsevier Applied Science, London and New York. NKA/RAS-450(89)6, 1989.

6.4 NUREG/CR-3385. Measures of risk importance and their applications. Prepared by Vesely, W. E., Davis, R. S., Denning, R. S. and Saltos, N., Battelle Columbus Laboratories. July 1983.

6.5 Henley, E. J. & Kumamoto, H. Reliability engineering and risk assessment. Prentice Hall Inc., 1985.

6.6 Fussel, B. J. How to hand-calculate system reliability characteristics. IEEE Trans. on Reliability, R-24, No. 3, 1973.

6.7 Schmidt, E. R. et al. Importance measures for use in PRAs and risk management. ANS/ENS Topical Meeting on Probabilistic Safety Methods and Applications, February 24 - March 1, 1985, San Fransisco. Proceedings, Paper No. 83.

6.8 Uses of Risk Importance Measures. Technical Report, 1990 (Draft). NKA/RAS-450(89)2, NKS/SIK-1.

6.9 Andsten, R., Vaurio, J. Reliability importance measures and their calculation. Imatran Voima Oy research report IVO-A-01/89. Helsinki 1989.

6.10 Pörn, K. A Tentative Application of Risk Importance Measures. Studsvik/NP-87/109, NKA/RAS-450-S(87)6, 1988.

6.11 Lindley, D. V. Making Decisions, Second edition, John Wiley & Sons, 1988.

6.12 Pörn, K. Analysis of parametric uncertainty in the PSA of Forsmark 1/2, Studsvik NP-88/46 (in Swedish), 1988.

7. OUTLINE OF CASE STUDIES

In order to test and verify the methods and criteria developed, practical case studies have been performed during the development work. The objective of the case studies was also to provide a support for utilities' and authorities' decisions of TS modifications. The case studies have mainly been carried out by use of utilities' or authorities' resources or funding.

The actual results and conclusions from the case studies are specific for TVO and Forsmark nuclear plants and are seldom transferrable between the plants, because even small differences in design and procedures may be important. Available models and data can, however, often be utilized in a new application after reasonable modifications.

7.1 Continued power operation versus plant shutdown in failure situations of residual heat removal systems

This case study [7.1] is the most recent made at the TVO plant for the evaluation and balancing of TS by means of probabilistic methods [7.2]. The primary aim is to consider the LCOs of multiple failure situations in the residual heat removal (RHR) systems of this BWR plant. The plant shutdown risk is compared with the risk of continued power operation over the expected equipment repair times. The operational alternative with the minimum risk was searched, i.e. the minimum probability that the RHR function is not available when called for.

The relative benefits of the power operation alternative can mainly be attributed to the low transient frequency during the power operation state compared with the risk of introducing an isolation transient or an off-site power disturbance while shutting down the plant. Also the decreased reliability of the remaining parts of the RHR systems to start and operate, assuming multiple failure state in the RHR systems, contributes to the disbenefit of the shutdown alternative.

Adequate modelling of the significant phenomena and risk predictions have necessitated the development and use advanced sequence modelling and quantification methods. This in turn implies that a lot of effort is required to carefully address uncertainties. Systematic sensitivity analyses have aided to verify the conclusions.

The results justify the allowance of a reasonable repair time during plant operation also in situations of three or all four RHR subsystems failed, which contrasts to the existing specifications that require a prompt plant shutdown in such situations. Appropriate modifications in the LCOs, including operational instructions, for RHR systems have been specified by the utility and passed on for review of the Finnish authority.

This case study is used as a practical example in the sections 4.1 and 4.3 of this report.

REFERENCES

7.1 Kosonen, M., Piirto, A., Saarenpää, T. & Mankamo, T. Continued operation versus shutdown in failure situations of residual heat removal systems - Application of risk analysis methods for the evaluation and balancing of limiting conditions of operation. Teollisuuden Voima Oy, NKA/RAS-450F(88)1, April 1988.

7.2 Kosonen, M., Piirto, A., Vanhala, J., Mankamo, T. & Pulkkinen, U., Experiences of the use of PSA methods at the TVO power plant. Teollisuuden Voima Oy, June 1986.

7.2 Preventive maintenance of standby safety systems during power operation

In connection with a test period of performing preventive maintenance (PM) during power operation at the Forsmark 2 plant in 1985, a number of probabilistic analyses were performed on system level as well as on plant level [7.3, 7.4]. The system level analyses formed part of the verifications submitted to the authority together with the request for a TS change, while the plant level analyses were performed as a case study within the NKA/RAS-450 project.

7.2.1 System level calculations

The system level analyses concerned unavailabilities due to PM isolations in the following standby safety systems:

- 322, Containment cooling system
- 323, Emergency core cooling system
- 327, Auxiliary feedwater system.

The analysis quantified the system failure probabilities when performing PM on one out of four subsystem, assuming the system capacity to be 4 x 50 % or 4 x 100 % (corresponding to the situation after a LOCA or transient, respectively). The main contributor to the uncertainty was assumed to be the estimation of the parameters of the CCF model. Therefore, a systematic sensitivity analys with respect to these parameters was also included. Some general conclusions concerning the PM effect on system failure probability are:

- CCF parameter uncertainty is very important for the quantitative results in the 4 x 100 % subsystem case,
- "pessimistic" CCF parameters give a negligible quantitative effect from PM, while "optimistic" parameters give a significant effect,
- with the planned PM volume (about one week yearly for each subsystem) the system failure probability increases over one operating year by about 6 %.

7.2.2 Plant level calculations

The Forsmark 3 PSA plant models were applied as the source material for this study. The performance of the analysis on plant level has some advantages compared to the system level analysis. Thus, plant level analyses make it possible to:

- quantify the effects of a number of simultaneous outages of different subsystems,
- quantify the effects of PM isolations on shared auxiliary systems,
- compare entire PM schemes with each other.

The plant level analysis of the Forsmark PM covered the following systems in addition to the three front-end systems listed above:

- 321, Shutdown cooling system
- 711, Shutdown secondary cooling system
- 715, Shutdown cooling water system
- 654, Diesel system.

The quantification was made by recalculating dominating PSA core melt sequences using the PM schemes as boundary conditions. The PM is performed in two four week campaigns, where one subsystem at a time is taken off-line for a week. The two campaigns (PM1 and PM2) involve PM on the following standby safety systems:

PM1:	321,322,323,327,711
PM2:	654,715.

Results were presented for two safety functions, makeup water supply and residual heat removal. It should be noticed that PM is not performed on the reactor protection systems during power operation at the Forsmark 1 and 2 plants. The one-time risk increase during the PM period was presented along with the average increase over one operating year. In addition, an alternative to the proposed PM scheme was evaluated. The changes evaluated consisted of putting redundant systems (323 and 327) in different PM campaigns, and in putting functionally serial systems (711 and 715) in the same campaign.

The original PM layout resulted in an annual average increase in core damage frequency of 6.4 %. The alternative

PM layout resulted in rather negligible reductions of this increase. In the pilot project, these quantitative results were considered together with the qualitative aspects concerning maintenance planning, performance, and quality. All these three aspects were considered to benefit greatly from performing part of the PM during power operation compared to the refuelling outage.

As a result of the Forsmark 2 pilot project, PM during power operation was considered feasible and acceptable and is now being carried out on a regular basis in all three Forsmark plants as well as in the Oskarshamn 3 plant.

REFERENCES

7.3 Knochenhauer, M. The Forsmark 2 Preventive Maintenance Project. Experiences and Results from the Probabilistic Calculations. ABB Atom Report RPA 86-330, NKA/RAS-450S(86)1, October 1986.

7.4 Knochenhauer, M. Plant Level Probabilistic Evaluation of Preventive Maintenance during Power Operation in Forsmark 2. ABB Atom Report RPC 87-61, NKA/RAS-450S(87)4, August 1987.

7.3 Assessment of component reliability by analysis of failure data and testing

Four of the case studies performed within the project, sponsored by the Swedish State Power Board and the Swedish Nuclear Power Inspectorate, dealt with various aspects of periodic testing of equipment in standby safety systems. A general description is given in [7.5].

The two focal points have been either the testing as such or the component failure data, which are based largely on failures appearing at testing.

The problem of testing vs. failure data has been seen and analysed from the point of view of PSA applications. A detailed description of these problems appearing in preparation and use of data is given in section 5.1 of this report. The following problems are addressed in the case studies:

1. Coverage of testing, i.e. the extent to which the whole equipment is involved in the test actions.
2. Applicability of failure data to real demands, i.e. the extent to which operating conditions during the real demands differ from the test conditions.
3. Dependence of the component reliability on the length of the test interval.
4. Development of time dependent failure model.

7.3.1 Coverage of testing

The first analysis [7.6] concerned the auxiliary feedwater system (327) of the Forsmark 1 and 2 plants, and aimed at evaluating the degree of coverage of each periodic test or preventive maintenance action. Thus, the study addressed the problem how the contents and frequency of tests and preventive maintenance influence the system reliability.

The active components of the system 327 were divided up into blocks representing separate functions, e.g. logics, switchyard equipment and motor. Each test and maintenance action was then analysed in order to evaluate to what extent each of the separate functions was verified (full/partial/no verification). The results were presented as a "Coverage Chart" for each test and maintenance action. The test coverage chart for the yearly revision test of RPS signals is shown in Chapter 3, Fig. 3.6.

Based on failure reporting in the local work order system, in the ATV data base and in RO reports, all functionally critical failures that had occurred 1981-86 were analysed and used as a basis for a sensitivity analysis. The failures indicated a rather high percentage (about 30 - 50 %) of failures that had either been caused at a test or remained undetected after a test.

The sensitivity analysis consisted of time-dependent calculations using the FRANTIC computer program [7.7]. These calculations showed that test introduced failures are a less serious problem than the ineffectiveness of the test, and that the system reliability is highly time dependent.

7.3.2 Applicability of failure data to real demand situations

Quantitative estimates of component failure parameters are usually based on failures that have to a considerable degree appeared at testing. Due to the imperfect coverage of testing, and due to the fact that many of the situations encountered and qualitatively evaluated in a PSA can never be reproduced in a test, these test detected failures are not sufficiently representative. Therefore periodic tests are representative only as long as real operating conditions do not deviate too much from testing conditions.

A procedure for qualitatively identifying significant deviations from nominal operating conditions has been developed and tested in an analysis of motor-operated valves (MOV) of four safety systems in Forsmark 1 and 2 [7.8]. The analysis was also used as the basis for a thinking-model to be applied in a quantitative analysis.

The most important parameters that were expected to differ between test conditions and real demands, were absolute pressure, differential pressure, temperature, and voltage level. These parameters were studied for the MOVs during all feasible PSA scenarios and compared with testing conditions. Four types of scenaria were defined:

1. Normal operating conditions, i.e. after most plant transients
2. Conditions after a loss of coolant accident, LOCA
3. External pipe break within the system
4. Extreme operating conditions ("worst case" considered in PSA).

The main results from the analysis were the following:

- For some MOVs substantial deviations were identified, mainly high differential pressures and big temperature changes.
- Conditions after a plant transient will usually be very similar to test conditions. This indicates, that failure data based on tests covering the function of the whole component should have a rather good applicability.
- The different MOV types (gate, globe, and ball valves) are in a different way vulnerable to deviating operational conditions. Similar differences apply to the type of MOV action required (open/close). As an example, the gate valves are more sensitive to the differential pressure than the other valve types.

7.3.3 Component reliability versus test interval length

The test interval length of the MOVs is an important parameter when it comes to direct influence on the component reliability. Current Nordic data bases do not present standby failure rates for MOVs. It was therefore decided to perform a pilot project [7.9]. The MOVs belonged to three standby safety systems and one continously operating system in nine Swedish and Finnish ABB Atom BWRs. The MOV population studied was rather homogeneous with respect to design and operating conditions.

The analysis covered a total of 78 reactor years. The valves were divided into groups according to their test interval length (1, 3, or 12 months). A total of 564 failures were found and analysed with respect to functional criticality, failure cause, way of detection, and detection time (revision period or operating year).

As might be expected, differences were identified between the plants. These were partly due to "real" plant-to-plant differences, but were mainly due to random variations in the underlying data and to systematic errors arising from differing reporting practices. The total results, based on a summation of individual plant data give a relationship between MOV unavailability (q) and test interval length

(TI). This case can be described by a time-independent and a time-dependent part in the model:

$$q(TI) = 1.4E-04 + 2.8E-06/h * TI$$

In this case, the time dependent part will dominate. The above integration of all MOVs presupposes that the population studied is reasonably homogeneous.

The analysis also resulted in the identification of a number of problems concerning the quality and interpretation of failure data. These problems have been treated in Chapter 5 in this report.

7.3.4 Development of a time dependent failure model

A concluding analysis was performed, aiming at providing an extension and a summary of the work performed previously [7.10]. The analysis was also an attempt to connect and translate previous qualitative works on this matter to a quantitative failure model for MOVs. The data was focused on the Forsmark 1 and 2 plants. Along with the ATV reports previously evaluated, RO reports were also evaluated in order to provide detailed information on failure mechanisms, with the view of getting a deeper qualitive understanding of the failure causes of MOVs, and on the circumstances of the functional failures.

A major potential problem identified concerns incorrect torque switch settings, due to drifting, incorrect calibration or unsuitable design specifications. In order to estimate the severity of the problem a separate study was made of the outcome of all torque switch calibrations performed in the Forsmark 2 plant in 1986-1989. A very high proportion of the MOVs turned out to deviate from the nominal torque settings, some of the deviations are considerable.

The quantitative model developed was thus based on the outcome of the analysis of MOV failure reports as found in the ATV system and in RO reporting. The unavailability model includes a best estimate part formed by contributions from:

- latent standby failure buildup
- repair critical failures
- runtime failures (occurring during valve activation)
- test introduced failures (eg. component misconfiguration).

For these contributors the material from this analysis, as well as from analyses performed previously, was considered to be of sufficient quality to make possible the calculation of a point estimate.

As part of the analysis, a test case was evaluated in order to demonstrate how the use of this modified failure model influences the outcome of a PSA performed with generic failure data from the T-book. Some of the main conclusions from the MOV test case are:

1. The introduction of a time dependent model with respect to test interval time has resulted in a substantial reduction of the originally calculated average core melt frequency.
2. The plant risk effects seem to be similar on accident sequences belonging to the make-up water supply and to the residual heat removal.
3. The failure probability due to incorrect torque switch setting may potentially have a very great influence on quantitative PSA results, especially concerning extreme operating conditions.

However, for the contribution related to the torque switch calibration, data indicated a major influence but allowed no definite conclusions to be drawn. For this reason it was decided to perform a systematic sensitivity analysis. The sensitivity analysis was to include normal as well as extreme operating conditions. Two obvious conclusions can be drawn from the quantification:

1. The large discrepancy between the MOV data presented in the T-book, where time-dependent effects are distinguished from time-independent effects, and the time-dependent model as developed in the pilot study on MOV data, will influence a corresponding difference on plant risk level.

2. The unresolved issue of the criticality and extent of the torque setting problem, has a major impact on the MOV failure probability, especially in cases with non-standard operating conditions.

REFERENCES

7.5 Knochenhauer, M. Verification of System Reliability by Analysis of Failure Data and Testing, PSA'89 International Topical Meeting on Probability, Reliability and Safety Assessment, Pittsburgh, Pennsylvania, April 2 - 7, 1989. ABB Atom Report RPC 88-153, NKA/RAS-450S(89)1.

7.6 Karlsson, C., Knochenhauer, M. Evaluation of the Effect of Periodic Testing and Preventive Maintenance on the Auxiliary Feedwater System in Forsmark 1 and 2. ABB Atom Report RPC 87-54, NKA/RAS-450S(87)5, August 1987.

7.7 Vesely, W. E., Goldberg, F. F. FRANTIC - A Computer Code for Time Dependent Unavailability Analysis, NUREG-0913, October 1977.

7.8 Eriksen, L., Knochenhauer, M. Impact of Differences in Testing Conditions and Anticipated Real Demand Conditions on Reliability Data for Motor Operated Valves. ABB Atom Report RPC 88-44, NKA/RAS-450S(88)2, June 1988.

7.9 Knochenhauer, M. Pilot Project on Valve Data Analysis. ABB Atom Report RPC 88-59, NKA/RAS-450-S(88)3. June 1988.

7.10 Knochenhauer, M., Tuvesson, L. Development of a Time-dependent Failure Model for Motor Operated Valves Based on Analysis of Failure Data and Testing, ABB Atom Report RPC 89-69, NKA/RAS-450-S(89)2. September 1989.

7.4 Test scheme rearrangement for diesel generators at Forsmark 1/2

Forsmark 1 and 2 units each have four diesel generators (DG), which have been tested once a week since the start of the commercial operation in 1981. In every fourth test the DG is loaded (LT) while the other weekly tests are just start tests (ST). In annual tests, during the refuelling outage, the loss of power in buses is simulated. In addition, the DGs become challenged, in average about once a year, in random isolation transients, loss of power bus events or off-site power disturbances.

At the plant, the operating staff had begun to experience that the start tests are unnecessary frequent, and requested for a systematic analysis of the influences of lengthening the test interval. Such an analysis was carried out in cooperation with the operation and maintenance staff from the Forsmark plant [7.11, 7.12]. The analysis utilized available PSA information [7.13], and benefitted much from the earlier Finnish-Swedish DG study [7.14].

The analysis started with a thorough analysis of the incident reporting from 1981-87, extracted from the Swedish RO data base. These data provided a good comprehension about the selective effectiveness of the annual tests and actual demands as compared to the periodic ST/LTs. The unavailability model, applied first at the DG aggregate level, produced the sensitivity for the ST/LT interval. Three alternative test schemes with a decreasing number of STs were specified, and the influences were evaluated by use of Forsmark 1/2 PSA at the level of reactor core damage risk.

The study resulted in a proposal of a test scheme with two weeks ST/LT interval. LT were placed at every fourth week per DG, but evenly staggered in the four subs. There are a number of technical aspects, which seem to be better balanced in the proposed scheme. Especially, the pairwise staggered scheme is believed to be a reasonable compromise between risk of systematic errors in testing and control of the risk of latent multiple CCFs. A change in the technical specifications according to the proposal has been specified by the utility and has been reviewed by the Swedish authority. A trial period for this change is going on at one DG before the final authority decision. The experiences of this analysis have contributed also to the development of the existing incident reporting systems.

This case study is discussed in more detail in the sections 3.3 and 3.4 of this report.

REFERENCES

7.11 Engqvist, A. & Mankamo, T. Test scheme rearrangement for diesel generators at Forsmark 1/2. PSA'89 International Topical Meeting on Probability, Reliability and Safety Assessment, Pittsburgh, April 2-7, 1989, NKA/RAS-450(89)3.

7.12 Mankamo, T. & Engqvist, A. Failure mode analysis and classification for standby diesel generators at Forsmark 1/2. NKA/RAS-450(89)1.

7.13 Forsmark 1/2 PSA. Swedish State Power Board, 1988.

7.14 Pulkkinen, U., Huovinen, T., Mankamo, T., Norros, L. & Vanhala, J. Reliability of diesel generators in the Finnish and Swedish nuclear power plants. Technical Research Centre of Finland, Report VTT Research Notes 1070. NKA/RAS-450F(89)5, Espoo, October 1989.

8. CONCLUDING PROJECT SUMMARY

The main results of the NKA/RAS-450 project are summarized in this last technical chapter of the report. The degree to which the objectives of the project were achieved are discussed and topics for continued work are proposed. Potential opportunities for further use of the project results are also presented.

8.1 Method development

The analyses and criteria, developed during the project, can be divided into three groups:

- probabilistic resolution strategies and decision supporting measures
- risk and reliability assessments
- reliability data bases.

A large number of work reports, which include a detailed documentation of the method and criteria development have been compiled in an extensive technical documentation [1.1]. Several practical case studies were performed in order to test and verify the above methods and criteria and to identify needs for method development and adaptation.

8.1.1 Development of probabilistic resolution strategies and decision supporting measures

Probabilistic resolution strategy
The proposed probabilistic resolution strategy covers the whole spectrum of tasks involved in the evaluation of a Technical Specification problem. The significant factors to be taken into account, and the modelling and data needs, often go beyond the scope of an ordinary PSA. The resolution flow diagram is divided into a prestudy stage and a probabilistic study stage. The later stage will be performed if the prestudy shows that safety or cost benefits are likely

to justify a further probabilistic study. In Chapters 3 and 4 of this report the resolution flow diagram has been applied to analysis and proposal of a test scheme rearrangement and an allowed outage time modification.

Risk importance measures

The risk importance measures are means to present contributions to the absolute risk in form of relative information. Relative contributions and relative changes are often a more suitable basis than the absolute PSA numbers for drawing conclusions and for prompt decision making in specific operational situations. Ready-for-use results needed for temporary exemptions from TS may be provided by precalculated risk importance measures. The use of risk increase factor in TS considerations, for evaluation of the safety significance of a fault or an isolation of equipment due to maintenance, was also further developed and tested. A hierarchical procedure for the calculation of risk importance measures has been introduced within the project.

8.1.2 Development of risk and reliability assessments

In order to provide a proper perspective, it will often be necessary to calculate more than one risk measure. For instance, a risk that results in a negligible annual average risk increase according to a PSA study may still be unacceptable due to a very high risk level during specific outages of equipment or due to dramatically increased risk for a plant transient.

The three variable risk approach

An approach searching for minimum risk in failure and repair situations, during power operation of a plant, has been studied and proposed. The choice between the operational alternatives in TS should be made with due regard to the measures of the instantaneous risk frequency, the expected risk over the failure situation, and the impact of the adopted rules on the integrated risk over the plant lifetime. Risk comparison of alternative operational modes has necessitated the introduction of advanced modelling of event sequences, phased missions and recovery options, with the associated need to obtain relevant data. As these needs go beyond the scope of usual PSAs, a development and adaptation of the analysis and quantification methods was needed, although an existing PSA greatly helps, as it provides a frame for models and data applied.

Effectiveness of surveillance tests of standby equipment
The surveillance tests are aimed at simulating real demands as closely as possible, but there still remain many differences compared to abnormal conditions. A systematic procedure for qualitative identification of differences between test conditions and anticipated accident conditions has been developed and applied for motor-operated closing valves. The use of functional block techniques also showed encouraging results when evaluating the coverage of component and system tests in an auxiliary feedwater system.

Risk quantification of alternative test schemes of redundant equipment
Methods for quantification of risk effects of alternative test schemes of redundant equipment, and methods for identification of human originated test and maintenance failures, were further developed and tested. In our practical analyses of the effectiveness of standby equipment testing, the detailed analysis and modelling work could be confined to the system or component level, and the higher level influences could be determined by help of an existing plant-specific PSA.

8.1.3 Planning of reliability data bases

Specific data needs in optimization of Technical Specifications
The need for data and other information for optimization of Technical Specifications is more extensive than in an ordinary reliability analysis. Additional needs were

identified and specified when performing failure data analyses of motor-operated closing valves, emergency diesel generators and auxiliary feedwater systems.

ATV Reliability Data System

Adequate data for the analysis of surveillance test and maintenance effectiveness, and the proneness to introduce human errors in test and maintenance activities, so far seem to be very difficult to obtain from the Swedish ATV Reliability Data System. In the ATV system, attention should be paid to collection, analysis and use of this data at the individual plants for feedback of component experience and analysis of failure trends. A part of this information should also be extracted to other similar plants and central organizations for further use, such as comparison of experiences and reliability analysis.

Specific data treatment methods

Specific data treatment methods, for analysis of ageing trends and repair time distributions of standby components, were tested and found suitable for practical needs in the project. A Bayesian estimation of parameters, in a linear failure model for standby component, was also tested.

8.2 Essential practical results and findings

8.2.1 Practical results for utilities and authorities

The task of optimization of Technical Specifications

The purpose of TS is to provide an envelope for safe plant operation. The rules of TS concern both the baseline risk of the plant by specifying the intervals and contents of periodic testing, and accepted temporary risk increases by specifying limiting conditions for operation. Thus, the TS ultimately provide a controlled way of trading excessive safety margin for operational flexibility. Therefore the optimizing of TS has a twofold meaning:

1. Generally to make optimal use of the available flexibility provided for a specific set of TS rules.
2. Specifically, to solve individual TS problems in an optimal manner, normally by minimizing either the baseline risk or some other relevant risk measure.

The practical case studies have resulted in the following support for utilities' and authorities' present and future decisions on modifications of technical specifications.

Identification of operating modes that give minimum risk in multiple failure situations

It was concluded that usually the total average risk can be affected relatively little by the optimal choice of the allowed outage times (AOT). However, in the cases of multiple failures in a safety system, order of magnitude differences may exist between the expected risks over the failure situation in question, depending on which operational mode is selected. The central LCO issue, the decision between repairs during continued power operation or plant shutdown for repairs, has also a significant economic consequence because of the high income loss caused by a forced plant shutdown. The results of the TVO case study, concerning failure situations in the residual heat removal systems, justify the allowance of a short repair time (AOT) during power operation also in situations with three or all four subsystems failed. This result contrasts with the existing specifications that then require a prompt shutdown of the plant.

Furthermore, the potential opportunities to use the reactor water clean-up and plant heating systems as a back-up path for residual heat removal became evident in the system analysis of this TVO study.

Preventive maintenance of standby safety systems during power operation

Performing preventive maintenance (PM), in one subsystem out of four during power operation in the newest Nordic BWR plants, has many qualitative benefits compared to PM during refuelling outage. The qualitative benefits were not possible to express in quantitative terms, but it can be expected that improved equipment reliability, at least partially, counterbalances the few percent's unavailability contributions from the PM periods during power operation. One disadvantage of performing the PM during refuelling outage is that it is loaded with a large number of tasks within a tight time schedule. Within the project the temporary risk increments, caused by isolation of equipment due to PM during power operation, were evaluated by adaptation of a PSA plant level model. The results of these risk quantifications at plant level, and the designed excess margin to the single failure criteria with one subsystem unavailable, made it possible to justify the introduction of a specific amount of preventive maintenance during power operation at the Forsmark 1, 2 and 3 plants.

In order to avoid risks for inadvertent reactor scrams, PM on reactor protection systems is not performed during power operation at Forsmark 1 and 2 plants.

Test scheme rearrangement of diesel generators
An analysis of test efficiency, and quantification of the risk effects of alternative test schemes for redundant emergency diesel generator equipment, has resulted in the proposal of a modified test arrangement including less start tests and a pairwise staggered time scheme. A trial period for this TS change is going on at the Forsmark 1/2 plants before the final authority decision.

Test conditions of motor-operated valves versus real demands
When comparing the accident and testing conditions for motor-operated closing valves (MOV) in safety systems, considerably deviating operating conditions were found in some cases, concerning e.g. differential pressures over slide and increasing temperatures. This finding is also significant for the PSA issue, because failure data mainly originates from surveillance tests and the reliability of some MOVs may thus be questioned in more severe accident

scenarios. Appropriate studies and corrective actions for reliability and testing improvements of valves are under way at the power companies.

Systematic analysis of safety-related occurrences
The different case studies of motor-operated closing valves, emergency diesel generators and auxiliary feed water systems have included practical qualitative and quantitative analyses of operating experience using the reporting of safety-related occurrences (Swedish RO) as data. The studies resulted also in recommendations to increase the explanatory parts of the reporting of failure causes and to decrease the amount of coding, in order to enhance the feedback of this proper operating experience for planning of corrective actions and for analysis of test and maintenance effectiveness.

8.2.2 Improved understanding in safety-related decision making

Reduction of potential precursors to high risk situations
The above TVO shutdown risk analysis concerning the residual heat removal function shows an example where the probability of the safety function to be unavailable, when demanded, is much more sensitive to the reliability of the equipment and operations than to the AOTs of equipment. This result depends on the undetected unavailability time due to latent faults in standby equipment. The frequency of failures and disturbances is not directly treated in TS, but it determines the likelihood of entering into rare multiple failure situations. Hence, we want to strongly emphasize the primary role of reliability assurance measures for the achievement of low failure and disturbance frequencies at the plants. This would also reduce the integrated risk over the plant lifetime.

Reduction of uncertainty in safety-related decision making
The use of PSA and reliability methods has helped to identify, analyze and present temporary high risk situations

in advance. The understanding of complex operational, maintenance and testing situations is enhanced by systematic treatment and presentation of the many factors affecting the plant safety and availability. This use has the potential to improve the readiness and knowledge of the management and staff of the plant and the authorities to plan, manage and supervise complex operational activities or situations at a nuclear power plant.

The use of probabilistic decision criteria
Obviously, the decision criteria in TS evaluations can never be expressed entirely in quantitative terms. Thus, it will always be necessary for authorities to define frames. A recommended way for making decisions based on probabilistic evidence is to proceed in two steps:

1. Quantitative demonstration of numerical acceptability, with or without the use of a formal acceptance criterion.
2. Case-by-case decision based on weighing quantitative results against qualitative assumptions and boundary conditions.

8.3 Work left and areas not covered

Comparing with the original objectives of the project, there are two essential topics which were only partially achieved:

- Balancing between safety and economy
- Planning of experience data bases to be used for utilities' and authorities' assessment of alternative requirements in technical specifications.

8.3.1 Balancing between safety and economy

In the management of nuclear safety the primary emphasis is on the prevention of accidents, particularly accidents which could result in severe damage of the reactor core. The possibility of such accidents constitutes a significant economic risk for the utility, and indirectly for the whole industry since an accident in one plant may lead to consequential shutdowns in other plants for extended periods. It is acknowledged that this economic risk adds the motivation of the Nordic utilities to reduce the accident probabilities to very low levels.

In our project an economical optimization could be the achievement of as low accident probability as reasonably achievable by use of constrained economical resources. In practice this is done by selecting one out of a number of feasible TS alternatives.

Balancing of safety and economy using cost-benefit analyses or multiple objective optimization has thus not been explicitely studied in this project. Furthermore, such balancing was not needed, when possibilities to attain greater operational flexibility, cost-effectiveness or energy availability at a preserved or enhanced safety level were studied.

The multiple objective optimization goal has not yet been achieved, but it seems not to be necessary either in the treatment of most of the TS problems.

8.3.2 Planning of experience data bases

Our results and proposals have been specified and can be used as a basis for introduction of improvements in the reporting of safety related occurrences (RO) and in the ATV Reliability Data System. A specific plan for the improvement of existing data and information systems was not prepared. Participation in the compilation of the next Swedish Reliability Data Handbook was not included in the scope of this project, but the NKA/RAS-450 project has provided an input for the planning and compilation of this reliability data book through an active information exchange.

8.4 Future plans

As indicated in this report, there remains important research, development and application work to be done. In the long run, one should try to attain the Living Probabilistic Safety Assessment (LPSA) by continuously using new experience from operation, maintenance and design to update the PSA models and data, and by making systematic use of PSA for decision support in matters concerning safety. Incidents should be analyzed to indicate improvement needs both at the plant and in the PSA.

Safety evaluation

A significant part of these development needs will be addressed by the Nordic project NKS/SIK-1 on safety evaluation during 1990-93. This project is concerned with two areas complementary to each other:

- Living PSA development and application, and
- Operational safety indicators.

The Living PSA development and application

The living PSA concept can be developed and tested gradually within a selected part of following application areas:

- Long-term risk planning of TS rules, maintenance, testing procedures and designs.
- Retrospective evaluation of incident, failure and maintenance situations, including exemptions from TS rules.
- Control and monitoring of plant safety status.

A Living PSA is planned to be a flexible system for assessing relative changes in the reactor core damage frequency caused by permanent changes in designs or by temporary changes in operating situations. Tools for qualitative analyses should also be included in the development of Living PSA.

Plant-specific safety indicators

The living PSA issues are closely related to development of plant-specific safety indicators. They are used for identification and presentation of reliability trends and levels, based on analysis of the own operating, failure and maintenance experience from the plants. Such operational safety indicators provide timely indications of changes in the factors contributing to the risk level of the plant and thus give early warning if the plant's safety margins are decreasing.

Enhancement of the PSA use in decision situations

The use of PSA in supporting decision making must still be improved. Therefore it is necessary to realize the uncertainties and limitations behind the risk models, data and boundary conditions, as well as to understand that risk is perceived in various ways. Thus issues in decision making under risk, as well as efficient ways for presentation of decision supporting results, will be studied within this project.

A system for controlling operational safety

One objective of the NKS/SIK-1 project is to define a feasible risk and reliability based system for control of operational safety to supplement the present technical specifications, as well as for development and verification of safety at an operating plant. Selected parts of such an information system will be tested in practical case studies which form the basis for definition of the information system concept. The case studies will also include an evaluation of the benefits and limitations of the use of such a system in different application areas. In connection with practical case studies for specific nuclear power plants, the method and model development needs can also be identified and the methods can be tested and models verified.

8.5 Concluding remarks

The Nordic working group

The project has promoted the level of expertise in the Nordic countries. The most part of the project work has been carried out by a Nordic working group, consisting of experts on operational safety, PSA and reliability methods. Representatives from utilities, regulatory authorities, research institutes, vendors and consultants have worked in this group. The group has communicated with the Nordic nuclear power utilities and authorities and others interested in the subject and arranged several project seminars in Sweden and Finland. In this way the people actively engaged in the working group have received wide support and constructive critisism, which has had a productive influence on method and criteria development and in practical utilization of the results.

Benefits of practical applications

The NKA/RAS-450 project has contributed to the development of Technical Specifications and of test and maintenance practices of nuclear power plants in Finland and Sweden. It has also contributed to the development of the living PSA issue, the PSA methodology and the reliability data systems. Practical applications of PSA methods have made and can further make the operation and maintenance safer through TS changes, and more flexible by modifying requirements that are excessively stringent but not safety significant.

Reference for preparation of similar TS evaluations

This project is not proposing a total revision of the present Technical Specifications, which are now well established documents in the Nordic countries. Instead of that, the project provides a framework and reference for the utilities and authorities to prepare similar probabilistic evaluations and justifications of permanent TS modifications needed for other components, systems and plants.

The methods and principles developed can also be modified for use in other safety and reliability applications, e.g. in complex process and offshore plants.

Participation of plant personnel

The results of this and other PSA projects can be fully utilized only if decision makers and plant staff strengthen their understanding of the benefits and limitations of probabilistic safety assessment. In most cases this could be achieved by their increased participation in definition and performance of practical application studies.

The project documentation can be used as a basis for education and training of plant staff in risk and reliability assessment related to issues concerning Technical Specifications, probabilistic safety principles, testing and maintenance.

9. PUBLICATIONS AND REPORTS

General Reports 1985

RAS-450(85)1 Optimization of Technical Specifications by Use of PRA Methods. Project Description. 7 June 1985.

RAS-450(85)2 Preproject Survey. Optimization of Technical Specifications by Use of PRA-methods. 29 August 1985.

RAS-450(85)3 Optimization of Technical Specifications by Use of Probabilistic Methods. Project Description. Rev. 29 November 1985.

RAS-450(85)4 Göran Ericsson. A Summary of Comments from Scandinavian Power Utilities and Authorities. Asea-Atom. Rapport KPA 85-111 (in Swedish). Dat. 9.11.1985.

RAS-450(85)5 Kari Laakso & Urho Pulkkinen. Minutes from Preproject Seminarium at SKI in Stockholm (in Swedish). VTT. 19.6.1985.

General Reports 1986

RAS-450(86)1 Research Project Report 1985. Optimization of Safety Technical Specifications by Use of Probabilistic Methods. 15 January 1986.

RAS-450(86)2 Project Phase 1 Report. Optimization of Technical Specifications by Use of Probabilistic Methods. General Principles and Criteria. November 1986.

RAS-450(86)3 Optimization of technical specifications by use of probabilistic methods. Project description. Rev. 29.10.86.

RAS-400(86)1 SRE-Symposium 1986. Workshop on Risk Analysis - Methods and Applications. Summary of Discussions. Edited by J. Järvinen & K. Laakso. VTT/SÄH Report 46/86. Espoo, Dec. 1986.

General Reports 1987

RAS-450(87)1 Optimization of Technical Specifications by Use of Probabilistic Methods - Summary Work Report of Project Phase 1. 14 March 1987.

RAS-450(87)2 Stefan Brolin, Antti Piirto, Kari Laakso, Björn Wahlström. Technical Specifications for Nordic BWRs. Structure, Experiences and Ongoing Programs. CSNI/Unipede Specialist Meeting on Improving Technical Specifications for Nuclear Power Plants. Madrid, Spain. September 1987.

RAS-450(87)3 Seminar 2.4.87 concerning project NKA/RAS-450 (in Swedish). Swedish State Power Board, Råcksta. SSPB Report PKA-98/87.

General Reports 1988

NKA/RAS-450-88(1) NKA/RAS-450 (1985 - 1987). Optimization of Technical Specifications Using Probabilistic Methods - A Nordic Perspective. Summary Report 1985 - 1987. NKA Report 28.4.1988.

NKA/RAS-450-88(2) Optimization of Technical Specifications Using Probabilistic Methods - Proposed Work Plan 1988 - 1989. 12.4.1988.

NKA/RAS-450-88(3) Kari Laakso, Urho Pulkkinen, Alf Engqvist, Michael Knochenhauer, Antti Piirto, Tuomas Mankamo, Kurt Pörn. Optimization of Technical Specifications Using Probabilistic Methods. A Nordic Approach. Presented at the IAEA Technical Committee Meeting on the "Use of Probabilistic Safety Criteria", 11 - 15 April, 1988, Vienna.

NKA/RAS-450-88(4) NKA/RAS-450 (1985 - 1989). Optimization of Technical Specifications Using Probabilistic Methods - A Nordic Perspective. Summary Report of Project Phase 2. 9 December 1988.

NKA/RAS-450-88(5) Kari Laakso, Alf Engqvist, Michael Knochenhauer, Mikko Kosonen, Tuomas Mankamo, Kurt Pörn. Optimization of Operational Safety Rules Using Probabilistic Methods. Presented at the SRE-Symposium 1988. Västerås, Sweden. October 10 - 12, 1988.

General Reports 1989

RAS-450-89(1) Tuomas Mankamo, Alf Engqvist. Failure Mode Analysis and Classification for Standby Diesel Generators at Forsmark 1/2. - Experiences from a practical case study. Draft Technical Report 19.2.89.

RAS-450-89(2) Tuomas Mankamo, Kurt Pörn, Kari Laakso, Michael Knochenhauer. Uses of Risk Importance Measures. Draft Technical Report. 20 January 1989.

RAS-450-89(3) Tuomas Mankamo, Alf Engqvist. Test Scheme Rearrangement for Diesel Generators at Forsmark 1/2. PSA'89 International Topical Meeting on Probability, Reliability and Safety Assessment, Pittsburgh, Pennsylvania, 2 - 7 April 1989.

RAS-450-89(4) Optimization of Technical Specifications by Use of Probabilistic Methods - A Nordic Perspective. Summarized Work Documentation of the Project 1985-89. June 1990.

RAS-450-89(5) Urho Pulkkinen, Kurt Pörn. Uncertainty in Safety Analysis and Safety Related Decision Making. Proceedings of SRE-Symposium 1989. Reliability Achievement, p. 215-227. Elsevier Applied Science. London and New York.

RAS-400F(89)1 NKA/RAS-450/470-Seminar of the Development Projects 9.3.1989. Edited by J. Holmberg & K. Laakso. VTT/SÄH Report 17/89 (in Finnish). Espoo, June 1989.

Swedish Reports 1986

RAS-450S(86)1 Michael Knochenhauer. The Forsmark 2 Preventive Maintenance Project. Experiences and Results from the Probabilistic Calculations. Asea-Atom. Report RPA 86-330. Dat. 24 October 1986.

RAS-450S(86)2 Kurt Pörn and Stephen Dinsmore. Studsvik Energiteknik Ab. A Hierarchical Procedure for Calculation of Risk Importance Measures. Studsvik Report NP-86/125. Presented at SRE-Symposium 1986, Otaniemi, Finland, 14 - 16 October 1986 and at SNS/ENS/ANS Topical Meeting on Probabilistic Safety Assessment and Risk Management PSA '87, Zürich, Switzerland, September 1987.

RAS-450S(86)3 Göran Ericsson, Michael Knochenhauer, Göran Hultqvist. Optimization of Technical Specifications Using Probabilistic Methods. Presented at the SRE-Symposium 1986. Otaniemi, Finland. 14 - 16 October 1986.

RAS-450S(86)4 Ralph Nyman, Lennart Carlsson, Lars Andermo. How to Introduce Trend Analysis Utilizing Probabilistic Methods. Proceedings of the SRE-Symposium 1986. Otaniemi, Finland. 14 - 16 October, 1986.

Swedish Reports 1987

RAS-450S(87)1 Michael Knochenhauer and Alf Engqvist. Using PSA Models for Planning and Evaluation of Preventive Maintenance during Power Operation. CSNI/Unipede Specialist Meeting on Improving Technical Specifications for Nuclear Power Plants. Madrid, Spain. September 1987.

RAS-450S(87)2 Stefan Hirschberg and Michael Knochenhauer. The Role of Sensitivity Analysis in Probabilistic Safety Analysis. SMIRT9, 9th International Conference on Structural Mechanics in Reactor Technology. Lausanne, Switzerland. August 1987.

RAS-450S(87)4 Michael Knochenhauer. Plant Level Probabilistic Evaluation of Preventive Maintenance during Power Operation in Forsmark 2. Asea-Atom Report RPC 87-61. 13 August 1987.

RAS-450S(87)5 Claes Karlsson/Michael Knochenhauer. Optimization of Technical Specifications. Evaluation of the Effects of Periodic Testing and Preventive Maintenance on the Auxiliary Feed Water System in Forsmark 1 and 2. ASEA-Atom Report RPC 87-45 (in Swedish). 16.8.1987.

RAS-450S(87)6 Kurt Pörn. A Tentative Application of Risk Importance Measures. Studsvik Report NP-87/109. 5 December 1988.

Swedish Reports 1988

NKA/RAS-450S(88)1 Stefan Hirschberg, Michael Knochenhauer. Applicability of Probabilistic Safety Criteria in View of Evaluation of PSA Results. Presented at the IAEA Technical Committee Meeting on the Use of Probabilistic Safety Criteria, Vienna, Austria, April 11 - 15, 1988.

NKA/RAS-450S(88)2 Lennart Eriksen, Michael Knochenhauer. Impact of Differences in Testing Conditions on Reliability Data for Motor Actuated Valves. ABB Atom Report RPC 88-44, 88-06-01.

NKA/RAS-450S(88)3 Michael Knochenhauer. Pilot Project on Valve Data Analysis. ABB Atom Report RPC 88-59. 88-06-10.

NKA/RAS-450S(88)4 Michael Knochenhauer. A Tentative Evaluation of the Impact of Testing and Maintenance on System Reliability. Presented at the SRE-Symposium 1988. Västerås, Sweden. October 10 - 12, 1988.

Swedish Reports 1989

RAS-450S(89)1 Michael Knochenhauer. Verification of System Reliability by Analysis of Failure Data and Testing. Presented at PSA'89 International Topical Meeting on Probability, Reliability and Safety Assessment, Pittsburgh, Pennsylvania, 2 - 7 April 1989.

RAS-450S(89)2 Michael Knochenhauer. Decision Situations and Criteria in Modification of Technical Specifications. ABB Atom Report RPC 89-46. March 1990.

RAS-450S(89)3 Michael Knochenhauer, Lars Tuvesson. Development of a Time-Dependent Failure Model for Motor Operated Valves Based on Analysis of Failure Data and Testing. ABB Atom Report RPC 89-69. September 1989.

RAS-450S(89)4 Peter Jacobsson, Michael Knochenhauer. Importance Measures for Forsmark 3 Safety Systems Applied to Preventive Maintenance. ABB Atom Report RPC 89-96. December 1989.

RAS-450S(89)5 Peter Jacobsson, Michael Knochenhauer. Uncertainty Analysis of Dominating Sequences in Forsmark PSA Applied to Preventive Maintenance. ABB Atom Report RPC 89-97. December 1989.

RAS-450S(89)6 NKA/RAS-450 Seminar. Swedish State Power Board. Stockholm, September 26, 1989 (in Swedish). Ed. by Alf Engqvist. Swedish State Power Board Report PK-23/90.

Finnish Reports 1985

RAS-450F(85)1 Mikko Kosonen, Antti Piirto, Juhani Vanhala, Tuomas Mankamo, Urho Pulkkinen. Applications of the Use of PRA-Methods in the Re-Evaluation of Technical Specifications at the TVO Power Plant. June 1985.

RAS-450F(85)2 Tuomas Mankamo. Preproject Survey - International Developments. 27 August 1985.

RAS-450F(85)3 Tuomas Mankamo. Decision Event Tree Method. Presented at the SRE-Symposium 1985. Trondheim. Avaplan Oy. 30 Sept. - 2 Oct. 1985.

Finnish Reports 1986

RAS-450F(86)2 Tuomas Mankamo & Urho Pulkkinen. Test Interval Optimization of Standby Equipment. Technical Research Centre of Finland, Research Notes 892, September 1988.

RAS-450F(86)3 Tuomas Mankamo. Decision Event Tree Method Description with an Example on the Technical Specifications of Two Redundant Diesel Generators. Avaplan Oy, Technical Report. Draft Report 1986.

RAS-450F(86)4 Tuomas Mankamo. Comments on Vesely's Manuscript. (Determination of allowed outage times from a risk and reliability point of view, July 13, 1985). Avaplan Oy, Draft PM, October 1985.

RAS-450F(86)5 Tuomas Mankamo. Review of Socrates Models and Applications. Avaplan Oy. Draft, 14 May 1986.

RAS-450F(86)6 M. Kosonen, A. Piirto, J. Vanhala, T. Mankamo, U. Pulkkinen. Experiences of the Use of PSA Methods at the TVO Nuclear Power Plant. June 1986.

RAS-450F(86)7 M. Kosonen, T. Saarenpää, J. Vanhala, T. Mankamo. Continued Plant Operation Versus Shutdown in Failure Situations. Proceedings of the SRE-Symposium '86. Otaniemi, Finland. 14 - 16 October 1986.

RAS-450F(86)8 T. Mankamo. Phased Mission Reliability. A New Approach Based on Event Sequence Modeling. Proceedings of the SRE-Symposium '86. Otaniemi, Finland. 14 - 16 October 1986.

RAS-450F(86)9 K. J. Laakso. Interactive Use of Systematic Plant Disturbance Analyses and Probabilistic Risk Assessments. VTT. Proceedings of the SRE-Symposium '86. 14 - 16 October 1986. Otaniemi, Finland.

Finnish Reports 1987

RAS-450F(87)1 Antti Piirto, Tuomas Mankamo, Kari Laakso. Development of Technical Specifications Using Probabilistic Methods. CSNI/Unipede Meeting on Improving Technical Specifications for Nuclear Power Plants. Madrid, Spain. September 1987.

RAS-450F(87)2 Tuomas Mankamo. Is It Beneficial to Test/Start up the Remaining Parts of Standby Safety System at a Failure Situation? PSA'87. International SNS/ENS/ANS Topical Meeting on Probabilistic Safety Assessment and Risk Management. Zürich, Switzerland. September 1987.

RAS-45CF(87)3 Urho Pulkkinen, Tapio Huovinen. Parameter Estimation of the Linear Standby Failure Model. VTT. 1987.

RAS-450F(87)4 Antti Piirto, Tuomas Mankamo. Decision Alternatives in Failure Situation in Residual Heat Removal Systems at TVO. NKA Seminarium om Riskanalys och Säkerhetsfilosofi. (In Swedish) VTT. Otnäs, Finland. 12 - 13.11.1987.

Finnish reports 1988

NKA/RAS-450F(88)1 Mikko Kosonen, Antti Piirto, Tapio Saarenpää, Tuomas Mankamo. Continued Plant Operation Versus Shutdown in Failure Situations of Residual Heat Removal Systems - Application of Risk Analysis Methods for the Evaluation and Balancing of the Limiting Conditions for Operation. Teollisuuden Voima Oy Report, April 1988.

NKA/RAS-450F(88)2 Pekka Pyy, Tapio Saarenpää. A Method for Identification of Human Originated Test and Maintenance Failures. Presented at the IEEE Fourth Conference on Human Factors and Power Plants. Monterey, California, 5 - 9.6.1988.

Finnish Reports 1989

RAS-450F(89)1 K. Simola, T. Huovinen, K. Laakso. Failure Trend Analysis of Motor Operated Valves in TVO and Forsmark Plants. Work Report VTT/SÄH 2/89.

RAS-450F(89)2 K. Simola, T. Huovinen, K. Laakso. Repair Time Distributions of Motor Operated Closing Valves at TVO and Forsmark Plants. Work Report VTT/SÄH 5/90.

RAS-450F(89)3 Urho Pulkkinen, Kaisa Simola. Statistical Sensitivity Analysis of Linear Standby Failure Model. A Case Study of Motor-Operated Valves at TVO and Forsmark nuclear power plants. Work Report VTT/SÄH 10/89.

RAS-450F(89)4 Tuomas Mankamo. Phased Operations and Recovery Options - Advances in Event Sequence Quantification. PSA'89, Pittsburgh, April 1989.

RAS-450F(89)5 Urho Pulkkinen, Tapio Huovinen, Leena Norros, Tuomas Mankamo & Juhani Vanhala. Reliability of Diesel Generators in the Finnish and Swedish Nuclear Power Plants. VTT Reserach Notes 1070. Espoo, October 1989.

ABBREVIATIONS AND TERMS

Selected Abbreviations

ABB	Asea Brown Boweri, Sweden, Switzerland
AFWS	Auxiliary feedwater system
AOT	Allowed outage time (of safety-related equipment)
ATV	Arbetsgruppen för Tillförlitlighet, Värmekraft, (Reliability data system), Sweden
BWR	Nuclear power plant with boiling water reactor
CCF	Common cause failure
CCI	Common cause initiator
CM	Corrective maintenance
CUT	Component unavailability time
DG	Diesel generator
EPRI	Electric Power Research Institute, U.S.A.
EPS	External power source
F1,2,3	Forsmark nuclear power plant, unit 1, 2, 3, Sweden
IAEA	International Atomic Energy Agency, Vienna
LCO	Limiting Conditions for Operation
LIT	Mänsklig tillförlitlighet - The Nordic project on human reliability (1981 - 1985)
LOCA	Loss of Coolant Accident (in nuclear reactors)
LORHR	Loss of residual heat removal function
MCS	Minimum cut sets
MOV	Motor operated valve
NEA	Nuclear Energy Agency, OECD, Paris
NKA	Nordic liaison committee for atomic energy
NRC	The Nuclear Regulatory Commission, U.S.A.
OECD	Organization of Economic Cooperation and Development, Paris
PM	Preventive maintenance
PRA	Probabilistic risk assessment
PSA	Probabilistic safety assessment
PWR	Nuclear power plant with pressurized water reactor
RAS	Nordisk kärnsäkerhetsforskning om riskanalys och säkerhetsfilosofi (Nordic program on Risk Analysis and Safety Philosophy, 1985-89)
RHR	Residual heat removal function (of a nuclear reactor)
RHRS	Residual heat removal systems

RPS	Reactor protection system
SKI	Swedish Nuclear Power Inspectorate
SSPB	Swedish State Power Board, Vattenfall
STI	Surveillance test intervals
STUK	Finnish Centre for Radiation and Nuclear Safety
TS	Technical Specifications
TVO	Teollisuuden Voima Oy, Finland
VTT	Technical Research Centre of Finland

Selected Terms and Definitions Used

Allowed Outage Time This stipulates the maximum allowed outage time (AOT) for an equipment in a safety system. The plant must usually be placed to a safer operational state, if the operability of the faulty equipment is not reached within its AOT.

Baseline Risk Frequency This is the risk level of the plant during power operation assuming that no failures are detected in safety systems and no subsystems are intentionally isolated for maintenance. Temporary outages of equipment in safety systems will increase the total plant risk level over the baseline risk frequency.

Basic Event A reliability analysis can be carried out down to a component failure mode or human error level where sufficiently reliable experience data can be obtained. The failure and error events, included in a reliability model, at the most detailed level are called basic events.

Critical Fault The fault is critical if it prevents directly the operability of equipment.

Instantaneous Risk Frequency This is the real time risk frequency of the plant based on the current operational state of the plant and its safety systems. The risk profile of a plant can be shown by the instantaneous risk frequency as a function of time.Sudden plant transients in combination with temporary outages of safety equipment may increase significantly the risk frequency over the baseline risk level.

Limiting Conditions for Operation

The limiting conditions (LCO) for operation are rules to be followed in order to maintain the plant operation within the bounds of safety analysis. The LCOs specify requirements on the number of subsystems operable at different operational states and the allowed outage times for equipment. These operational rules shall assure that safety systems are either ready for use or functioning on real demands, i.e. plant transients and accidents.

Minimal Cut Set

A cut set is a combination of basic events, e.g. component failures or human errors, leading to system failure. A cut set is called Minimal Cut Set, if the intended system function can be achieved by elimination of a single basic event only.

Nominal Risk Frequency

The total risk as calculated in PSA is the average risk over the baseline and sudden and temporary risk increase states. This means the result obtained by use of nominal failure probabilities for the systems and operators. It is usually feasible to define this average risk frequency from a PSA as nominal risk frequency and apply this average value as a reference risk level.

Non-Critical Fault

The fault is non-critical, if the operability of equipment is unaffected by the fault and its repair.

Reliability Assurance

Periodic testing and preventive maintenance are methods in parallel to condition monitoring, status monitoring, walk-arounds and local inspections aimed for reliability assurance of equipment and systems. Related analysis and planning methods for reliability assurance are e.g. reliability centered maintenance, and detailed performance indicators, including analysis of operating experience and trend analysis.

Repair-Critical Fault

The fault is repair-critical, when the repair prevents the operability of the equipment but the fault only did not affect the operational readiness.

Risk Frequency

The risk is here expressed in terms of risk frequency, i.e. frequency of an accident. The term can mathematically be defined as expected number of accidents over a given time period or alternatively as probability of accident per unit of time. Usually the risk frequency is expressed in units 1/year, and as a long term average, neglecting the actual time dependence in short term. The accident to be studied in the level 1 PSAs is severe reactor core damage event.

Risk Importance Measures

Risk importance measures are means to present contributions to absolute risk in the form of relative information, which often is more suitable than absolute numbers for making conclusions. The basic importance measures are defined as risk increase factor, risk decrease factor and fractional contribution. An important use of risk increase factor, in TS considerations, is that it classifies the systems and components according to the risk impact of their unavailabilities.

Technical Specifications

The Technical Specifications (TS) are safety rules, approved by the regulatory authority, stipulating the limits and conditions for safe operation of a nuclear power plant.

Test Effectiveness

A set of capabilities which considers the design of hardware, built in test, test equipment and test program. Test effectiveness applied for standby equipment addresses especially the ability of a given test to identify and localize latent faults. Test effectiveness measures include, but are not limited to, fault coverage, fault resolution, mean fault recognition time, mean fault localization time, and diagnostic correctness. In TS considerations this indicator may be defined as the ratio of the number of deficiences discovered at periodic tests to the total number of deficiences, which have contributed to unavailability of equipment.

THE NKA/RAS-400 STEERING COMMITTEE

Lennart Hammar	SKI	Chairman
Torstein Bøhler	Scandpower A/S	
Arne Hedgran	The Royal Institute of Technology	
Hannu Koponen	Finnish Centre for Radiation and Nuclear Safety	
Hans Larsen	Risø National Laboratory	
Bo Liwång	SKI	Coordinator
Franz Marcus	NKA	

LIST OF PARTICIPANTS IN THE NKA/RAS-450 PROJECT

ABB Atom AB Reactor Division S-721 63 Västerås	Göran Ericsson Peter Jacobsson Michael Knochenhauer Lars Tuvesson
Avaplan Oy Kuunsäde 2 DE SF-02210 Espoo	Tuomas Mankamo
SKI **Swedish Nuclear Power Inspectorate** Box 27106 S-102 52 Stockholm	Lennart Carlsson Gunnar Johansson Christer Karlsson Bo Liwång
Studsvik Nuclear Safety and System Analysis S-611 82 Nyköping	Kurt Pörn
TVO **Teollisuuden Voima Oy** SF-27160 Olkiluoto	Mikko Kosonen Antti Piirto Juhani Vanhala
Vattenfall **The Swedish State Power Board** S-162 87 Vällingby	Alf Engqvist Göran Hultqvist Martin Resare
VTT **Technical Research Centre of Finland** SÄH, P.O Box 34 SF-02151 Espoo	Kari Laakso * Antti Lyytikäinen Urho Pulkkinen Kaisa Simola

* Project Leader