IAEA-TECDOC-729

Risk based optimization of technical specifications for operation of nuclear power plants

INTERNATIONAL ATOMIC ENERGY AGENCY IAEA

The IAEA does not normally maintain stocks of reports in this series. However, microfiche copies of these reports can be obtained from

INIS Clearinghouse
International Atomic Energy Agency
Wagramerstrasse 5
P.O. Box 100
A-1400 Vienna, Austria

Orders should be accompanied by prepayment of Austrian Schillings 100,— in the form of a cheque or in the form of IAEA microfiche service coupons which may be ordered separately from the INIS Clearinghouse.

The originating Section of this document in the IAEA was:

Safety Assessment Section
International Atomic Energy Agency
Wagramerstrasse 5
P.O. Box 100
A-1400 Vienna, Austria

RISK BASED OPTIMIZATION OF TECHNICAL SPECIFICATIONS FOR OPERATION OF NUCLEAR POWER PLANTS

IAEA, VIENNA, 1993
IAEA-TECDOC-729
ISSN 1011–4289

Printed by the IAEA in Austria
December 1993

FOREWORD

In recent years more and more countries have applied probabilistic safety assessment (PSA) to optimize various aspects of nuclear power plant operation. Although applications like the optimization of maintenance and of plant backfitting are emerging, one of the most important applications of PSA remains the optimization of operational limits and conditions (technical specifications). Technical specification requirements, such as allowed outage time (AOT) and surveillance test interval (STI), are relatively simple to model in PSA. The effects of changes in technical specifications can be clearly identified. Therefore, plant specific PSA offers a means for the optimization of technical specifications in terms of safety.

The IAEA Technical Committee Meeting on the Use of PSA to Evaluate Nuclear Power Plant Technical Specifications held in June 1990 recommended that a report be prepared detailing relevant methods and providing case studies on the optimization of technical specifications. This report addresses the rationale and discusses the methods and approaches for optimizing technical specifications, summarizes all recent applications of the method and presents case studies detailing two distinctive approaches. One of the case studies was prepared specifically for this TECDOC, while the other was modified especially for the IAEA.

This document was prepared in a series of Consultants Meetings held since 1991. The main author was T. Mankamo of Avaplan Oy, Finland, who prepared several sections and wrote the case study in Appendix II. P. Samanta of Brookhaven National Laboratory, USA, and T. Robert Tjader of the US Nuclear Regulatory Commission prepared various sections, including other case studies, and reviewed the entire report. A. Dykes of Pickard, Lowe and Garrick, USA, S. Deriot of Electricité de France and J. Holmberg of the Technical Research Centre of Finland made valuable comments.

The preparation of this document was carried out partly under the ongoing Nordic research project Safety Evaluation by Use of Living PSA and Safety Indicators NKS/SIK-1 and benefited from the research results of the USNRC project Procedures for Evaluating Technical Specifications. The IAEA project officer for the PSA applications programme is B. Tomic of the Safety Assessment Section, Division of Nuclear Safety.

EDITORIAL NOTE

In preparing this document for press, staff of the IAEA have made up the pages from the original manuscript(s). The views expressed do not necessarily reflect those of the governments of the nominating Member States or of the nominating organizations.

The use of particular designations of countries or territories does not imply any judgement by the publisher, the IAEA, as to the legal status of such countries or territories, of their authorities and institutions or of the delimitation of their boundaries.

The mention of names of specific companies or products (whether or not indicated as registered) does not imply any intention to infringe proprietary rights, nor should it be construed as an endorsement or recommendation on the part of the IAEA.

CONTENTS

1. INTRODUCTION TO IMPROVEMENTS TO TECHNICAL SPECIFICATIONS UTILIZING PSA RELATED METHODS

1.1. BACKGROUND

Technical specifications (TS) for nuclear power plants define the limits and conditions as a way to assure that the plant is operated safely and in a manner which is consistent with the assumptions made in the plant safety analyses. These requirements have been developed, applied and improved in most countries over a period of years, and have, in general, been based on deterministic analysis and engineering judgement as to the amount of margin of conservatism that is necessary. A plant TS is strictly followed during all stages of plant operation and thus it is important that these requirements are stated clearly, capable of being met and consistent from risk considerations.

Experience with plant operation has indicated operational and safety concerns with some of the requirements. Some elements of the requirements may be considered unnecessarily restrictive and may not be beneficial to safety. With the availability of probabilistic safety assessments (PSAs) and reliability analysis, there is a significant interest to improve these requirements. Using these reliability and risk based methods, a number of TS requirements in many countries have already been modified.

To enhance the effectiveness of technical specifications, several studies have been undertaken by the IAEA and many Member States. In June 1990, the IAEA convened a Technical Committee Meeting on the Use of Probabilistic Safety Assessment to Evaluate Nuclear Power Plant Technical Specifications [1] and initiated pilot study programmes. Participation and presentation of technical papers by many countries in this meeting exemplify the significant interest in this area.

1.2. OBJECTIVE OF THE REPORT

The objective of the report is to present an overview of the risk and reliability based approaches (using a PSA) for improving nuclear power plant TS. In that sense, it will provide an information base to the Member States in seeking PSA based applications to enhance the effectiveness of their technical specifications. To achieve this objective, the report discusses the basic objectives and reasons for seeking TS changes, the methods, data requirements and uses of different types of applications, and an overview of different applications that have been completed, including detailed descriptions of selected applications.

1.3. SCOPE AND USE OF THE REPORT

The report gives an overview of the important aspects involved in a PSA based analysis of TS requirements and states the types of application that can be effectively carried out, based on the experience gained so far. The report is not intended to provide detailed guidance to carry out these applications; detailed analyses presented in many of the references can provide the information needed on that aspect.

Technical specifications generally cover the following areas: (a) safety limits and limiting safety system settings; (b) limiting conditions for operation (LCOs) including allowed outage times (AOTs) and action statements; (c) surveillance requirements (SRs) including surveillance test intervals (STIs); (d) design features; and (e) administrative requirements. Based on the operating experience and the PSA applications conducted so far, the primary areas needing improvement are the AOTs (within the LCOs) and the SRs. Accordingly, this document focuses on those aspects. It is estimated that approximately one-third of the modification issues of LCOs and SRs are amenable to analysis using PSA based methods.

In this report TS requirements during the power operation of a nuclear power plant are addressed. TS requirements during other modes of plant operation are different and can be addressed in a similar manner, especially if PSAs for corresponding plant operational modes are available. However, improvements of TS requirements during these modes (other than power operation mode) are not considered within the scope of this report.

The report is expected to be used in several ways. First, it may be used by regulatory authorities and nuclear utilities to identify their need for using a PSA to plan improvement of the TS. Second, it will provide guidance to the individuals involved in carrying out these applications in terms of the methodology, data needs, and availability of information; and finally, it can provide guidance to those involved in developing PSAs on the applications that can be planned so that PSAs can be developed or extended accordingly.

1.4. OUTLINE OF THE REPORT

Following the introduction, Section 2 presents the basic objectives and reasons in seeking PSA based applications for improving TS. The section also defines the types of applications defined in the report. Section 3 presents a discussion of the risk related definitions, methodology, data needs, and the method chosen in problem solving. An overview of important applications is presented in Section 4. Section 5 summarizes the concluding remarks.

The appendices present additional detailed information. Appendix I presents a detailed analysis of the test strategy for a reactor protection system. Appendix II presents a detailed analysis of AOT issues in a residual heat removal (RHR) system for a boiling water reactor (BWR) plant. Definitions and a list of abbreviations are included at the end of the report.

2. PSA APPLICATIONS TO IMPROVE TECHNICAL SPECIFICATIONS

This section focuses on the different types of PSA based applications that can be performed to improve nuclear power plant TS and gives a broad overview of the areas of applications. The objectives in PSA based applications and the reasons for seeking the TS changes are defined, and the types of applications that have been carried out to improve aspects of TS are briefly discussed. The following sections present the methodology, data requirements and the details of specific applications.

2.1. OBJECTIVES IN PSA BASED APPLICATIONS

The basic objectives in a PSA based analysis and modification of TS requirements can be summarized as follows:

- To assure that any changes in TS do not compromise the basic intent of TS in assuring margins of safety during normal and accident conditions;
- To obtain a quantitative assessment of the risk impact of the changes and to provide a quantitative basis as a justification; and
- To make it acceptable and defensible to regulatory authorities whose approval is usually required.

These items are discussed further below.

Technical specifications are primarily designed to assure safe operation of a nuclear power plant in all modes of operation and particularly, in case of adverse conditions when equipment which must operate to prevent or mitigate the consequences of an accident will be capable of performing its function when called upon. Any changes in technical specifications must, thus, assure that their basic intent is not compromised.

A probabilistic safety assessment (PSA) of a nuclear power plant provides a quantitative representation of the safety level of the plant through assessment of the probability of accidents and their consequences. One of the factors that influences or is incorporated in this modelling and quantification process is the TS requirements. For example, safety system component unavailabilities, which are inputs to a PSA quantification process, are defined in terms of STIs and maintenance unavailabilities. STIs are usually defined within the surveillance requirements (SRs) and maintenance unavailabilities are influenced by (or reflections of) AOTs defined in LCOs. Thus, changes in the TS requirements can be assessed quantitatively using a PSA.

This ability to quantitatively assess the impact of changes in TS requirements is significant. Admittedly, certain aspects, which are discussed later, are to be handled qualitatively, and there are areas of uncertainty in the quantitative evaluation. Nevertheless, the quantitative assessment of the changes can be used to demonstrate whether the risk impact of the change is acceptable or not. As will be discussed later, many TS requirements can be changed without decreasing safety, i.e. with minimal or negligible increase in the risk level. At the same time, many requirements where changes can improve safety can be strengthened or areas that are previously undefined, but now known to be risk relevant, can be appropriately defined.

Typically, in all countries any changes to TS will require approval of regulatory authorities. Without the use of a defensible analysis of the requested change, such an approval is unlikely. Use of PSA to quantitatively demonstrate that the risk impact is acceptable becomes a defensible argument to justify such changes. However, as discussed later in this report, proper procedures shall be followed and appropriate evaluations must be performed.

2.2. CHANGES IN TS

The reasons for seeking changes in TS are many and may depend on a particular type of TS requirement. However, experience with TS and the changes that have been accepted in different countries or are being contemplated, identify major problem areas and reasons for seeking these changes. The primary reasons for seeking these changes can be summarized as follows:

- Experience with plant operation indicates that many requirements are unnecessarily restrictive and may not be beneficial to safety;
- The requirements are not consistent with risk; thus, the emphasis of TS is not in proportion with risk implication;
- Actions required by TS are not justified on risk arguments; and
- The requirements are unnecessarily burdensome and may be diverting attention away from safety significant aspects.

The following discussions clarify these reasons and can be used to identify which of these conditions apply to a specific plant to initiate a risk based analysis to seek appropriate changes.

TS requirements were originally based on deterministic analyses and engineering judgements. Experience from operating nuclear power plants shows that in many cases the requirement may be unnecessarily restrictive or not conducive to safety, and thus changes may be desirable. For example,

the limiting conditions for operation (LCOs) define allowed outage times (AOTs) to complete repair of inoperable components. If the repair cannot be completed in the prescribed time, the plant is typically required to be brought to the shutdown state. However, the existing AOT, in some cases, is not adequate to complete the types of repair that are necessary to be performed. An increase in the AOT to complete repair may be more desirable compared to the change in mode of plant operation (transferring to shutdown mode).

PSA based analysis of TS requirements has shown that the risk implication of the requirements vary significantly, i.e. the risk impact of one requirement may be orders of magnitude different from others. It may be interpreted that many requirements whose risk impacts are minimal, or are orders of magnitude lower than others, are unnecessary or need modification to make them more risk effective. One reason for TS modification may be to make requirements more consistent in a risk scale, whereby the effectiveness of the requirements are improved. This would mean both relaxation of many requirements and, also, strengthening of others.

Certain aspects of TS are not clearly defined. Many of these aspects may have significant risk implications and PSAs may be used to define the requirements. For example, in the USA, AOTs were originally intended to be used for performing corrective maintenance; but with plant experiences it is now evident that performing routine preventive maintenance can improve the reliability of components, which is an important aspect in assuring safety levels of nuclear power plants. Thus, allowing preventive maintenance during power operation appears desirable. But care must be taken to assure that the risk due to the unavailability of the component is controlled. PSAs can be used to identify such usage of TS requirements which are not clearly defined in the existing technical specifications.

TS requirements should be coherent, i.e. they should not result in increased risk, as opposed to providing alternate, safer options. PSA based evaluations can be performed to identify and modify such requirements, whereby the action required by the TS are justified on risk arguments. An example of such a TS action statement is the immediate requirement for a shutdown in the case of multiple failures in standby service water (SSW) and residual heat removal (RHR) systems of a BWR plant, or in the auxiliary feedwater system (AFWS), RHR system or component cooling water (CCW) system of a PWR plant. Typically, in case of multiple failures of redundant trains, where the risk of continued operations was judged to be high, the plant is required to be moved to the shutdown state, where the risk was earlier considered to be lower. However, since these systems are also required in transferring the plant to the shutdown state, the risk of shutdown may be higher than continued operation over normal repair times of one day or shorter. Such conditions may also apply for other systems not involved in transferring the plant to the shutdown state. For example, the high pressure injection system (HPIS) may be disabled from automatic operation, which makes the shutdown state vulnerable to spontaneous leakages as well as to flow diversification errors. PSA based evaluation can be performed to define appropriate risk effective action requirements with consideration of comparative risk between continued operation and plant shutdown.

Modifications of TS can also be justified to improve resource allocation, which results in improved safety. Current requirements may at time be burdensome; the number of surveillances required during power operation is considered by many to be excessive and diverting resources away from safety significant aspects. As discussed before, many of the requirements may have a minimal risk implication. The requirements may be redefined whereby resource allocation becomes appropriate (in proportion with risk implication) without affecting the risk level of the plant.

2.3. TYPES OF PSA APPLICATIONS TO MODIFY TS

In this section the different types of PSA based applications to improve TS are defined and the reasons for seeking these modifications are described.

Modifications to AOT requirements

Experience indicates that in many cases AOTs are unnecessarily restrictive and, in some other cases, they may not be consistent with risk considerations. These AOTs can be modified to streamline plant operations and to avoid unnecessary plant shutdown without incurring undue risk.

PSAs can be used to consistently evaluate the safety influence of specific AOTs to assess:

- The increased risk during operation due to increased AOTs; to justify changes to AOTs when the risk impact is minimal;

- The relative risk between shutdown and continued operation especially in case of multiple failure situations in safety systems that are required during shutdown; to determine a reasonable AOT to minimize the overall contribution of risk during operation and the risk of shutdown in such failure situations;

- The risk impact of continuing operations for equipment which can only be repaired when the plant is in a shutdown state.

Experience gained from PSA based applications so far indicates that a number of AOT requirements can be modified to obtain operational flexibility. Section 4 presents examples of AOT modifications justified using probabilistic methods and desired from a plant operation viewpoint.

Modifications to surveillance requirements

Surveillance requirements (SRs) for safety system components are intended to detect any failures so that the components are repaired and remain available for accident situations. SRs cover the type of surveillance test, the frequency of surveillance or, in other words, surveillance test intervals (STIs) and surveillance test placements, i.e. the strategy of performing test of one train in relation to the test of a redundant train. The reasons for modifying SRs can be summarized as follows:

- The frequency of the tests required appears unnecessary and can be reduced both from the safety and operational standpoints;

- The test method might be refined to better cover different failure modes or reduce unnecessary wear; the test frequency might be adjusted to balance adverse effects of testing with the benefit of detecting failures;

- The test procedure might be improved to reduce test related plant transients, or the test can be moved from the power cycle to the shutdown period;

- Staggered tests over redundant trains can be rearranged for operational benefits or for enhanced control of systematic errors/common cause failures.

PSA based applications have been performed to demonstrate that the incremental risk due to increase in test intervals can be minimal and, in certain cases, the benefits of test placements in reducing common cause contributions can be substantial. Optimization of test intervals considering test caused transients and test caused wear has also been demonstrated to seek a balanced requirement.

Use of AOTs for preventive maintenance during power cycle

The AOTs were primarily designed for corrective maintenance to be performed in case of failures of safety system components. It is now realized that preventive maintenance (PM) plays a very important role in assuring availability of components contributing to safety. With appropriate care, the concept of AOT can be broadened to include PM during power operation.

PSA based applications can be used to optimize PM in the following ways:

- Scheduling PM during a power cycle that has small risk impact; this could better balance workloads during refuelling outage;

- Modification of PM which has minimal risk impact, i.e. the instantaneous risk and the average risk contribution are minimal;

- PM activities across different systems/subsystems can be combined to both minimize the risk impact and to obtain operational flexibility;

- The plant operating state (power operation, cold shutdown, etc.) which has a minimal risk impact due to the equipment outage for PM can be identified.

The PSA application for PM scheduling presented in Section 4 assesses the risk due to the unavailability of the component for performing the PM, but does not address the benefit in terms of improved component performance due to the PM. In this application, the scheduling of PM, and the PM duration is assessed to contribute small risk to justify use of TS for such activities.

Plantwide TS approach using a living PSA

A broad application for PSA in defining TS will be to use a 'living PSA', that is maintained and updated to reflect any plant changes, to prescribe requirements as a replacement for current TS requirements. In such an approach, within a general guideline for controlling risk and acceptable actions, PSA analysis is used in a routine basis to provide requirements for the situations that arise in the plant. Availability of fast running computer tools and progress in PSA development provide an opportunity for such an application. In fact, the Essential System Status Monitoring (ESSM), in operation at the Heysham plant in the United Kingdom, can be considered as such a system for TS application [2]. One can argue that ESSM is a tool for approximately monitoring the risk level in a plant to make judgements about test/maintenance activities and cannot be considered a 'living PSA'. Without addressing the validity of the concept in ESSM, one can note that the system, using quantitative risk assessment in the background, defines corrective maintenance durations during power operation and scheduling of surveillance tests and preventive maintenance. Other countries are exploring such concepts.

Notwithstanding many difficulties and implementation issues that may need to be resolved to move towards such a risk monitoring and configuration control system, as opposed to current deterministic approaches, there are many advantages that have resulted in significant interest in such a concept. The interesting attributes of such an approach can be summarized as follows:

(1) The risk monitoring and configuration control system will require actions consistent with risk implication providing full operational flexibility in areas unimportant to risk;

(2) Risk significant aspects, for example simultaneous outages of multiple components, can be better controlled. This may mean better control of operational events with significant risk implication;

(3) The effectiveness of TS requirements can be assessed through evaluation of the action required and the ability in controlling risk significant events during plant operation; and

(4) The system can provide specific guidance to the operators in failure situations, instead of requiring a shutdown. These guidances may be directed towards assuring availability of redundant equipment whereby a successful operation in case of an accident becomes likely. The system can also inform the operating staff about any violations of deterministic rules that should be followed.

3. OVERVIEW OF METHODS, DATA AND APPLICATION ISSUES

This section presents an overview of the methods used for TS applications, the data needed for such applications, and the prerequisites for efficient implementation of these applications. In presenting this overview, the plant TS states and the basic related risk concepts are defined.

3.1. PLANT TS STATES AND BASIC RISK CONCEPTS

3.1.1. Baseline and LCO states

The principal plant states, as relevant to TS considerations, and associated risk concepts are illustrated by a state model and a schematic risk level diagram in Figs 3.1 and 3.2 [3].

The baseline state is used for the normal power operation state of the plant, where the safety systems are in their normal state.

For most safety systems the baseline state means standby condition without any components known to be inoperable. The latent failures of these components are only detected by surveillance tests, or at demand situations. Their likelihood is the prime ingredient of the system failure probability, if a demand occurs during the baseline state. It should be noted that many standby components also need to operate after startup, over a mission period, which is specific per demand. The unreliability over the mission period also contributes to the overall system failure probability in the baseline state.

For some safety systems, or components, the normal state may also be the operating state. Consequently, failures of those components are usually directly revealed by instrumentation or process symptoms. If an initiating event occurs during the baseline state, the instantaneous unavailability is initially zero for these systems, but these systems may fail during the mission period. Therefore, the overall failure probability per demand is non-zero also for these kinds of systems or components.

Disconnection for testing or maintenance, and detection of critical faults in surveillance testing of standby components, or failure to run of operating components, etc., are thus deviations from the baseline state and mean entering specific LCO states, as shown in Fig. 3.1.

Most LCO states are concerned with single component repairs or maintenance downtime, and multiple failures of redundant components (most likely CCFs) within one system. It is important to separate the situations with overlapping unavailability in other safety systems. Many such combinations are risk significant because the remaining safety system configurations may imply significant increase in the risk level. Such combination events should be considered explicit disjoint LCO cases.

It needs to be emphasized that Fig. 3.1 is a schematic illustration only. The more complex state/transition scenarios for combination events are not shown. Also different shutdown modes or progression while shutting down and starting up the plant are not shown in this conceptual diagram.

3.1.2. Risk level variation over plant TS states

The risk level is basically measured in terms of the instantaneous risk level, i.e. probability of accident per unit of time. In a Level 1 PSA, the frequency of reactor core damage is calculated and usually expressed in units of [/year]. (Extending the risk based approach to Level 2 or 3 PSA is not considered here.) Basically, the risk level is a time dependent variable. First of all, it fluctuates along with the test and switchover scheme of safety system components. Usually this fluctuation of the risk level is relatively small within the baseline or a specific TS state, in comparison with the risk level

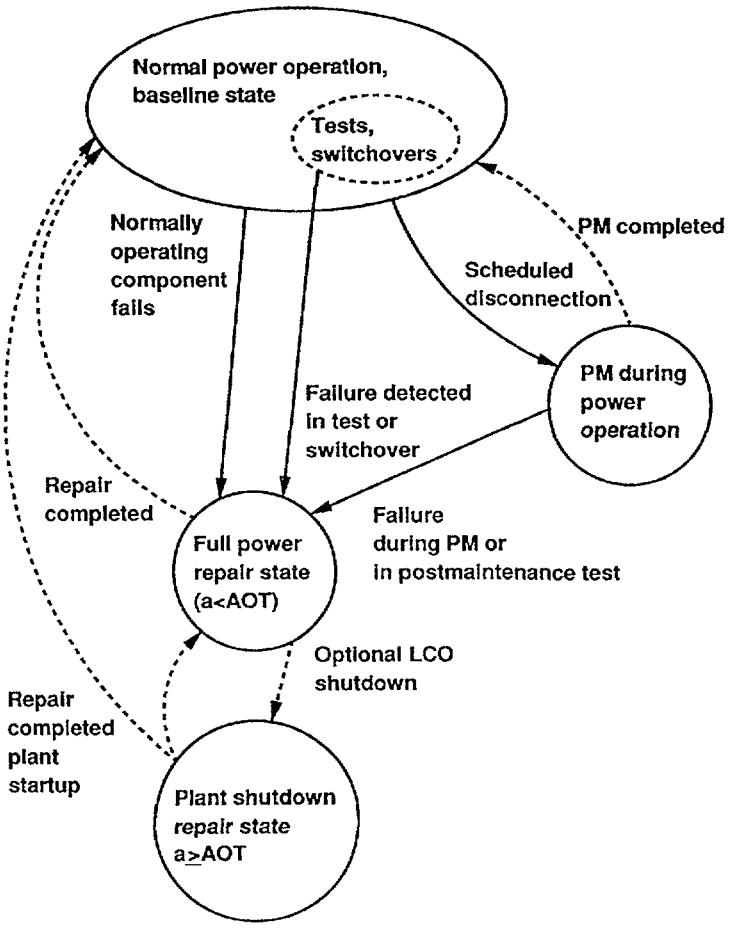


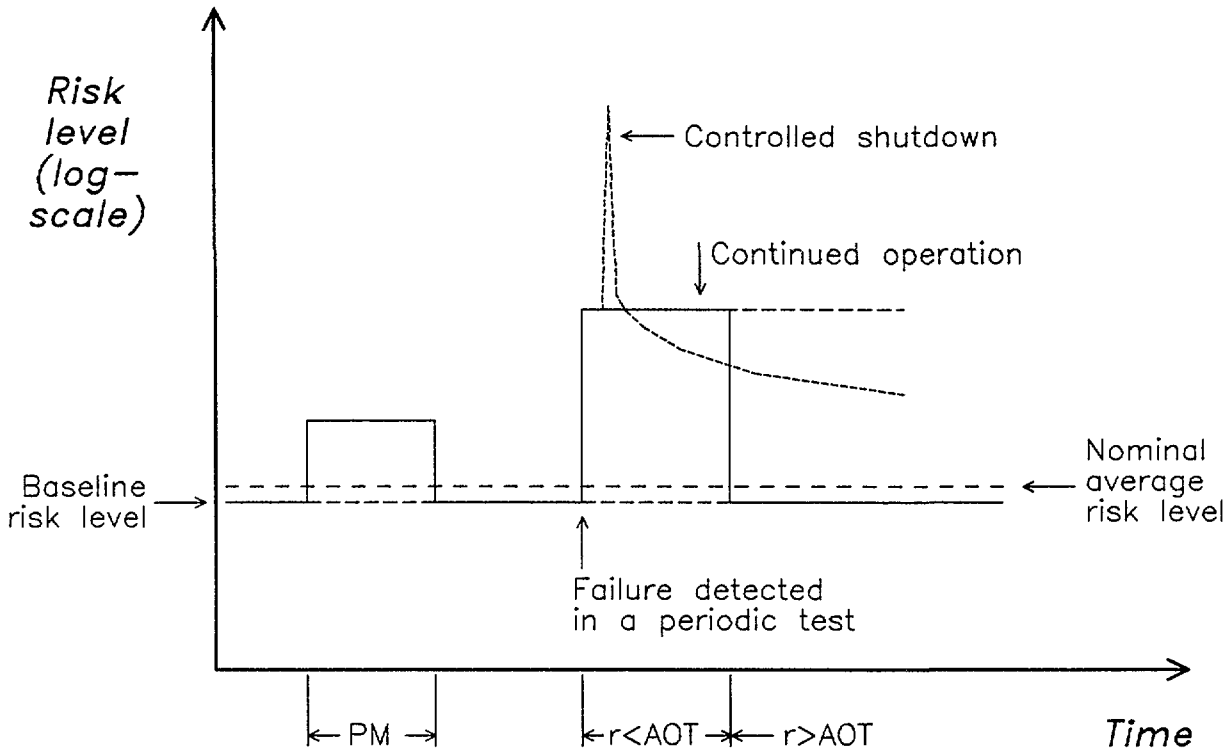
FIG. 3.1. State model of the baseline and LCO states.

difference of the baseline and LCO states. Hence, fine details in time dependence is often not explicitly calculated, but instead, the average risk level within a given state is calculated and considered adequate for TS evaluations. Correspondingly, the risk levels are drawn constant in the schematic presentation in Fig. 3.2.

When considering the risk of an LCO shutdown of the plant, the actual time dependence cannot be omitted. First, there is a risk peak associated with the possible disturbance transients during power reduction and reactor cooldown phases, as shown in Fig. 3.2. Also, the failure to start systems needed in the shutdown state, such as residual heat removal systems, contribute to this risk of changing plant state. Second, after shutdown, the instantaneous risk level decreases along with the diminishing decay heat level, because this allows more time for recovery in case a critical failure combination occurs later in the zero power state. This behaviour is important to take into account, because it is one of the prime motivations for the LCO shutdown. These aspects will be discussed in more detail in Appendix II in connection with the TVO/RHR study.

3.1.3. Risk measures and criteria for TS considerations

All exceptions from the baseline state, both detected features or intentional maintenance disconnections, mean temporary increase in the plant risk level, as illustrated in Fig. 3.2. Each of



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

FIG. 3.2. Principal risk definitions when considering PM and AOT situations during the power operation state.

these excursions, including also combination events, should be covered by an AOT, shutdown requirement or some flexible rule. In order to measure the risk importance of a deviation state, the following three variables need to be considered in parallel:

(1) Instantaneous risk level. Both the relative increase from the baseline, and the absolute level need to be considered.

(2) Expected risk over repair downtime or maintenance period, i.e. the integrated risk over the duration time. For failure situations, the expected risk over the repair time in the full power state should be compared with the risk of the plant shutdown alternative in order to make repairs in the zero power state. Besides this comparison, the expected risk over one downtime can be compared with the average annual risk to justify a flexible AOTs. In general, the risk of each single downtime should be a small fraction of the average annual risk in order to be able to limit the cumulative risk of successive downtimes.

(3) Addition in the long term average risk, i.e. the product of the occurrence rate and expected risk per single occurrence (of a specific failure or maintenance disconnection). This so-called delta risk includes a control over occurrence rate, while the other two measures discussed above are

situation specific and do not address the frequency of occurrence. The delta risk is usually small for single components, mostly less than one percent of the average risk level. However, the delta risk summed over all components covered by AOTs, and an eventual PM scheme in power operation state, may become significant and need to be especially considered against acceptability criteria.

The role and priority of the three principal measures in making conclusions varies from case to case, as will be discussed in connection to reviewing recent applications in Section 4. A more comprehensive discussion of the risk measures and acceptance criteria, applicable to TS considerations, is presented in Refs [4–6].

3.2. BASIC PSA BASED APPROACHES

In performing PSA based applications for modifications of TS requirements, basically a quantitative assessment of the risk impact of the modified requirement(s) is being made. However, all aspects cannot be addressed quantitatively. The intent is to quantitatively address those aspects that are dominant risk contributors and to present qualitative considerations for others. Also, because of the uncertainties in the PSA methodology and due to the lack of knowledge for parameters relating to the changed requirement, sensitivity evaluations are necessary to be performed to study the range of the risk impact. Based on the assessed risk impact, a decision is required on whether the change being evaluated is justified. This section presents a brief discussion on these items for different types of application.

3.2.1. Methodology considerations for AOT evaluations

Quantitative and qualitative evaluations

The allowed outage time (AOT) of a standby safety system component defines the time period the component may be unavailable during power operation before a plant shutdown is required. In deciding on an AOT, one needs to make a judgement whether shutdown is the safer alternative and if transition to the shutdown state is feasible without undue risk given the failure situation. In many cases, the risk of continuing operation is significantly higher than the risk of transition to the shutdown state to complete repair. Many of the applications can be performed focusing on the risk of continued power operation, given a failure situation. First, the risk considerations in these types of applications are discussed, followed by AOT evaluations that require consideration of LCO/shutdown related risk.

For a risk based evaluation, the primary quantitative assessment focuses on the risk impact due to the AOT period. As mentioned previously, this requires assessment of three types of risks: (i) instantaneous (increased) risk level when the AOT component is in the failed or repair state, (ii) the integrated risk over an AOT or downtime period, and (iii) the expected risk addition over a long period, taking into account the frequency of maintenance performed on the component.

As discussed, the same AOT is generally used both for scheduled preventive maintenance (PM) or unscheduled corrective maintenance (CM). However, in some countries (e.g. Sweden and Finland) AOTs for scheduled PM are different than that for unscheduled CM. The considerations and criteria for these two uses of AOTs are slightly different and should be addressed in a risk based evaluation. The details of these applications can be observed in the summary of the applications presented in Section 4 and in the associated references. The general methodological considerations are discussed here.

A more challenging extension becomes necessary if LCO/shutdown related risk is significant for the AOT issue. Recent experience shows that at least in the case of RHR and other systems specifically needed in a zero power state (e.g. shutdown/standby service water systems) the

LCO/shutdown related risk is substantial and needs to be considered for proper handling of the AOT issue. Availability of a zero power PSA extension (often called a shutdown or refuelling PSA) becomes extremely useful in conducting these types of AOT evaluations.

Special efforts may still be needed in order to incorporate the disturbance transient risk related to a controlled shutdown during the power reduction and reactor cooldown phases which may not be covered either by the full power or low power PSA. Another special item is the safety credit of diminishing the decay heat level after successfully entering the zero power state and stable shutdown cooling — which is the prime justification of an LCO/shutdown — and should be realistically considered as it allows longer times for recovery if critical failures occur later during the shutdown cooling mission. This may necessitate closer thermohydraulic calculations for the process behaviour in different accident scenarios. The TVO/RHR study, presented in Appendix II, represents a full scope pilot application on this type of risk based AOT consideration.

The assessment of the AOT risk impact can typically be performed at the core damage frequency level, which requires a Level 1 PSA. When a Level 1 PSA is not available, system/function level evaluation using a system/function fault tree model for quantifying system/function unavailability can be used. But a system/function level evaluation requires additional caution. Experience has shown that drawing definite conclusions from system/function level evaluations may be difficult [7].

In deciding on an extended AOT, one motivation is to provide adequate repair times which will result in improved component performance, i.e. requiring less repairs or corrective maintenance in the long run. This aspect can be discussed qualitatively if considered applicable for the component for which AOT is being modified.

Sensitivity analyses

Sensitivity analyses should be performed for the important data and modelling uncertainties:

- For a given AOT, the average repair time for the component may be significantly lower. Sensitivity analyses may be performed to assess the risk impact covering the average repair time over the entire AOT period. In many cases, the use of entire AOT in the analysis will be conservative, but still may justify the extension;

- If the AOT component is a contributor to common cause failures, then sensitivity analyses should be performed assuming different increased failure rate for the redundant component. When test of the redundant component is not performed before a repair is initiated then, because of common cause failure potential, there may be increased likelihood of failure of the redundant component, which is addressed in this analysis;

- If as part of the AOT extension any additional plant actions, for example testing of other components, reduced/increased PM, are being included, then sensitivity analyses should address the impact of these actions;

- For cases where the shutdown risk is significant, sensitivity analyses are required to address (a) the uncertainty in the transient data during transfer to the shutdown mode, (b) the need for additional testing when one or more failure is detected, and (c) the alternatives available for moving the plant from the operational state to the shutdown state.

3.2.2. Methodology considerations for SRs

In performing a risk based evaluation of surveillance requirements–surveillance test intervals (STIs) and surveillance test arrangements or test strategy, the risk impact of altering these requirements can be quantified. In using PSAs for these evaluations one must assure that PSAs include

appropriate component level models. PSA models in many cases use a time independent or average component unavailability model, which needs to be modified to include the test interval for studying the impact of surveillance requirements.

The issues associated with risk analyses of surveillance requirements are extensive; and all aspects cannot be addressed using quantitative models. This is because there are practical and technical aspects which are either difficult to quantify or for which satisfactory quantitative models have not yet been developed. In some cases, data are not available to justify a specific quantitative model. Here, considering these limitations, we have defined both quantitative and qualitative aspects of the analyses. Conceivably, data and models will be available in the future for some of the items addressed within qualitative analyses. There are examples where in selective cases these items are addressed quantitatively.

Quantitative analyses

For assessing the risk impact of surveillance requirements, the following risk contributors should be addressed quantitatively:

(a) Risk contribution associated with failures between tests: this risk is due to the fact that for a standby equipment any failure occurring during the standby period will persist until the next test or next time the equipment is required to function. Thus, if such a failure occurs, the equipment is inoperable for a period of time that on the average is equal to one half the test period (assuming the failure is likely to occur anytime during the test period). Detecting this risk is the primary motivation for performing surveillance tests.

In this analysis it is assumed that the component failure rate is constant and will remain unaffected by the changes in the test frequency. If it is judged that changes in STI can increase the component failure rate, then a more detailed evaluation is necessary.

(b) Risk contribution associated with the component being unavailable during the test: this contribution needs to be considered when the test requires that the component be reconfigured away from the safe position for the test. This contribution, in many cases, may be small and may be neglected in PSA models.

(c) Risk contribution associated with human error of restoration following test: the probability of a human error, disabling a component, can be an important contributor and is typically, included in PSA models. The probability of these test associated human errors are assumed to be constant, i.e. independent of number of tests, in a PSA. With this assumption, changing of STI is not affected by this contribution. However, this aspect is important and should be assessed in modifying SRs.

(d) Risk contribution associated with the test arrangements or test strategy: the placement of one test relative to another can significantly affect both the risk due to common cause failures and between test risk contribution of the system (containing redundant components). Addressing this aspect requires modelling the time dependent portion of individual component unavailability and the common cause contribution. Appendix A presents a detailed evaluation of consideration of test strategy in defining surveillance requirements focusing on a system level evaluation.

(e) Risk contribution associated with failures that can be associated directly with the testing process: Classification as 'test caused' requires that the failure be directly associated with actions to accomplish the test. Failures that could occur also during a safety related demand are excluded unless it can be shown that it is a time related random failure associated with the running phase of system operation. In many cases, data may not be available that separate those failures that are directly associated with the testing process. Inclusion of this contribution may be necessary if the extension obtained otherwise is not sufficient, or if this is the primary reason for seeking the extension.

Qualitative evaluations

A number of other risk contributors, discussed below, should at least be addressed qualitatively. Depending on a particular surveillance test and the type of modification desired, one or more of these may need to be addressed in detail, using qualitative models.

(a) Test caused transients: the probability of test caused transients is usually not treated separately in a PSA. These types of transients are assumed to be included in the initiating event frequency. Most tests do not cause any transients and the contribution of this aspect can be qualitatively addressed to be negligible. In other cases, for example main steam isolation valve (MSIV) testing or turbine bypass valve testing, such contributions may not be negligible and should at least be discussed qualitatively. Quantitative analyses [8] may be performed to obtain more precise STIs.

(b) Test caused degradation: this contribution relates to degradation in component performance due to the increasing number of test demands and can often be dismissed by qualitative considerations as decreasing when the test interval is increasing. Emergency diesel generator and auxiliary feedwater pumps are commonly considered to degrade due to test demands. If the effect of test caused degradation is considered to be significant, sensitivity analyses can be performed using engineering judgements.

(c) Deficiency in testing: qualitative evaluations should be performed to identify whether the failure modes critical to risk are being identified by the test. One must assure that the test is able to detect with high efficiency the failure modes of interest from risk considerations. If deemed important, the influence of test effectiveness can be evaluated by a dedicated model consideration, and using engineering judgements.

The risk impact of a surveillance test can be evaluated at the core damage frequency level when a Level 1 PSA is available. When studying test arrangement or test strategy within one system, system/function level evaluations may be adequate. When evaluating the impact of changes in surveillance requirement of multiple systems, the individual analyses cannot be simply combined to obtain the overall impact. PSA evaluation with modified STIs for the components in question should be performed, otherwise the interaction term, i.e. the product terms containing the increased unavailability of two components with increased test interval, will be neglected.

Sensitivity analyses

The quantitative analyses of surveillance requirements should be supplemented with sensitivity analyses addressing the relevant aspects. Desirable sensitivity analyses can address one or more of the following:

(a) Sensitivity with respect to time independent (demand) and time dependent (standby time) contribution to component unavailability. A component unavailability in a simple form can be represented as a sum of time independent and time dependent contribution [26]. However, this separation is usually not clearly known. But, when the time independent portion is larger, the relative benefit of a surveillance test in detecting the failure is smaller. This aspect, should thus be addressed in a sensitivity analysis to show how the decision on STI change would be affected by this separation.

(b) Sensitivity with respect to common cause failure contribution. The common cause contribution may significantly influence the surveillance test needs and surveillance test arrangements for redundant subsystems. A sensitivity analysis with respect to common cause failure rates, for components judged to be contributors to common cause failures, should be presented when justifying any changes to test intervals and test arrangements of these components.

(c) Sensitivity analysis with respect to alternate test schemes. If different test strategies may be followed, then sensitivity analyses should be performed to assess the impact of individual strategies. Approximate evaluation using a PSA model, which averages STI test scheme influence, is often considered adequate.

3.2.3. Criteria consideration

In accepting a modification to a TS requirement based on quantitative risk evaluation, numerical criteria may be required to decide the acceptable change. In general, the numerical criteria should be considered along with other practical, engineering considerations and sensitivity analyses. The criteria requirements may vary from one Member State to another.

In principle, any increase in risk associated with TS changes should be minimal or negligible. In cases where trade-offs are relevant, the need for criteria does not exist, the net change in risk can be demonstrated to be negligible or even negative, i.e. the risk level is expected to improve. Trade-off consideration may involve extending a number of AOTs or STIs in exchange for reducing a smaller number of AOTs/STIs. Another type of trade-off may involve increasing the test interval in return for a specific test arrangement to be followed. Also, for evaluating AOTs when the risk of shutdown is significant, comparison of two alternatives, continued operation and shutdown, may be used (see Appendix II).

3.3. DATA NEEDS FOR TS STUDIES

This section focuses on special data needs for a risk based evaluation of TS requirements. These data are in addition to the data available as part of the PSA study. It must be emphasized that, if planned early, many of the data discussed below can be collected during the PSA data collection process without much additional resources. At the same time, all the items are not necessary to initiate a TS evaluation process. As discussed previously, uncertainties in data can, to some extent, be handled through sensitivity analyses. In general, use of plant specific data, when available, is strongly encouraged.

3.3.1. Data needs for surveillance requirements

The data needs for analyses of surveillance requirements can be summarized as follows:

- List of the components being tested; any component realigned from the safety position during a test; duration of the test; and the test frequency recommended by the manufacturer. If specific information is not available, then approximate data can be used.

- The efficiency of the test, i.e. the failure modes detected by the test (in regard to components, support system interfaces, etc.). Bounding assumption can be made if detailed information is resource consuming to obtain.

- Surveillances that have potential for negative effects, i.e. may cause disturbances including potential for introducing plant transients, or may cause unnecessary wear of the equipment.

- The failures observed for a component, during a surveillance test or otherwise, may need to be evaluated to determine whether the failure mechanism is demand or standby time related. Separation of failure data into these categories may require detailed information and/or engineering judgement. Obtaining plant specific data on this separation may be difficult; alternatively, data pooled over a large number of components may be used, supplemented by sensitivity analyses.

The detailed information requirement discussed above is needed for a precise evaluation of the surveillance requirements which may be performed for risk significant components. However, obtaining this kind of detailed information on a plant specific basis may require a careful evaluation and interpretation of operating experience. Usually, the available failure classifications and short event descriptions from information bases may not be sufficient. Additional details need to be discussed with the plant staff in order to properly interpret the information content. A detailed analysis studying surveillance consideration for DGs is presented in [9], with a summary description in Section 4.

3.3.2. Data needs for analyses of allowed outage time and preventive maintenance scheduling during power operation

A screening evaluation of AOT risk impacts can be initiated with the data compiled during the Level 1 PSA. The data needs for more detailed evaluation, particularly when the relative risk of shutting down is also considered, are summarized below:

- Distribution of repair times of components: this is needed to judge whether adequate AOT is being provided for completion of repair. This distribution can also be used to estimate the expected risk for a given AOT. The distribution of repair time may shift when an AOT is being changed. However, information about such an influence on the distribution is not expected to be available when the AOT modification is being studied. The repair time distribution which is relevant for the existing AOT can be used assuming that the same repair policy will be followed.

- Frequency of maintenance: the frequency of maintenance performed on a component may be a factor of 3 to 10 higher than the failure frequency [10]. Since AOTs are used for all such maintenance, the frequency of maintenance should be used in estimating the average long term risk due to AOT.

- Schedule for performing PM: maintenance scheduling used by the plant, defining the situations when multiple equipment or system trains may be taken down for PM.

- Restoration probabilities for components in PM: during a component outage for PM, if a component is requested to function, it may be possible in certain situations to restore the component within a reasonable time. If bounding evaluations show that early restoration is not likely, then the component will be considered fully unavailable. If detailed evaluations considering restoration possibilities are to be performed, then data defining restoration probabilities should be obtained.

For the analysis of AOT considering risk of shutdown, the following additional data are needed:

- Realistic estimates of likelihood of multiple failures, i.e. CCF data for component/systems required for shutdown;

- Likelihood of LCO/shutdown related disturbance transients during power reduction/reactor cooldown;

- Time margin for recovery, i.e. as allowed by suppression pool heatup in a boiling water reactor, level reduction in steam generators in a pressurized water reactor, reactor coolant boil-off down to a critical level, warmup in case of failure of component/room cooling, etc.; this is related to the evaluation of safety credit from entering a stable shutdown state as discussed in Section 3.2;

- Disabling activation signals, or whole safety systems, from automatic operation in shutdown states; special system configuration arrangements and operator actions while changing between different operation modes.

These special data needs are discussed in more detail in Appendix II, based on the experience and insights from the TVO/RHR study.

3.4. CONSIDERATIONS IN THE ANALYSIS OF TS PROBLEMS AND MODIFICATIONS

In analysing a TS problem, careful consideration must be given to a number of aspects so that the effort remains focused and the resources required are manageable. Usually, available resources are limited and, accordingly, the TS problem to be analysed and the scope of the analyses should be appropriately defined. This is important since through appropriate problem selection and focusing on a limited area, at least limited improvement will be achieved. Also, limited modification in many cases may be justified, which could be sufficient, without performing a detailed analysis that may provide a larger flexibility but will require significant resources.

In the early states, the following aspects must be considered:

(a) The TS problem area to be analysed should have sufficient justification for seeking a change;
(b) There must be realistic alternatives that can be analysed; and
(c) The database needed to support the analyses should be accessible without significant effort.

The justification needed for seeking a change may be similar to that presented earlier in this document. For a specific application dealing with AOT modification, plant may have data showing that repair times needed were large and AOT modification can avoid unnecessary shutdown or that the requirement appears inconsistent in comparison to others and may reduce burden during operation. Similarly, surveillance can be shown to be burdensome in that it requires reduction of plant power level or that a test has detected few or no failures. Typically, for AOT and STI requirements, the changes required can be made realistic by limiting the amount of extension requested. The database requirements, as defined in the previous section, must be available in some processed form. If the database needs to be developed through searching basic raw data, then the required effort can become significant. Usually, if the database used in the PSA is maintained carefully, it will provide a good starting data source for TS application. If plant specific data cannot be obtained, then generic data can relatively easily be located. In general, TS problem areas that have been addressed by others previously, and are available, would be a valuable source of information.

During the analyses stage, the following aspects should be considered:

(a) The existing PSA should be used to the extent possible;
(b) Practical constraints which may limit the possible solutions should be considered early;
(c) Aspects that are to be qualitatively addressed and those to be treated quantitatively should be clearly defined;
(d) Sensitivity analyses that will need to be performed should be defined so that the data collection effort can be appropriately identified.

The use of existing PSA is justified not only because it can save the additional resources for the TS analyses, but also because it can provide the basis for the review and for future updating of analyses for the specific TS requirements. Typically, the PSAs are reviewed and the use of the PSA will shorten the review requirement of the TS modification.

A solution being analysed should consider practical considerations. In fact, a selected set of practical alternatives that may be acceptable should be defined early so that the analyses can focus on these aspects. For example, in studying test strategy for redundant components, the alternatives that are feasible from consideration of available test personnel should be considered. This may require abandoning the option that is most risk effective from PSA/reliability analyses but cumbersome to implement.

An early determination of aspects to be handled quantitatively versus those to be addressed qualitatively will streamline the application. Discussions earlier in the section along with the availability of data should be used to make this judgement. However, care should be taken that the analysis is not overly qualitative, which may limit the improvement that can be justified. For example, in seeking extensions to STIs, as discussed, a number of items can be addressed qualitatively and still a sufficient extension can be justified.

Due to the difficulty in obtaining plant specific data, certain aspects should be addressed using sensitivity analyses. Defining those aspects that are to be handled in this way will limit the effort required. Modelling assumptions and data ranges can then accordingly be defined for sensitivity analyses. Usually, sensitivity analyses can slightly restrict the results obtained from specific quantitative analyses. But such care is appropriate in defining TS requirements. For example, in the analyses of STI extension, separation of demand and standby time contribution may not be precisely known and the limiting case obtained in a sensitivity analysis may be sufficient and can be easily justified as an acceptable modification.

The action statements requiring plant shutdown in order to undertake maintenance for safety system components also have an economic impact. Balancing between safety and economic incentives is a difficult issue and not covered in this context. It is a subject of further research and development such as undertaken in the ongoing Nordic project NKS/SIK-1, where decision analysis tools are applied in a TS exemption case [11, 12].

Finally, at the completion of the analyses, development of a clear, detailed documentation is essential. In addition to quantitative analyses performed, this documentation should include:

(a) A list of reasons why the TS improvement is desirable;
(b) Modelling and data assumptions included in the analyses that have bearing on the TS requirement being addressed;
(c) The results obtained from quantitative analyses and how practical considerations have been used to decide on the desired new requirements;
(d) The details of sensitivity analyses and how it has been used to decide or limit the TS change being requested; and
(e) A clear summary presentation of the assessed impact on the plant risk (e.g. changes in the CDF) for the alternatives evaluated.

4. RECENT APPLICATIONS

This section surveys recent TS applications, with special emphasis on those which were completed after the IAEA Technical Committee Meeting held in June 1990 or which were not presented there. The following aspects of each case study are briefly summarized:

- Description of the problem;
- Main results obtained and decisions for implementation;
- General insights obtained.

This survey is limited to representative cases of different types of problems, which can provide useful input for starting new applications, and is by no means considered complete. For more details on methods and data used, specific references cited should be studied.

The case studies selected are sorted and grouped in Table 4.1 according to the relevant TS issue. An overview of the main extensions or supplemental work required in addition to a standard plant specific PSA (Level 1) is also presented.

The case studies presented are grouped in four categories. The first three categories are respectively related to ST arrangements, PM scheduling for a BWR and AOT analysis of a RHR system, whereas the fourth category presents applications concerning changes to multiple AOT and STI requirements in an integrated approach.

TABLE 4.1. MAIN CHARACTERISTICS OF SELECTED CASE STUDIES (These are discussed in more detail in the respective sections of this document)

Subject area/case study	Extensions and supplements to PSA	
	System/component level	Plant level
ST arrangements		
1. DG test re-arrangement at Forsmark 1/2	Detailed analysis of DG experience at the plant.	DG importance measure using core damage frequency (CDF) model.
2 ST strategy for RPS	Detailed system level time dependent analysis.	
3. ST/test caused risks	Detailed component level model incorporating test caused transient effect.	CDF level analysis including test caused transient risks.
4. ST strategy for nuclear instrument channels	Careful distinction of the different failure modes.	
PM arrangements		
5 PM scheduling for Nordic BWRs		Evaluation of CDF influences for alternative PM schedules in redundant trains and functionally redundant systems.
AOT considerations		
6 TVO/RHR study	Repair/recovery time distributions for components and system functions.	Modelling and quantification of LCO shutdown risk, credit from diminishing decay heat in zero power state
Integrated ST/AOT considerations		
7. RHR/ECC (BWR)		Plant level trade-off to optimize AOT/STI modification
8 Screening analysis of STS		Plant specific analysis as a screening evaluation for generic changes to STS.
9. ESFAS AOT/STI (PWR)	Detailed system fault trees	
10. BWR isolation instr. not common to RPS and ECCS	Detailed function level analysis.	
11. TS extension at STP	Impact of AOT extension on maintenance duration distribution.	Evaluation of AOT/STI changes using the plant specific Level 1 PSA.

4.1. TEST SCHEME REARRANGEMENT FOR DIESEL GENERATORS AT FORSMARK 1 AND 2

Forsmark units 1 and 2 each have four DGs, which are tested once a week (Fig. 4.1). In every fourth test the DG is loaded, while the other weekly tests are just start tests. In annual tests, during the refuelling outage, the loss of power in the buses is simulated.

At the plant, the operating staff had begun experiencing that the start tests are unnecessarily frequent and requested a systematic analysis of the length of the test interval. A thorough analysis of the DG operating experience for the period 1981–1987 was performed resulting in an assessment of the effectiveness of different test methods. Unavailability analysis reinforced the qualitative insight that the frequency of start tests can be relaxed. The study resulted in a proposal of a test scheme with two weeks start test/load test interval, every second test being a load test, and pairwise staggered over the four redundant DGs (see Fig. 4.1). Especially, the pairwise staggered scheme is considered to be a reasonable compromise between controlling the risk of systematic errors in testing and detecting latent multiple CCFs [9].

A trial period of the proposed change at one DG is ongoing before a final decision by the authority. Recently, similar detailed analysis of DG operating experiences at all Swedish and the Finnish TVO plants have been completed [13]. The results confirm the insights about the efficiency of different test methods obtained first from the limited Forsmark 1 and 2 database.

SEQ1 T = 1 week →

Sub 1	L	S	S	S	L	S	S	S
Sub 2	S	L	S	S	S	L	S	S
Sub 3	S	S	L	S	S	S	L	S
Sub 4	S	S	S	L	S	S	S	L
Week	1	2	3	4	5	6	7	8

PST2 T = 2 weeks →

Sub 1	L		S		L		S	
Sub 2		L		S		L		S
Sub 3	S		L		S		L	
Sub 4		S		L		S		L
Week	1	2	3	4	5	6	7	8

FIG. 4.1. Base test scheme (SEQ1) and proposed scheme (PST2) for the four redundant DGs at Forsmark 1 and 2 [9].

S = Start test; L = Load test; T = Test interval.

4.2. SURVEILLANCE TEST STRATEGY CONSIDERATIONS FOR THE REACTOR PROTECTION SYSTEM

This application presents an evaluation of the effect of commonly used test strategies, sequential and staggered, on the system unavailability.The use of risk analyses demonstrates the relative benefits and difficulties of one strategy over another.

Surveillance requirements (SRs) in nuclear power plant technical specifications define the tests to be performed on safety system components and specify the intervals at which they should be performed. But the strategy to be followed in scheduling the tests, i.e. the actual placement of tests in relation to each other, is often not specified. In deciding on modifications to surveillance test intervals (STIs), the test strategy to be employed also needs to be considered as it is an important element in defining the risk that is being accepted due to the modifications.

In Ref. [14] an overview of the influence of test strategy on redundant system unavailability is presented. It discusses the relative effects of staggered and sequential testing on various contributors affecting the system unavailability and the core damage frequency calculated in probabilistic safety assessment (PSA) of nuclear power plants. Benefits of staggered testing in reducing these contributors and the practical considerations in implementing such test strategies during operation of nuclear power plants are discussed. This application is presented in detail in Appendix I.

The application presented focuses on quantitative assessment of the influence of different strategies (evaluated at the system unavailability level) and on the benefit of considering the test strategy when evaluating/justifying extensions of surveillance test intervals. The effectiveness of test strategy is quantified using the FRANTIC III [15] computer code for the GE reactor protection system (RPS), with 1-out-of-2 twice logic configuration. The system consists of four independent logic channels. The test strategies evaluated are: (a) a sequential test strategy where all four channels are tested one after another; (b) an evenly staggered test strategy where testing of all four channels are equally separated from each other, i.e. for a prescribed test interval of 4 weeks, channel A is tested at the end of first week, channel B is tested at the end of the second week, and so on; and (c) a semi-staggered test strategy, where one channel from each trip system is tested sequentially, but staggered with respect to the remaining two channels which are also tested sequentially. For sequential testing, when human error common cause failure probability h_{ccf} (seq) is dominant, significant improvement in system unavailability is obtained using an evenly staggered test strategy. Otherwise, a factor of 3 improvement is obtained. Semi-staggered test strategy shows approximately a factor of 2 improvement and higher when h_{ccf} (seq) is dominant.

Figure 4.2 shows the RPS average unavailability (test interval = 12 weeks) for changes in the contribution of common cause failures occurring between tests [signified by changes in CCF(T)] and for different assumptions in the human error common cause failure probability CCF(HE). The figure also shows the relative benefit of different test strategies that can be employed in a reactor protection system.

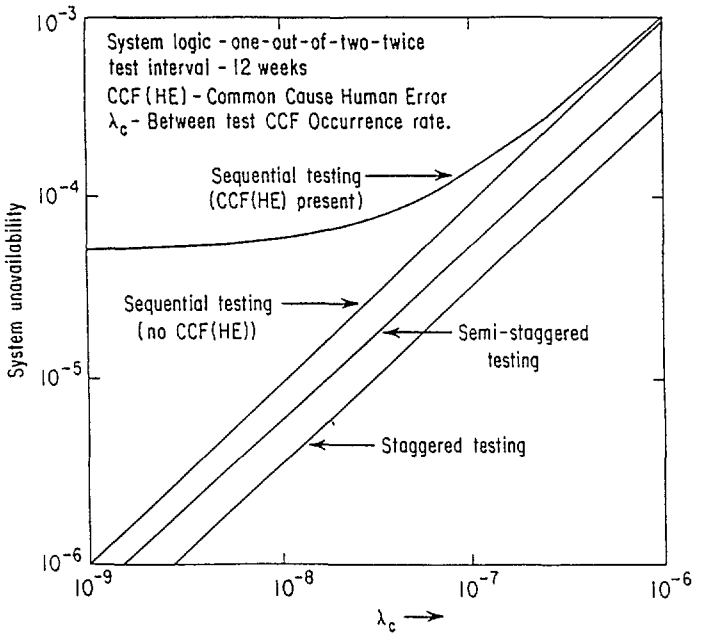


FIG. 4.2. RPS average unavailability as a function of common cause failure (occurring between tests) rate for different test strategies.

4.3. RISK BASED EVALUATION OF SURVEILLANCE TESTS INCLUDING RISKS CAUSED BY TESTS

Recently, PRA based methods were developed to quantify the important adverse effects of testing, i.e. plant transients and equipment degradations [8]. Figure 4.3 shows a typical result of the risk effectiveness evaluation of testing, with respect to transients that may be caused during quarterly testing of main steam isolation valves at BWR plants. This figure depicts the sensitivity of three kinds of test related risks to the variation of test interval, T: (1) the test caused core damage frequency contribution due to transients, R_{trip}, (2) the test detected core damage frequency contribution, R_D, and (3) the total core damage frequency impact of the test, R_T, which is the sum of R_{trip} and R_D.

An important conclusion relevant to the redefinition of a standard test interval is that the interval for MSIV operability testing, i.e. 91 days, can be extended without undue increase in the risk impact. For example, if the test interval is extended to 150 days, R_D increases because the test is more likely to detect failures, while R_{trip} decreases because less testing during a given time period will result in less transients. However, as shown by a dotted curve in Figure 4.3, the total risk impact of the test, R_T, only marginally increases when T is changed from 91 days to 150 days.

The results of quantitative risk evaluation, such as presented above, can be used to evaluate surveillance requirements, in conjunction with qualitative evaluations from engineering considerations and operating experience, such as evaluations of radiation exposure to plant personnel from the tests and test caused operator burden of work.

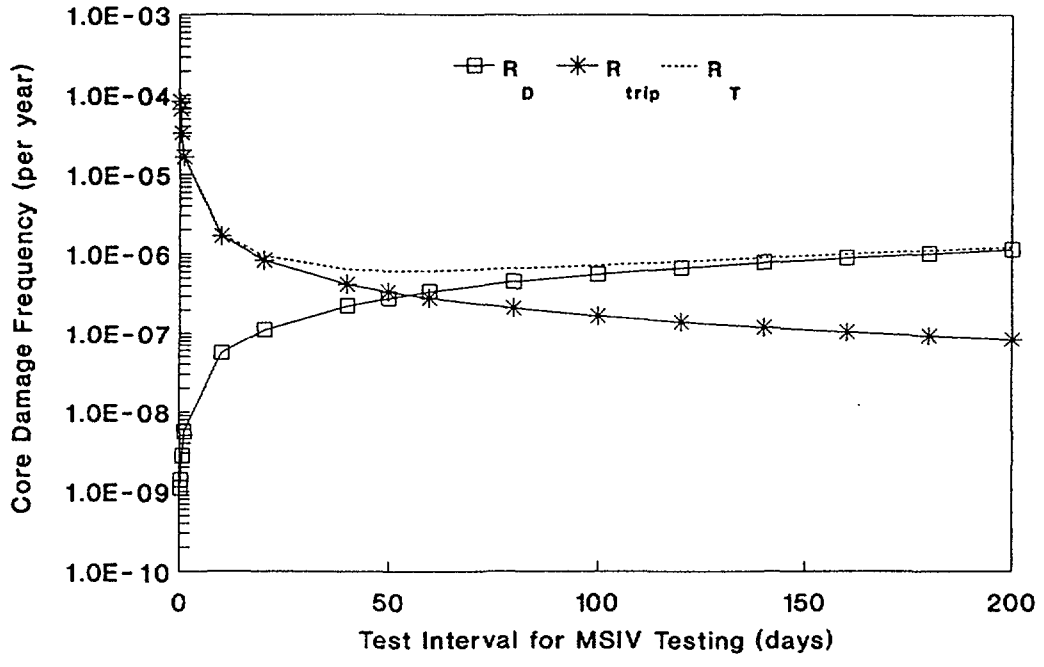


FIG. 4.3. Sensitivity of the core damage frequency impact to the test interval for the main steam isolation valve testing (R_D = test-detected risk impact; R_{trip} = test-caused risk impact due to transients; R_T = total risk impact of the test).

4.4. RISK BASED EVALUATION OF SURVEILLANCE TEST INTERVALS CONSIDERING THE CONTRIBUTION OF DIFFERENT FAILURE MECHANISMS

In this application [16, 17], the surveillance test intervals (STIs) for the excore nuclear instrument channel drawers are evaluated to determine if there is a risk based justification to extend the monthly functional test to a longer interval. This equipment provides a voltage corresponding to the magnitude of neutron flux to the plant protection system (PPS) for reactor trip functions. In addition, the outputs of this system are actively displayed in the control room.

The analysis was accomplished in two stages. First, the functions of various component parts of the system were identified and correlated against the test procedures to verify completeness and to identify duplications. Then, a quantitative evaluation examined the unavailability of the channel outputs to satisfy the trip logic of the PPS. A fault three analysis defined the minimal cutsets for failure of the trip logic function, with full consideration of the potential for common cause failures.

The time dependence assessment assigned anomalies into four categories, each of which is modelled by a parameter of SOCRATES [29]: monitored, standby time related, demand related, and test caused. These categories were chosen based on the circumstances under which the failures were detected. For example, anomalies detected during normal daily operations were classified as monitored. Those revealed during the monthly test were classified as standby, unless they occurred as result of a human error that immediately left the system in a failed or degraded condition. Those that were immediately detected during a test but that resulted in additional downtime for repair were classified as test caused. Human errors that were detected at some later time were classified demand related.

The severity assessment weighted each failure by the conditional likelihood that the observed out-of-tolerance condition could result in a voltage below the trip setpoint, given that a trip condition exists. The analyst used the judgement of the I&C group technicians to estimate an 'equivalent functional failure' likelihood for each anomaly. For example, a slightly out-of-tolerance voltage reading for the response of the operational amplifier to the test signal might be judged to have a 10% probability of producing an inadequate signal during an actual overpower transient. It would be assigned an 'equivalent functional failure' value of 0.1. It should be noted that failures involving drift were also subjected to a drift study to provide confidence that the variations were random and the STI extension would not adversely impact out-of-tolerance readings.

The sum of the equivalent functional failure likelihoods in each failure category was then used in a two stage Bayesian update to obtain site specific failure parameters for use in SOCRATES. The total operating time and failures observed in a peer group of plants were used to establish the generic failure parameters. This was then updated with the operating, test, and failure history of the subject plant.

The uncertainty of the resulting parameters was considered by accomplishing sensitivity calculations across the potential range of failure parameters. Sensitivity studies on the impact of various testing strategies on system unavailability can be easily accomplished with SOCRATES by specifying ranges and intervals of test intervals and testing parameters. All combinations are then automatically calculated and summarized in tables.

The optimum interval balances the decrease of unavailability produced by the earlier detection of standby failures produced by the shorter test intervals with the increase in unavailability produced by test caused failures and the inability to override the alignment of the more frequent tests.

The results of the evaluation are shown in Fig. 4.4. These results indicated that:

- The unavailability of the system is relatively insensitive to the test interval, varying by only 10% for intervals ranging from 1 to 4 months. The risk contribution of monitored and demand related failure mechanisms is not influenced by the testing policy, and approximately two-thirds of the operational failures of the channels were immediately monitored in the control room;

- A surveillance test interval of 90 days produced the lowest value of system unavailability. This extension reduced the contribution of test caused failures to average system unavailability, bringing them in closer balance with standby time related failures;

- Test caused failures of the cable connectors when the drawer containing the electronics is opened and closed during the test accounted for almost one-half of the effective system failures observed. The evaluation process generated suggestions to avoid problems with the cable connectors in the future.

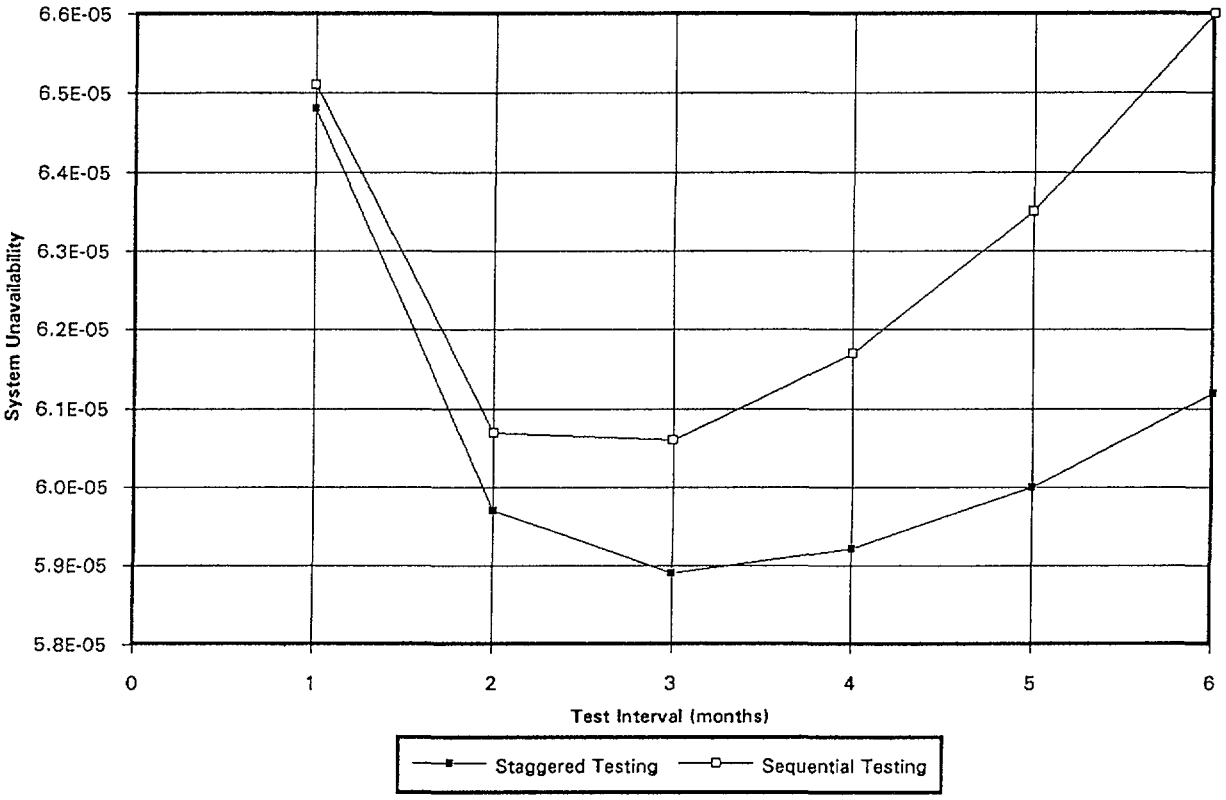


FIG. 4.4. Influence of the STI and test scheme on the unavailability of three out of four ex-core nuclear instrument channels.

4.5. EVALUATION OF THE ALLOWED OUTAGE TIME FOR THE RESIDUAL HEAT REMOVAL SYSTEM OF THE TVO PLANT IN FINLAND

This application is fully described in Appendix II, representing the contents and results of the basic study, completed in 1989. This case study is a pioneering venture for a consideration of the AOT issue as a relative risk comparison between continued power operation (CO) over the repair time versus controlled shutdown (SD), with due consideration to both shutdown related transient risks and failure risks while in cold shutdown state for the repairs.

The risk comparison approach is illustrated in Fig. 4.5, where the two primary risk variables are considered. In the instantaneous risk level, Fig. 4.5a, the main interest focusses on whether a lower risk level will be reached after plant shutdown, because this is a precondition for the SD alternative being at all viable from the risk point of view. In the cumulating risk over predicted repair time (Fig. 4.5b), the main focus is on the crossing point of SD/CO alternatives. SD alternative is motivated for longer repairs than the threshold value. Therefore, this risk variable should be considered most essential in the determination of a proper AOT in the SD/CO comparison approach.

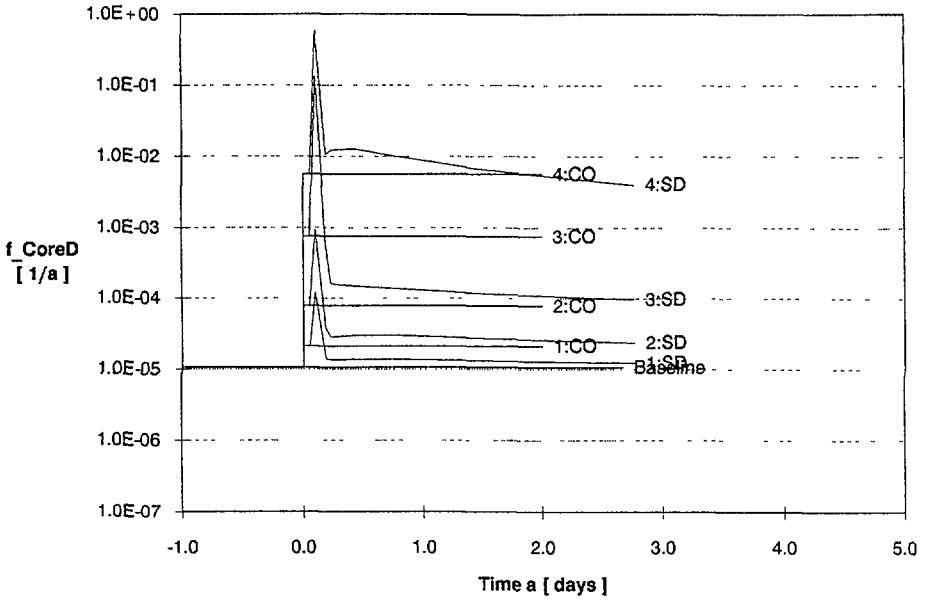


FIG. 4.5a. Instantaneous risk level for the continued operation (CO) and plant shutdown (SD) alternatives in failure situations of RHR trains 712. For example, 2:CO denotes the continued operation alternative in the failure situation of two RHR trains being inoperable.

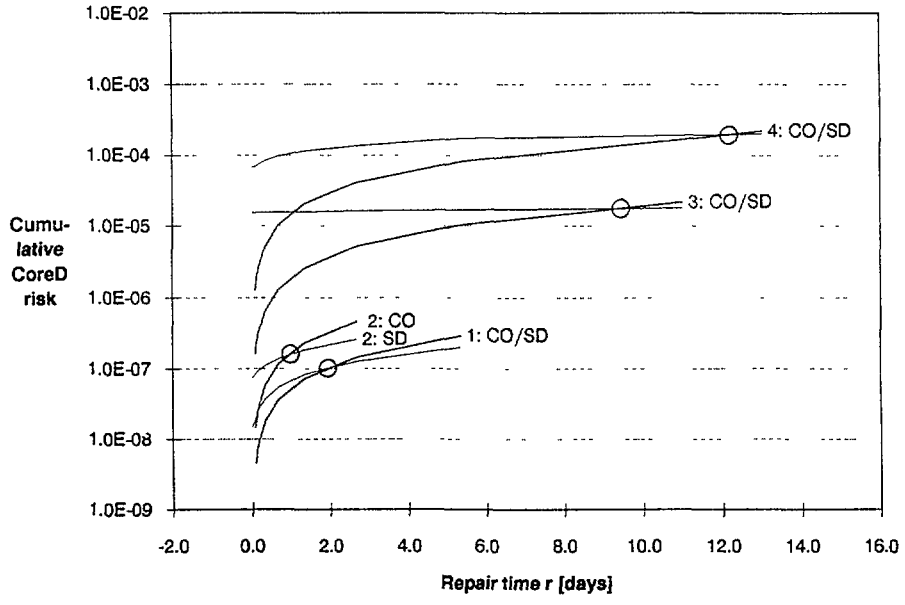


FIG. 4.5b. Cumulative risk over predicted repair time in failure situations of RHR trains 712. For example, 2:CO denotes the continued operation alternative in the failure situation of two RHR trains being inoperable.

The RHR systems were chosen based on discussion with the plant staff, who thought that a plant SD, especially in case of all RHR trains failure, may not be logical. The study resulted in the conclusion that AOTs should be given also for higher order failure situations of the RHR trains [18].

A TS modification plan, including refined instructions for the multiple failure situations of RHR trains, was submitted to the regulatory body. The basic study was limited to cover internal initiating events. A severe fire event at TVO II in April 1991, which caused a loss of station power of 7.5 hours from full power, led to a request to consider the influence of fire and flood events in regard to the RHRS/AOT issue. Corresponding PSA extensions were under way at the plant and were utilized as a framework for a corresponding extension of the RHRS/AOT study. The results showed that some specific fire and flood initiators have a significant contribution in multiple failure situation of RHR trains, but produce only a small influence on the relative results between the operational alternatives. It could thus be concluded that the original recommendations on AOT modifications are still valid.

4.6. PREVENTIVE MAINTENANCE STUDIES FOR THE NORDIC BWR PLANTS

In the newest Nordic BWR plants with four redundant safety systems, PM is currently allowed in one subsystem at a time during power operation. Each subsystem is allowed a cumulative time amount over a year for preventive maintenance. The calculated risk increase is a few percent [19, 20]. It has been minimized by grouping PM in functionally linked subsystems and by excluding simultaneous disconnection of redundant system parts. The small contribution is partly explained also by the fact that in the four redundant systems the CCFs dominate the failure probability, and hence the disconnection of one subsystem has relatively minor effect.

Performing PM during the operation period has many advantages as compared to the refuelling outage period when a large number of tasks are performed in a tight 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. Also, it is possible to use the company's own maintenance personnel having special training. Quality control of the work can also be more effectively performed, and experts from the manufacturers can be more easily engaged when needed. With one subsystem affected at a time, it is easier to control eventual TS configuration violations. These qualitative benefits are difficult to express in quantitative terms, but can be expected to counterbalance, at least partially, in form of the improved equipment reliability, the few percent increase in unavailability contribution from the PM periods [4].

Currently, follow-up studies are ongoing to evaluate the experience gained. These are expected to result in refinements of the PM schedule details. Also the influence on the reliability of the maintained components will be investigated.

4.7. TS IMPROVEMENTS TO CONTAINMENT HEAT REMOVAL AND EMERGENCY CORE COOLING SYSTEMS (BWR)

In this case study application [21], risk and reliability based methods are used to consider improvements to a group of surveillance test intervals (STIs) and allowed outage times (AOTs) for emergency core cooling system (ECCS) equipment, containment heat removal equipment, and supporting systems in a boiling water reactor (BWR). This application demonstrates trade-offs among a set of AOT/STI requirements to achieve a desirable set of STIs and AOTs. In these types of applications, a small group of AOTs and STIs is tightened to make it possible to extend a larger group of less sensitive AOTs and STIs. The intent of such modifications is to reduce the plant operating cost and burden by relaxing requirements and at the same time, assure that the combined effects of the changes maintain the plant safety. The advantage in this type of application is that there is no need to define the threshold for increase in risk due to TS changes. However, it requires identification of STI and AOT packages that maximizes a plant's operation objectives.

The application carried out for the Hatch-2 plant in the USA used the SOCRATES computer code to evaluate the combined effects of 36 AOT and STI requirements. A cost index, determined by a survey of plant operating personnel, was used to assign a relative value to each technical specification change. Using a Monte Carlo procedure to generate thousands of possible combinations of these AOT and STI values, an optimal combination — the one with the highest cost index that did not reduce system unavailability was selected. The proposed set of STI and AOT changes can be characterized as follows: 3 STIs tightened, 24 STIs/AOTs extended, operating costs reduced by fewer tests and associated man-hours, avoidance of potential unnecessary plant shutdowns, improved repair of failed equipment, less wear on equipment, and reduced diversion of plant personnel. The calculated combined function failure frequency for the water injection function and the containment heat removal function is improved (i.e. decreased from 2.2×10^{-5}/year to 2.13×10^{-5}/year) from the base case (with current AOTs and STIs) to the recommended case (with changed AOTs and STIs).

4.8. RISK BASED ANALYSES AS A SCREENING METHOD TO EVALUATE PROPOSED CHANGES IN STANDARD TS

In this application [27], risk based analysis is used to assess the impact of proposed changes in the standard technical specifications. Here, the changes are originally developed based on deterministic arguments and engineering judgements, but PSA analysis is used as one of the screening criteria to proceed with the changes. This approach is used by the US Nuclear Regulatory Commission in developing their new standard technical specifications.

All proposed standard technical specification changes were examined, in order to identify those changes that could be evaluated with a risk based approach. All STI and AOT changes for components that could potentially contribute to boiling water reactor (BWR) or pressurized water reactor (PWR) plant risk were identified. In addition, there were several proposed changes in the electrical power system section of the new standard technical specifications that are not strictly AOT or STI changes but rather changes to the required configurations in case one or more components are out of service. The risk importance of these configuration changes were also analysed using risk based approaches.

4.9. MODIFICATION OF ALLOWED OUTAGE TIME AND SURVEILLANCE TEST INTERVAL FOR INSTRUMENTATION

In this application [22], STIs and AOTs for the Engineering Safety Features Actuation System (ESFAS) for Westinghouse plants are evaluated. In requesting these changes, the assurance of high reliability of RPS needed to maintained. The ESFAS AOT and STI requirements were considered to be unnecessarily restrictive and, in addition, ESFAS requirements needed to be consistent with RPS requirements (which were previously modified), since ESFAS shares common instrumentation with the RPS. The assessed core damage frequency impact of such changes was within 6 percent of the PSA calculated average CDF. Besides, a number of other aspects, treated qualitatively, were judged to reduce the assessed CDF impact. This included more efficient test and maintenance operations, reduction in human error rates and reduction in the number of inadvertent actuations of engineering safety features.

The specific changes to the ESFAS TS were as follows:

(1) An increase of the STI for ESFAS analog channels was accepted;
(2) The AOT for testing the analog channels was increased from 2 to 4 hours;
(3) The AOT for testing all components was increased to 4 hours in solid state systems;
(4) The AOT for testing logic trains and master relays was increased to 8 hours and the AOT for the slave relays may be increased to 12 hours in relay systems;
(5) The AOT for maintenance for all components was extended to 12 hours for both relay and solid state systems; and
(6) A staggered test strategy was not required for ESFAS and RPS analog channel testing.

4.10. EXTENSION OF SURVEILLANCE TEST INTERVALS AND ALLOWED OUTAGE TIMES FOR ISOLATION INSTRUMENTATION NOT COMMON TO REACTOR PROTECTION SYSTEMS OR EMERGENCY CORE COOLING SYSTEMS FOR BWR PLANTS

These analyses were conducted to ensure that the TS requirements for related instrumentations are consistent. Also, extending STIs for isolation actuation instrumentation has the potential for reducing wear due to excessive equipment test cycling and better optimizing the use of plant personnel, with resulting improvements in plant safety and operations.

In this application [23], the effect on isolation function failure probability of extending the STI was assessed. Additionally, the sensitivity of the isolation function failure probability values to allowed outage times for test and repair was examined. This analysis was conducted for each of the BWR groups (BWR-6, BWR-5/6, BWR-3/4 and BWR-2).

For this application, fault trees were developed for the isolation functions of interest to determine the impact of proposed technical specifications STI/AOT changes. The magnitudes of the changes in MSIV isolation function failure frequency were very small, less than 1.5 E-08/year. Because the failure frequency impact was minimal, the following changes were acceptable: change STIs for isolation actuation instrumentation not common to RPS or ECCS from 31 days to 92 days; change test AOTs from 2 to 6 hours; and change repair AOTs from 1 to 24 hours.

4.11. RISK BASED EVALUATION OF ALLOWED OUTAGE TIME AND SURVEILLANCE TEST INTERVAL EXTENSIONS USING A LEVEL 1 PSA

This evaluation [24] uses the Level 1 PSA for the South Texas Project Electric Generating Station to justify the extension of AOTs and STIs for a large fraction of the plant's safety related systems. The PSA provides an estimate of the core damage frequency, including internal and external initiating events and a complete uncertainty analysis.

The two plants at the site each have three electrically independent and physically separate safety trains, whereas their current technical specifications are similar to those that were developed for two-train designs. The additional redundancy provided by the third train created the potential for additional flexibility to perform testing and maintenance while maintaining a lower risk profile than that which would have existed with only two trains present. Therefore, extensions to AOTs and STIs for the three train systems were judged to be acceptable if they do not result in a significant increase in the core damage frequency.

The STPEGS PSA includes 35 system analyses using the RISKMAN [25] code which uses the large event tree approach. They model explicit contributions to system unavailability due to independent and common cause hardware failures, maintenance, testing and human error. These contributions were varied to reflect the impact of requested changes to technical specifications. Both the resulting system unavailabilities and the resulting change in the time averaged core damage frequency (CDF) were then calculated and compared to the base values.

- Extension of the AOTs impacts the maintenance duration distributions for at-power operations, making them longer. This, in turn, increases the unavailability due to maintenance in the systems analysis. Maintenance durations were developed as a function of both equipment type and AOT length.

- Extension of the STIs considers the unavailability impact of test alignments and failures during testing due to demand related mechanisms against the unavailability during the period of time that the component would be in an undetected failed state due to standby time related failure mechanisms.

In the evaluation of proposed changes to AOTs, industry data from similar plants on the duration of equipment maintenance outages were correlated to AOTs and, from this, AOT specific maintenance duration distributions were developed. As part of the evaluations of proposed changes to STIs, sensitivity studies were performed to investigate the impact of two different types of failure mechanisms contributing to the demand based failure rates: standby failures and shock induced failures at the time of demand. The testing intervals imposed by the STIs only impact the standby failure contributions.

The results for the 10 systems on which technical specification changes had the greatest impact on time averaged CDF are summarized in Fig. 4.6. The other systems for which changes to technical specifications were proposed had very minimal impact on time averaged CDF. (The utility is re-evaluating the rationale for the technical specifications of those top three systems.)

As a result of the PRA evaluation, the proposals for technical specification changes that increased the average core damage frequency by more than 10% were withdrawn from the set of proposed changes.

4.12. ADDITIONAL REFERENCES ON CASE STUDIES

Within the ongoing Nordic research project NKS/SIK-1, a living PSA model has been developed for the Oskarshamn 2 BWR and is being used in experimental applications. The applications include risk follow-up over one operating year, evaluation of AOTs and test intervals, and investigating risk monitoring and risk control approaches [28]. Another, benchmark type application was performed in order to test decision analysis tools in a TS exemption case [11, 12].

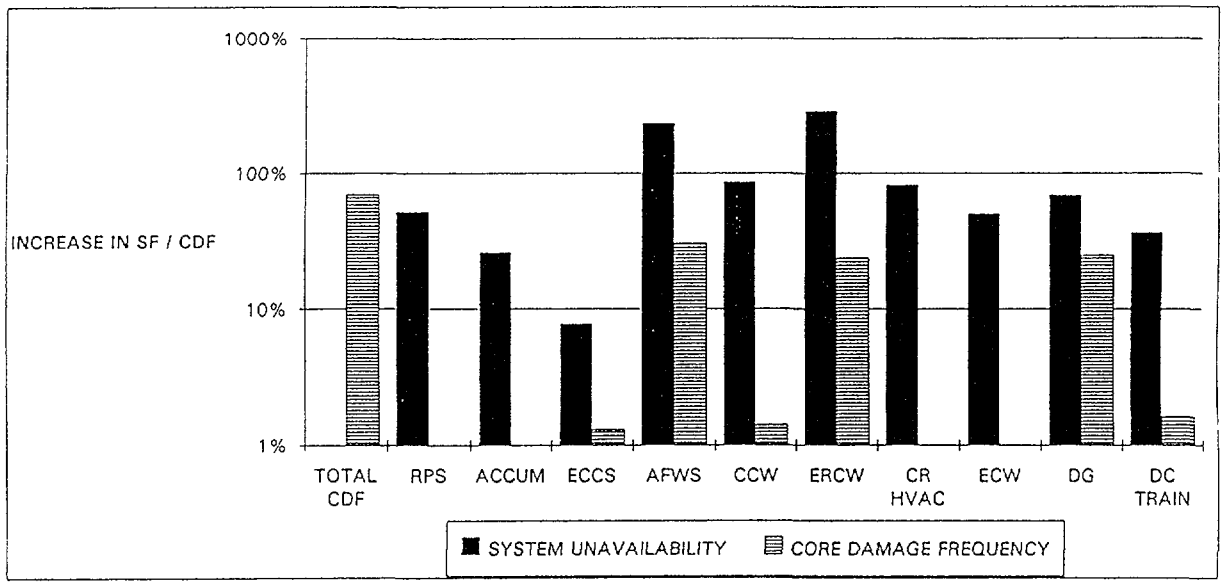


FIG. 4.6. Comparison of system and plant level impacts of AOT and STI changes at the South Texas Project Electric Generation Station.

5. CONCLUDING REMARKS

Existing PSA models, data and special tools allow efficient analyses of TS problem issues and provide an essential basis for making decisions with due consideration to safety influences in parallel to technical and operational features. As the benefits are so evident, more extensive use of PSA tools in improving specific TS requirements are strongly encouraged.

The development of a more plant wide approach to TS, as a part of overall operation and safety management, or so-called living PSA concept, risk monitoring and configuration control system are in progress. First implementations of such a system already exist at the Heysham plant in the United Kingdom. This type of development is expected to mature in the coming years.

REFERENCES

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Use of Probabilistic Safety Assessment to Evaluate Nuclear Power Plant Technical Specifications, IAEA-TECDOC-599, Vienna (1991).

[2] HORNE, B.E., "The use of PSA methods for planning the maintenance and testing unavailabilities of essential plant at Heysham 2 AGR power station", Use of Probabilistic Safety Assessment to Evaluate Nuclear Power Plant Technical Specifications, IAEA-TECDOC-599, IAEA, Vienna (1991).

[3] MANKAMO, T., A Risk-Based Approach to AOTs, Avaplan Oy, NKS/SIK-1(93)4, Helsinki (1993).

[4] LAAKSO, K. (Ed.), Optimization of Technical Specifications by Use of Probabilistic Methods — A Nordic Perspective, Final report of the NKA project RAS-450, Nord Series 1990 (1990).

[5] SAMANTA, P.K., WONG, S.M., CARBONARO, J., Evaluation of Risks Associated with AOT and STI Requirements at the ANO-1 Nuclear Power Plant, Rep. NUREG/CR-5200, BNL-NUREG-52024, US Nuclear Regulatory Commission, Washington, DC (1988).

[6] VESELY, W.E., Evaluation of Allowed Outage Times (AOTs) from a Risk and Reliability Standpoint, Rep. NUREG/CR-5425, US Nuclear Regulatory Commission, Washington, DC (1989).

[7] SAMANTA, P.K., VESELY, W.E., LOFGREN, E., BOCCIO, J., Risk Methodology Guide for AOT and STI Modifications, Rep. BNL A3230 12-02-86, BNL, Upton, NY (1986).

[8] KIM, I.S., MARTORELL, S., VESELY, W.E., SAMANTA, P.K., Quantitative Evaluation of STIs Including Test-Caused Risks, Rep. NUREG/CR-5775, BNL-NUREG-52296, February 1992, US Nuclear Regulatory Commission, Washington, DC (1992).

[9] ENGQVIST, A., MANKAMO, T., "Test scheme rearrangement for diesel generators at Forsmark 1/2", PSA '89 Int. Topical Meeting on Probability, Reliability and Safety Assessment, Pittsburgh, PA, 1989.

[10] DRAGO, J.P., et al., The In-plant Reliability Database for Nuclear Plant Component: The Pump Component, Oak Ridge National Laboratory, Rep. NUREG/CR-2886, US Nuclear Regulatory Commission,Washington, DC (1982).

[11] PÖRN, K., SHEN, K., Decision Making Under Uncertainty — A Pilot Study on Exemption from Technical Specifications, Studsvik/NS-91/90, NKS/SIK-1(91)29 (1992).

[12] HOLMBERG, J., PULKKINEN, U., Decision Analysis on an Exemption from Technical Specifications, Technical Research Centre of Finland, VTT/SÄH-4/92, NKS/SIK-1(92)8, Helsinki (1992).

[13] MANKAMO, T., "Test strategies for standby diesel generators", IAEA Techn. Committee Mtg on Advances in Reliability Analysis and PSA, Budapest, 1992.

[14] SAMANTA, P. GINZBURG, T., VESELY, W., Consideration of Test Strategy in Defining Surveillance Test Intervals, Rep. BNL A-3859, BNL, Upton, NY (1988).

[15] GINZBURG, T., POWERS, J., FRANTIC III, A Computer Code for Time-dependent Reliability Analysis, Methodology Manual, Technical report BNL A-3230, Upton, NY (1984).

[16] QUINN, E.L., DYKES, A.A., BOCKHORST, R., Risk-based Evaluation of Surveillance Test Procedures at San Onofre Nuclear Generating Station, Transactions, American Nuclear Society, Vol. 56 (1988) 343.

[17] DYKES, A.A., QUINN, E.L., Methodology for Developing Risk-based Surveillance Programs for Safety-related Equipment at San Onofre Nuclear Generating Station Unit 2 and 3, PLG-0575, Gaithersburg, MD (1992).

[18] MANKAMO, T., KOSONEN, M., "Operational decision alternatives in failure situations of standby safety systems", Use of Probabilistic Safety Assessment to Evaluate Nuclear Power Plant Technical Specifications, IAEA-TECDOC-599, IAEA, Vienna (1991).

[19] HEINONEN, R., PIIRTO, A., "Preventive maintenance of safety systems during normal power operation of TVO's nuclear power plant", IAEA Int. Symp. on Advances in NPP Availability, Maintainability and Operation, Munich, 1985.

[20] KNOCHENHAUER, M., ENGQVIST, A., "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, 1987.
[21] SULLIVAN, W.P. et al., Technical Specification Improvements to Containment Heat Removal and Emergency Core Cooling Systems, Rep. EPRI NP-5904, Palo Alto, CA (1988).
[22] WESTINGHOUSE ELECTRIC CORPORATION, Westinghouse Evaluation of Surveillance Frequencies and Out of Service Times for ESFAS, WCAP-10721, Pittsburgh, PA (1986).
[23] GENERAL ELECTRIC, BWR Extension of Surveillance Test Intervals and Allowed Outage Times for Isolation Instrumentation not Common to RPS or ECCS Instrumentation, GE-NEDC-31677P, San Diego, CA (1987).
[24] HOUSTON LIGHTING & POWER COMPANY, letter ST-HL-AE3283, File No. G20.02.01, G2.06, 10CFR50.90, to US Nuclear Regulatory Commission, Subject: South Texas Project Electric Generating Station, Units 1 and 2, Docket Nos STN 50-498, STN 50-499, Proposed amendment to the unit 1 and unit 2 Technical Specifications Based on Probabilistic Risk Analysis, dated February 1, 1990.
[25] PLG, RISKMAN, PRA Workstation Software, release 4.0, PLG, Inc., 1992.
[26] MANKAMO, T., PÖRN, K., HOLMBERG, J., Uses of Risk Importance Measures, Technical report NKS/SIK-1(90)6, Research Notes 1245, Technical Research Centre of Finland, Espoo (1991).
[27] NUCLEAR REGULATORY COMMISSION, Feasibility Assessment of Risk-based Approach to Technical Specifications, Rep. NUREG/CR-5742, Washington, DC (1990).
[28] SANDSTEDT, J., BERG, U., "Living PSA applications for a Swedish BWR with the aid of risk spectrum", 3rd Workshop on Living PSA Applications, Hamburg, 1992.
[29] WAGNER, D.P., VESELY, W.E., MINTON, L.A., SOCRATES: Risk-based Evaluation of Technical Specifications, Battelle Columbus, Rep. EPRI NP-4317, Palo Alto, CA (1985).

Next page(s) left blank

Appendix I

CONSIDERATION OF TEST STRATEGY IN DEFINING SURVEILLANCE TEST INTERVALS

EXECUTIVE SUMMARY

Surveillance Requirements (SRs) in nuclear power plant technical specifications define the tests to be performed on safety system components and specify the intervals at which they should be performed. But the strategy to be followed in scheduling the tests, i.e., the actual placement of tests in relation to each other, is oftentimes not specified. In deciding on modifications to surveillance test intervals (STIs), the test strategy to be employed also needs to be considered as it is an important element in defining the risk that is being accepted due to the modifications. This report presents an evaluation of the effect of commonly used test placement strategies (or test strategies), sequential and staggered, on the system unavailability and using risk analyses demonstrates the relative benefits and difficulties of one strategy over another.

Based on system reliability/availability analyses, which do not include many negative aspects of staggered testing, the benefits of staggered testing can be demonstrated. Staggered testing reduces (i) independent or random failure contributions, (ii) human error common-cause failure contributions, and (iii) contributions from common-cause failures occurring between tests. This results in lower peak and average system unavailability. The degree of reduction in system unavailability varies and depends primarily on the system logic configuration, the dominant failure modes within the system, and the actual staggered strategy used.

The negative aspects of staggered testing relates to i) test-caused failures that have risk implications, ii) potential for increased human error in testing from crew-stress, and iii) practical considerations in implementing a staggered strategy during power operations. An example of test-caused failures with risk-implications is the inadvertent scrams experienced during test and calibrations of Reactor Protection System (RPS) channels. In a staggered test strategy, a slight increase in the number of inadvertent scrams can be experienced due to an increased number of test set-ups necessary. This increased number of test set-ups, coupled with the fact that test crew are required to conduct a large number of similar, routine tests where failures occur rarely, results in boredom and crew-stress that can potentially increase the human error in testing. Current reliability analyses do not incorporate these "human" aspects in the quantification. Practical considerations such as the requirement of power reduction, if necessary, for the test become burdensome due to the increased number of test set-ups in a staggered test strategy. In the absence of a quantitative methodology that incorporates these negative aspects of testing, the results presented in this study focusses on quantification of the benefits of staggered testing over sequential testing. The decision on a test strategy, however, should balance the quantified benefits of staggered testing with qualitative consideration of the negative aspects.

The requirement of staggered testing should be considered when the negative aspects of such a strategy are considered to be of minimal impact and the associated benefits are significant. If the system unavailability remains acceptably low irrespective of the test strategy, the requirement for a test strategy may be unspecified whereby a sequential test strategy may be used by the plant operating staff. When increased test interval is being sought and the increase in the system unavailability is not desirable, a staggered strategy can be used to neutralize the increased system unavailability. When common-cause failures are dominant, but the system unavailability is low, then test intervals can be sufficiently extended such that the number of test set-ups necessary under a staggered test strategy will be no higher than that under a sequential test strategy. In such an arrangement only when a failure is detected, additional testing will be required to detect existence of any common-cause failure. Depending upon the dominant contributors to the system unavailability, specific acceptable test strategy that minimizes the negative impact of testing can be developed.

ACKNOWLEDGEMENT

The authors acknowledge Mr. Millard Wohl, NRC Lead Engineer of the project, and Mr. Edward Butcher, the Technical Specifications Branch Chief, for their many helpful technical discussions and support during the project. The technical and programmatic support provided by Dr. John Boccio, BNL, is greatly appreciated. Mr. William Gunther and Mr. William Luckas, Jr., BNL, significantly enhanced the risk evaluation by providing valuable insights into understanding the RPS test procedures.

Finally, we are very thankful to Ms. Jeanne Danko and Ms. Kathleen Nasta for their help in preparing the manuscript.

1. INTRODUCTION

Surveillance Requirements (SRs) in nuclear power plant technical specifications define the tests to be performed on safety system components and specify the intervals at which they should be performed. But the strategy to be followed in scheduling the tests, i.e., the actual placement of the tests in relation to each other, is oftentimes not specified. However, the placement of tests can be as important a factor as the adequacy of the test and the interval between tests in determining the risk contributions that are associated with surveillance test requirements.

In deciding modifications to surveillance test interval requirements, the requirement on placement of tests is therefore an important element to consider. Standard PRA techniques do not take into account the actual placement of tests. In this report, the effect of test placement on system unavailability is studied and the risk contributors associated with placement of tests are defined. In this study, the primary focus is on the risk contributors associated with a test placement strategy (or test strategy). In the evaluations presented here, quantification of the operational considerations is not included. The General Electric (GE) Relay Plant Reactor Protection System (RPS) is used as an example to demonstrate the impact of test placement strategy.

Following this introduction, Chapter 2 presents a discussion on the influence of test strategy on peak and average system unavailability. Chapter 3 presents the evaluation approach and a brief description of the GE RPS, which is used as an example in this study. Chapter 4 presents the results for the sensitivity analysis of different test strategies under various assumptions. Chapter 5 summarizes the findings and the insights obtained in this study.

2. INFLUENCE OF TEST STRATEGY ON REDUNDANT SYSTEM UNAVAILABILITY

The availability of components in a standby safety system is assured through periodic testing of the components. In determining the unavailability of a component (or conversely, the probability of availability when the component is required), one important factor is the time elapsed from the last successful component test. Thus, to achieve an appropriate level of availability for a single component one must define:

a) an adequate test to detect any failure of the component, and
b) an acceptable test interval for timely detection of a failure that may occur.

For a system consisting of a number of components, the above two requirements can be satisfied for each component in a number of ways as far as the actual placement of the tests is concerned, i.e., the actual times at which the tests are performed. The strategy followed in placing the test of different components is called a test strategy. The test strategy can have significant impact on the system unavailability.

The test strategies typically used in the safety systems of nuclear power plants can be defined in three categories. Sequential testing of n components in a specified test interval is accomplished by performing tests on n components in sequence at the end of the interval. For a sequential testing of three components with a given test interval T and test conduction time τ, the first component is tested in the interval T to $(T + \tau)$, the second in the interval $(T + \tau)$ to $(T + 2\tau)$, and the third is tested in the $(T + 2\tau)$ to $(T + 3\tau)$. Usually, τ is much smaller than T, and the cycle repeats at each test interval T. Staggered testing of n components in a specified test interval is accomplished by performing a component test at the end of a sub-interval where the test interval

is divided into n equal sub-intervals determined by the number of tests performed. In a perfect (or evenly) staggered schedule for a three-component system, the test interval T is divided in three equal intervals and the first component is tested in the interval T/3 to (T/3 + τ), the second in the interval (2T/3 + τ), and the third is tested in the interval (T + τ). Simultaneous testing of n components in a specified test interval implies that all n components are tested together at the end of the interval. Simultaneous testing of three components implies that all three are tested in the interval T to (T + τ). An unspecified test strategy only requires that test intervals be maintained and the placement of the tests will be at the discretion of individuals performing the test. We shall study particularly staggered testing versus sequential testing as different placement strategies.

Both the average unavailability and the peak unavailability (the maximum unavailability) of standby safety systems depend on the efficiency of the tests performed on its components, the interval at which the tests are performed, and the placement of the tests. In this section, a qualitative discussion on the influence of test placements on various aspects that contribute to the determination of unavailability is presented, which forms the basis for understanding the results presented later. Table 2.1 summarizes the effect of staggered testing versus sequential testing, and the following sections present more details on these effects.

Table 2.1 Comparison of Influences of Sequential Versus Staggered Test Strategy

Attributes	Effects of Staggered Versus Sequential Testing
Peak Unavailability	Lower for staggered
Average Unavailability	Lower for staggered
Potential for Human Error CCF*	Significantly reduced for staggered
Potential for CCF* occurring between tests	Potential for early detection and correction for staggered
Test Setup time/yr	Higher for staggered
Test conduction time/yr	Slightly higher for staggered
Occupational Exposure	May be higher for staggered
Inadvertent Scrams	Can increase for staggered

* The symbol CCF denotes common-cause failures which are multiple component failures resulting from a single cause.

2.1 Benefit of Staggered Testing in Reducing Independent Failure Contributions to System Unavailability

The independent failure contributions of redundant components where all failures are time related are influenced by the test strategy (for the same test interval) thus affecting both the peak and average system unavailability. Here the benefit of staggered testing in reducing the independent failure contributions to system unavailability (compared to sequential testing) is discussed for various system logic configurations.

Effect of Staggered Testing on Peak Unavailabilities: For a standby component tested at specific time points, its instantaneous unavailability grows following a test and reaches its peak just before the next test. This growth in unavailability depends on the failure rate of the component and on the length of the time period. In a system of redundant components, when tests are performed sequentially, component unavailabilities grow simultaneously and peak unavailabilities are concentrated at similar times resulting in higher values for the system unavailability. However, when tests are staggered, the individual component peak unavailabilities are distributed according to the different test times, and accordingly, the peak unavailability for the system is lower.

Consider a 4-unit redundant system under sequential and staggered test strategy to understand the behavior of peak unavailability. For the sequential test strategy, the peak unavailability occurs before the test, i.e., at times T, 2T,..., for a test interval T. For a perfect (or evenly) staggered test schedule, peaks of a much lower magnitude will occur at times T/4, T/2, 3T/4, T, 5T/4,... and so on.

Reduction in peak unavailability due to a staggered test strategy compared to a sequential test strategy depends on the system logic configuration, and on the staggered strategy implemented. Maximum benefit is achieved when perfect staggering is assumed. Green and Bourne[1] provide detailed mathematical derivation for a n-unit redundant system where each unit's unavailability is described in terms of its time related failure rate. Table 2.2 presents the factor reduction in the independent failure contribution for peak system unavailability in different system logic configurations. The factors in the table assume a perfect (or evenly) staggered strategy, but they are basically the same if the tests are not exactly staggered.

Table 2.2 Factor Reduction in Peak Unavailability for Staggered Testing (independent failure contribution)

System Logic Configuration	Reduction in Peak Unavailability for Staggering
1:2	2.0
1:3	4.5
1:4	10.7

Effect of Staggered Testing on Average Unavailability: The average unavailability obtained under a staggered test strategy is lower than that obtained in a sequential test strategy due to the smoothing effect on the peak unavailabilities (larger number of peaks with lower magnitude). Green and Bourne[1] provide derivation for n-unit (each described by time related failure rate) redundancy. Vesely et al.[2] presents a comparison of 2 diesel unit average unavailability for sequential and staggered test strategy. Table 2.3 presents the factor reduction obtained for different system logic configurations.

Table 2.3 Factor Reduction in Average Unavailability for Staggered Testing (independent failure contributions)

System Logic Configuration	Reduction in Average Unavailability
1:2	1.6
1:3	3.0
1:4	6.12

2.2 Benefit of Staggered Testing in Reducing Common-Cause Failure Contributions

In redundant systems, two types of common-cause failures can be identified which are influenced by test strategies: human error common-cause failures, CCF(HE), and common-cause failures occurring between tests, CCF(T). In reliable systems, these contributions can be dominant contributors and the benefit of a staggered strategy in such systems depends on the reduction achieved in these contributors. The following discussion details the effect of staggered strategy in these two types of common-cause failures.

Effect on Human Error Common-Cause Failure CCF(HE)

Following a test, a human error may inadvertently disable the component. Whenever a sequential test is performed on a group of components, a human error CCF is more likely in that given one error has occurred, the likelihood of another error being committed is high because of the closeness of the sequential tests. In a staggered testing strategy since the tests of the components are more separated, the dependency among the errors is expected to be less. That is, given a human error has been committed on one test, the likelihood of it being committed on the next test also is less because of the greater separation in time between the tests.

The benefit to be obtained by reducing this type of contributor to system unavailability depends on the common-cause human error probability. The type of staggering needed to obtain the benefit should be such as to provide sufficient separation among the tests to reduce the human error CCF to an acceptable value. Tests separated by days may be sufficient to reduce the human error CCF to an acceptable value, and perfect staggering may not be necessary.

Effect on Other Common-Cause Failures Which can Occur Between Tests, CCF(T)

The components in a standby safety system are susceptible to other common-cause failures which can occur between tests. The unavailability of a multiple train system is, in many cases, dominated by such common-cause failures. Staggering the tests can be effective in early detection of such failures thus influencing the unavailability of the system.

Consider a 1-out-of-3 unit system with a 30 day test interval. In a sequential test strategy the maximum time the system can be in the failed state will approximately be the length of the test interval, i.e., 30 days. In staggered testing, a strategy can be followed where at least one component is tested every 10 days, thus providing an opportunity to detect any common-cause failure that may have occurred over that time period. Accordingly, in such a strategy, the maximum time the system may remain failed due to common-cause failure will be 10 days, as opposed to 30 days, a factor of three decrease. Table 2.4 presents the factor reduction in CCF(T) contribution for different logic configurations.

Table 2.4 Factor Reduction of Common-Cause Failure Probability (Occurring Between Tests) Due to Staggered Testing

System Logic Configuration	Reduction in CCF Probability
1:2	2
1:3	3
1:4	4

The early detectability and the removal of common-cause failure by a staggered testing strategy depends on the system logic. In the above example, as long as one of the components is repaired, the effect of common-cause failure is removed. However, in a different logic configuration, for example, in a

2-out-of-4 unit system, at least 2 of the components should be repaired to obtain the maximum benefit. A staggered testing strategy is thus coupled with two choices whenever a failure is detected for any one of the components. In one, whenever a failure is detected, and common-cause failure is suspected, all other components are tested and repaired, as necessary. In the other, the test schedule is maintained irrespective of any failure detection. The placement of tests in a staggered schedule to minimize the effect of common-cause failure is complicated depending on the system logic and other errors that may be present in a testing and is discussed further for a one-out-of-two-twice logic system in Section 4.2.

2.3 Effect on Inadvertent Scrams Due to Staggered Testing

The increased test set ups necessary in a particular test strategy may affect the overall plant safety by influencing the number of reactor scrams that may result. The number of test set ups necessary for testing a group of components depends on the type of test strategy used. For a n-unit system, the number of test set ups in a year could be a factor of n higher for a staggered strategy as opposed to a sequential strategy if the sequential testing requires one test set up. The inadvertent scrams directly impact plant safety and the frequency of such scrams due to instrumentation testing was studied in Ref. 3. If the inadvertent scram probability is sufficiently high, then the inadvertent scram frequency due to staggered testing could significantly add to the scram initiating event frequency and offset the benefits of staggered testing. This is generally not the case, but should be checked on a case by case basis.

2.4 Practical Considerations in Implementing Staggered Testing

The implementation of test strategy during operation may impose a number of operational difficulties that should be considered if the difficulties are deemed substantial. Ref. 4 provides a description of such possible difficulties for the GE Reactor Protection System.

a. Certain types of tests require power level reductions to prevent plant scram resulting in a reduced capacity factor. A staggered test strategy as opposed to a sequential test strategy will increase the number of such power level reductions. For example, in GE RPS, functional tests of main steam isolation valves (MSIV), turbine stop valves, and turbine control valves may require reactor power level reduction (Ref. 4). In developing a test strategy, care should be taken to avoid staggering such tests to the extent possible. Staggered testing in such a system can involve staggering the channel functional tests for other variables, but performing sequential testing for those variables and components requiring power level reductions.

b. In certain plants, some of the testing are associated with personnel exposure and a staggered testing may increase the exposure level. This is generally insignificant.

c. Finally, a staggered strategy requiring an increased number of test set ups can be operationally burdensome compared to performing the tests together sequentially. From an operational point of view, the advantage of increasing a test interval is lost, if staggered testing is to be implemented requiring the same number of test set ups even though each requires a smaller number of tests.

3. EVALUATION OF IMPACT OF TEST STRATEGY: REACTOR PROTECTION SYSTEM

The evaluation of the impact of test strategy for a standby safety system is demonstrated in this study using a GE Reactor Protection System (RPS). The model and the data base for RPS relay plants presented in GE NEDC-30851P, Tech-

nical Specification Improvement Analysis for BWR Reactor Protection System, May 1985 (Ref. 3), are the basis for performing sensitivity evaluations under different test strategies with varied assumptions.

The choice of a RPS as a demonstrative example in this study was based on the following reasoning:

1. The RPS provides an interesting logic configuration (1-out-of-2 system, twice) and there are a significant number of tests performed on the system providing different alternatives for test placements.

2. Because of the redundancy, the RPS unavailability is low and is dominated by common-cause failures. This situation allows for an evaluation of the effectiveness of test placements in a highly reliable system and on reducing common-cause failures.

3. The technical specification of RPS does not have any requirement on placement of the tests. The frequency of tests that are currently required may actually not be necessary from a risk standpoint. In order to reduce the burden, the test intervals are being considered for extension and the necessity of requiring a specific test strategy to compensate the risk increase from the test interval extensions needs be addressed.

3.1 Brief Description of RPS

The brief description of RPS presented here is basically obtained from GE NEDC-30851P, Technical Specification Analysis for Reactor Protection System.

The RPS of the relay plants is used for the analysis. The RPS includes the power supplies, sensors, trip circuitry, bypass circuitry, and switches that cause rapid insertion of the control rods to shut the reactor down. The analysis and the discussion here are directed to the instrumentation logic of the system as the testing of RPS is performed on these logic channels.

The RPS consists of four independent logic channels (Figure 3.1). These four channels are divided into two trip systems. Trip System 1 consists of logic Channels A and C in redundant configuration and provides input for the trip actuation system by de-energizing Solenoid A for each of the hydraulic control units (HCUs) associated with each control rod. Similarly, Trip System 2 consists of logic Channels B and D in redundant configuration and provides input for trip actuation by de-energizing Solenoid B for each of the HCUs. A successful scram requires de-energization of both Solenoid A and B. Thus, the RPS logic consists of 1-out-of-2 (for each of trip system) configuration twice (since combined output of Solenoids A and B are needed).

Each channel consists of separate sensors, relays, and contactors. The particular system configuration considered contains a pair of contactors for each channel, providing added redundancy. Each trip system, i.e., a pair of channels, is connected to a separate power supply. During normal operation, all sensors and logic devices are in the non-tripped state.

A number of conditions, as defined in Ref. 3, can initiate a scram. Each of the RPS inputs are independently monitored by each channel. When a sensor signal exceeds the set point of the analog comparator unit (ACU), the ACU output changes state. The RPS is not tripped by a single signal, but another channel in the other trip system independently sensing a similar signal will satisfy the logic requirement and will de-energize all scram pilot solenoid valves causing a scram.

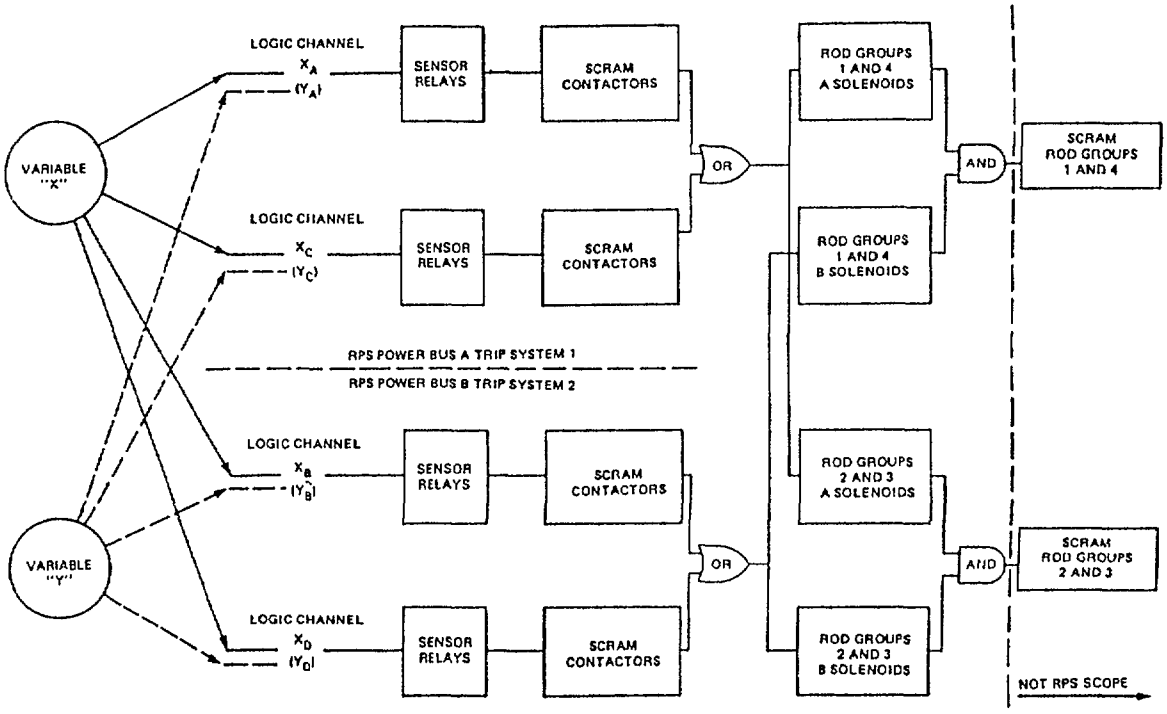


Figure 3.1. RPS relay configuration (reproduced from ref. 3)

The fault tree for the system considering the logic configuration and the success requirements for various RPS initiating signals is provided in Appendix A of GE NEDC-30815P (Ref. 3). The fault tree model, which was reviewed and considered adequate in the INEL study[5] was used in this study.

3.2 RPS Test Procedure and its Implication on Failure Detection

The technical specification of RPS requires that each RPS instrumentation channel be checked for operability by the performance of the channel check, channel functional test, and channel calibrations. These checks are performed on-line and are performed for various sensors detecting trip conditions. Typical test interval is one month, but for some designs the interval has been extended or is being considered for extension to 3 months. The placement of these surveillance requirements for different channels for the various sensors is analyzed in this study.

There are two other types of surveillances performed on the RPS. One involves the logic system functional tests and simulated automatic operation of all channels, and in the other the response time of each reactor trip functional unit is tested. Both these tests are to be performed at 18 month intervals and these are not considered in this study.

Each sensor channel function test includes full actuation of the associated logic, the scram contactors in each channel, and the individual scram pilot solenoid valves. Any failure in the channel to de-energize the solenoid valve is detected during the test. The broad steps in a typical channel test procedure includes verification that the pilot solenoid valves are energized, verification that no other channels are in calibration or test, setting of the stable current in the calibration unit, slowly decreasing the calibration current until the trip occurs, recording the trip and, if necessary, performing adjustments, and asking the operator to reset the half scram and to verify the associated alarm. (A half scram condition defines the situation when one trip system based on

either one of its two channels has provided a signal that de-energize one solenoid valve for each of control rod unit. A complete or full scram condition, where an actual scram takes place, occurs when the other solenoid valves for each of the control rod units are also de-energized.)

The objective of a surveillance test is to detect any failures and to repair or replace, as necessary. However, the performance of the test itself may also result in a failure, that may or may not be detected during the test. In addition, errors in following the procedure may also result in non-detection of failures. The placement of tests influences these associated errors.

Types of Errors Associated with Testing of RPS Channels

The errors associated with testing of RPS channels include failure of individual components and also common-cause failure of multiple components. For the RPS, consisting of very reliable components, common-cause failures are likely to be the dominant contributors to the system unavailability. In this section, various types of common-cause or dependent failures associated with testing are discussed.

Failure to Detect a Common-Cause Failure of Multiple Channels

The test procedure followed for a channel essentially involves feeding a scram signal and observing the half scram at the control panel. Following a test of one channel, the half scram signal is to be removed and the test should continue for another channel. However, a potential human error exists due to a lack of adequate communication, that the operator will fail to remove the half scram whereas personnel performing the test will assume that half scram has been removed and will proceed to test another channel. This will result in non-detection of failure in the second channel since the half scram that signifies a successful operation of the channel already exists. In a similar manner, the test of the remaining channel will proceed and, due to the existence of half scram, any failure present in these will also remain undetected. Thus, the error in this case is the common-cause error of failure to remove half scram for the remaining channels following the first channel test. The effect of the error is the non-detection of any common-cause failure present in the remaining channels. In this type of error, the first channel is successfully tested, but the failures present in the remaining three channels are not detected resulting in a system failure. If one assumes a common-cause failure of all four channels, then following the detection of failure of first channel one will proceed to repair the channel. At the completion of repair, when one proceeds to retest the channels, the error described above is likely to result in non-detection of the failures in the remaining channels.

The error being discussed essentially depends on the adequacy of communication between the operator and test personnel. One can distinguish between the two types of this error. One in which the half scram has not been removed for Channels B, C, and D at a given test. The other is where the half scram is not removed for Channels B, C, and D repeatedly at consecutive tests. The second is less likely unless it involves some systematic or procedural cause.

From the description of the error it is apparent that such an error is more likely when more than one test is being performed at a time. We will now discuss the effect of this error on detection of common-cause failure of the RPS scram contactors for different test strategies.

Consider a sequential test strategy in which each RPS sensor variable is tested in sequence for the four channels. In such a strategy, the test will continue from channel A to B to C to D, for example, for high reactor pressure sensor variable and following completion of test of all channels for a variable, the test will proceed for the next variable. In this test set up, if failure of scram contactors in any combination of channels exist, the error discussed above

will result in non-detection. In considering this error, the removal of half scram may take place at the very end of the test when sufficient time has elapsed or at the end of four channel tests for each sensor variable as opposed to each separate individual channel test. The modeling of this error is considered for this type of sequential test strategy in the next chapter.

Another type of sequential test strategy will involve testing each channel for all the variables before proceeding on to the next channel. In this strategy, if the error being discussed takes place, it will result in non-detection of common-cause failure of the scram contactors if the half scram is removed at the very end of the test. However, if the half scram is removed at the end of each channel test for all the variables, then the contactor failure in each channel can be detected. The improper testing of each channel for various sensor variables with failure to remove half scram may result in improper calibration for the variables, but the common-cause failure of the scram contactors will not remain undetected. This type of sequential test strategy is not specifically modeled in this analysis.

In a staggered testing strategy where testing of the four channels in the system are separated from each other, the error being discussed cannot result in non-detection of the common-cause scram contractor failure.The staggered testing strategy is effective in removing the effect of this type of error because it provides separation of sufficient duration between the channel tests such that the existence of the half scram is detected and removed.

An alternate staggered testing strategy could be where the tests are staggered in terms of the variables, i.e., all four channels for each variable will be tested at a time and the tests for the variables will be staggered. In such a strategy, the potential for the error being discussed exists and this type of staggered test strategy is not effective if the effect of such errors is to be minimized.

Failure of Multiple Channel at the Test Due to Human Errors (Human Error Common Cause)

During a test or following a test, a human error can disable a component wherein the component will not be available if needed in an accident. If multiple components are being tested together, a common-cause potential exists where the human error will fail all the components being tested. Two possibilities exist. In one, the failure occurs during the test, but detected and repaired before the test is completed. In the other, failure occurs at the end of the test and is not detected until the following test. Both of these types of failures are considered in the GE report (Ref. 3) and are analyzed in this study.

Specifically, the human error common-cause failure of importance in the GE RPS is that associated with the scram contactors. The two scram contactors in each logic channel are normally de-energized whenever an individual sensor and its associated relays are tested. Following the completion of a logic channel test, the contactors are re-energized. During this period the test personnel will disable the component such that it can fail to de-energize when a trip signal is received in the channel. The human error common-cause failure results when test personnel disable the scram contactors in the remaining channels following the failure in the first channel. In the following, the implication of these failures are analyzed in terms of the human errors in scram contactor failures for different testing strategies.

In a sequential testing strategy, tests of the channels are performed one after another and a failure in one can propagate to others. The type of failure that occurs during the test and is repaired before the test is completed will result in a common-cause failure of all the channels depending upon the repair strategy that is followed. To explain further, consider a test of channel A,

and a human error that disables the channel. If the error is detected before the channel test is completed, it will be corrected before proceeding on to test channel C, thus eliminating the potential for common-cause failure. However, if the error is committed, but not detected until at least three of the channels are failed and then corrected, then the common-cause failure exists due to this error for the short duration of the test time of the channels. The common-cause failure due to the error during the test is not likely and will have minimal impact on RPS unavailability. The other type of failure which disables the component at the end of the test and remains undetected until the next scheduled test is possible under the sequential testing strategy and its impact is evaluated in Chapter 4. The assumption of this failure is the same as that in the GE report (Ref. 3) except that different probabilities of this failure occurring were analyzed.

In a staggered testing strategy, the human error common-cause failure that disables all the scram contactors in the four channels A, B, C, and D is highly unlikely due to staggering of the channel tests. Sufficient time is expected to have elapsed between channel tests to remove any dependency among human errors from one channel to another. However, there is a small likelihood of this error occurring if it involves some systematic or procedural cause. In the application carried out in this study, the human error common-cause failure due to procedural causes (for example, wrong procedure) was considered negligible.

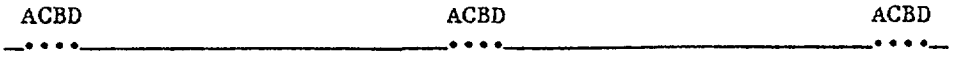
3.3 Selection of Test Strategies for Evaluation

The test strategies evaluated in this study for the RPS are composed of a sequential and two different staggered testing strategies. As the discussion in Section 3.2 entails, different sequencing of tests of the channels for various sensor variables is possible for either of the strategies. Also, different types of staggering can be implemented and two different staggered test strategies that are operationally feasible and attractive from a reliability standpoint are studied. In this study, the RPS unavailability for a particular sensor variable (MSIV closure) was evaluated and the strategies analyzed are presented below and shown in Figure 3.2.

Sequential Test Strategy: In this test strategy all four channels are tested, one after another in the following sequence - Ch. A, Ch. C, Ch. B, and Ch. D, at the interval defined. Two possibilities exist for testing all sensor variables. Either each variable is tested for all four channels or each channel is tested for all the variables. Assumptions in this study are more applicable to the sequential testing where each variable is tested for all channels.

Evenly Staggered Test Strategy: In this test strategy, the testing of the channels are evenly staggered in the test interval defined. For example, for the RPS system consisting of four channels and a prescribed test interval of 4 weeks, this strategy will imply that Ch. A is tested at the end of the first week, Ch. B is tested at the end of the second week, Ch. C is tested at the end of the third week, and Ch. D is tested at the end of the fourth week. However, since the system is dominated by common-cause failures, whenever a failure is detected it is likely to be a common-cause failure as opposed to an individual component failure. Accordingly, in this strategy two possibilities exist whenever a failure is detected. One is to strictly follow the test strategy, i.e., even if a failure is detected in one channel, say Ch. A, the testing of Ch. B will be performed as scheduled, i.e., one week from the test of Ch. A and so on for other channels. The other approach will be to test all other channels and perform necessary repairs following detection of a failure in any one channel. In this approach, the common-cause failure that may have occurred will be corrected at the earliest opportunity. This second approach to testing was considered as part of this staggered test strategy. Admittedly, this approach provides a higher benefit of staggered testing as opposed to that obtained in the alternate approach of strictly following the staggered strategy.

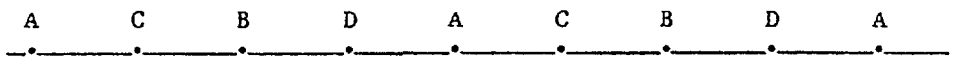
Semi-Staggered Test Strategy: In this strategy, one channel from each trip system is tested sequentially, but staggered with respect to the remaining two channels which are also tested sequentially. That is, for the RPS with a 4 week test interval, Ch. A and B are tested sequentially at the end of the second week and Ch. C and D are tested sequentially at the end of the fourth week. The advantage of such a test strategy is that the test associated common-cause failures discussed in Section 3.2 could only fail two of the channels and will not cause system failure. It also reduces the number of test setups necessary in an evenly staggered strategy although it is more than that required in a sequential test strategy.



Sequential Test Strategy

4 weeks

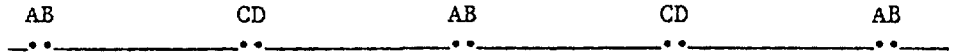
$P(CCF\text{-}HE) = P(A)\ P(CBD/A)$



Evenly Staggered Test Strategy

1 week

P(CCF-HE) = Residual value (e.g., the possibility that the operator does not reset to a failed signal and simply terminates the test).



Semi-Staggered Test Strategy

2 weeks

P(CCF-HE) = P(A) P(B/A) P(C) P(D/C)
(still requiring two independent failures)

A: Signifies test of Channel A
B: Signifies test of Channel B
C: Signifies test of Channel C
D: Signifies test of Channel D
(P(CCF-HE): Probability of human error common-cause failure of the channels.
P(A): Probability of human error failure of Channel X (X is either A,B,C, or D).
P(CBD/A): Probability of human error failures of channels B, C, and D given a failure in Channel A.

Figure 3.2. Different test strategies analyzed for a 4 week test interval for the RPS relay plant

3.4 Analysis of RPS Unavailability

The function of the Reactor Protection System (RPS) is to scram the reactor for various initiating events. The GE Report (Ref. 3) in its analysis of RPS unavailability divided the initiating events into three groups depending upon the number of diverse scram sensors that initiate the scram. Group I consists of 7 different initiating events with a total initiating frequency of 3.84 per year and Groups II and III consist of one event each with an initiating frequency of 0.54 and 0.02 per year, respectively. In this study, the scram for the MSIV closure event, which represents all the events in Group I because of the similarity in the extent of scram diversity, was analyzed.

The RPS unavailability for the MSIV closure event was calculated using the FRANTIC III computer code. The GE fault tree of RPS for this initiating event was used in the analysis, preserving the minimal cut sets with unavailability greater than 1×10^{-11}. The "min cut upper bound" formula was used in the FRANTIC analysis to obtain the system unavailability. The estimates for the FRANTIC model parameters is the same as that in the GE report (see Table B-1 and C-1, ref. 3) except in the situations where it was changed to perform the sensitivity evaluations.

The top event for the RPS fault tree is described as any one of the three events: a) simultaneous failure of Channels A and C, b) simultaneous failure of Channels B and D, or c) common-cause failure of the scram contactors. Among the three, the common-cause failure (Item (c)) dominates the system unavailability. In order to recover the common-cause failure, at least one contactor in each trip system, i.e., one scram contactor out of each pair of Channels A,C and B,D, should be repaired. Because of the dominance of the common-cause failures, the analysis presented in the next chapter focussed on this failure and the use of test placement in detecting and recovering from such failures.

4. RESULTS OF EVALUATION OF TEST STRATEGIES FOR GE REACTOR PROTECTION SYSTEM

The RPS unavailability for the MSIV closure event was analyzed for different test strategies described in the previous chapter and for changes in the test intervals. Sensitivity analyses were also performed for common-cause failure probability estimates and for changes in test duration time and allowed outage times. In this chapter, the benefits of staggered testing in reducing the system unavailability are discussed. Details of the evaluations are presented in Appendix A.

4.1 Benefit of Staggered Testing in Reducing the Average System Unavailability

The RPS average unavailability was studied for different test strategies (sequential, evenly staggered, and semi-staggered) to determine the reduction in the average unavailability that can be obtained through use of test strategies for the redundant channels. The different test strategies are described in Chapter 3 and the assumptions associated with each of the strategies are presented in Appendix A. Figure 4.1 presents the RPS unavailability as a function of the test intervals for different test strategies, and Table 4.1 provides the factor reduction in the RPS average unavailability when evenly-staggered and semi-staggered test strategies are used compared to a sequential test strategy.

The results show the benefit of staggered testing and the benefit depends on the common-cause human error failure probability, CCF(HE), of the scram contactors in the system. When common-cause human error of the scram contactors is present and its failure probability is of the order of 5×10^{-5}, a significant reduction in the RPS average unavailability is achieved due to either a evenly-staggered or a semi-staggered test strategy, where the probability of such a failure is negligible. Besides the effect of the staggered testing strategy in significantly reducing the common-cause human error contribution, it provides a

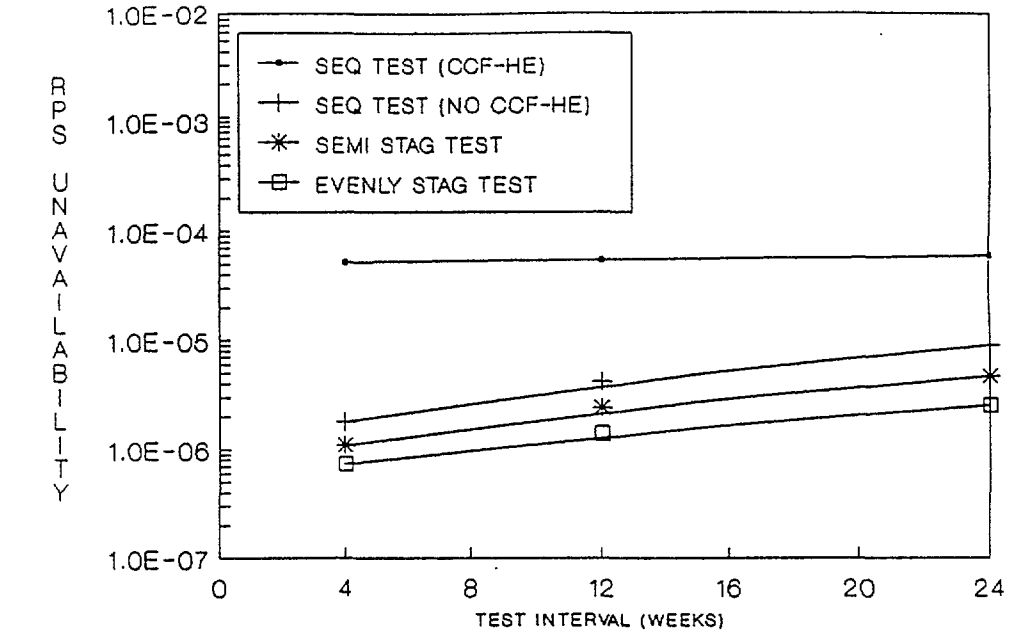


Figure 4.1. RPS average unavailability as a function of test interval for different test strategies.

Table 4.1. Benefit of Staggered Testing in Reducing Average RPS Unavailability

	Factor Reduction in RPS Average System Unavailability			
Test Interval	Evenly Staggered Strategy		Semi-Staggered Strategy	
	CCF(HE)=0	CCF(HE)=5.0(-5)	CCF(HE)=0	CCF(HE)=5.0(-5)
4 weeks	2.43	70.	1.63	47.1
12 weeks	3.0	38.5	1.75	22.5
24 weeks	3.56	23.5	1.93	12.8

reduction in the independent failure contribution and the contribution from common-cause failures that occur between tests. In the RPS average unavailability, this reduction is about a factor of three and two, respectively, when evenly-staggered and semi-staggered test strategies are considered. These results were obtained by comparing the RPS unavailabilities for the different test strategies assuming CCF(HE) = 0 in sequential test strategy.

The reduction in RPS average unavailability also depends on the test interval. For the RPS, the reduction in the average unavailability increases, not significantly, when common-cause human error is not a dominating contributor. The reduction decreases when common-cause human error is a dominating contribution (for evenly-staggered test strategy, the factor reduction in average unavailability decreased from 70 to 24 when test interval is increased from four to 24 weeks). This is because the common-cause human error probability, CCF(HE) is the same for different test intervals, and at higher test intervals, its dominance is reduced due to increased contribution of other failure causes (independent failures and common-cause failures occurring between tests).

A comparison of evenly-staggered strategy and semi-staggered strategy shows that the reduction in the RPS average unavailability is about a factor of two higher for the evenly-staggered strategy. The choice of a suitable staggered strategy depends on the acceptable level of system unavailability desired. When the primary objective is to reduce the potential for common-cause human error of the scram contactors that disables the system, the use of any of the two staggered strategies studied will suffice.

4.2 Benefit of Staggered Testing in Reducing the Peak System Unavailability

In a staggered test strategy, the individual component peak unavailabilities are distributed according to the different test times and consequently, the peak unavailability for the system is lower. In deciding on a test strategy, it is important to consider the peak system unavailability along with the average unavailability, since the peak unavailability can be significantly different even if the average unavailability is the same.

The RPS peak unavailability was analyzed for sequential, staggered, and semi-staggered strategies. The reduction in RPS peak unavailability was less than a factor of 2 compared to that obtained for RPS average unavailability (Tables 2.2 and 2.3).

4.3 Benefit of Staggered Testing in Reducing Common-Cause Failure Contributions to the System Unavailability

The test strategy employed in a system influences various contributors to system unavailability and the benefit of a staggered strategy compared to a sequential test strategy depends on the relative contribution of these contributors, namely, the independent failure contributions, human error common-cause failure contributions, and contributions from common-cause failures occurring between tests. In a system consisting of highly reliable components, common-cause failures (those occurring between tests and those due to human errors) are the dominant contributors. The GE RPS being analyzed in this study has similar characteristic where the common-cause failures contribute about 97% of the system unavailability. In this section, the benefit of staggered testing in reducing common-cause failure contributions in the GE RPS is presented by varying the assumptions of the common-cause failure contributions. The details of the sensitivity analysis conducted are presented in Appendix A.

Figure 4.2 shows the RPS average unavailability (test interval = 12 weeks) for changes in the contribution of common-cause failures occurring between tests (signified by changes in CCF(T)) and for different assumptions in the human error common-cause failure probability CCF(HE). The common-cause failure rate of non-detection, CCF(Non-Det.) (discussed in Section 3.2 and in A.1 of Appendix A), was assumed to be 2×10^{-3}, but similar results are obtained when this parameter is increased assuming increased dependence among the errors.

Table 4.2 presents the factor decrease in RPS average unavailability for evenly-staggered and semi-staggered test strategy compared to sequential test strategy for the various assumptions in common-cause failure contributions. Since the RPS unavailability is dominated by the common-cause failure contributions, the decrease in system unavailability is essentially due to the decrease in the common-cause failure contributions due to staggered testing. The results presented in Table 4.2 show that the benefit of staggered testing depends on the relative contribution of common-cause failure probability. When human error common-cause failure contribution is negligible, the factor decrease in the system unavailability due to staggered testing remains the same for assumption of increased common-cause failure (occurring between tests) rates. The presence of human error common-cause contribution shows different behavior where the benefit in system unavailability (in factor reduction) decreases as the common-cause failure (occurring between tests) rate increases. As the contribution of common-cause failures occuring between tests increases, it dominates the system unavailability, and the reduction is essentially the reduction obtained for this

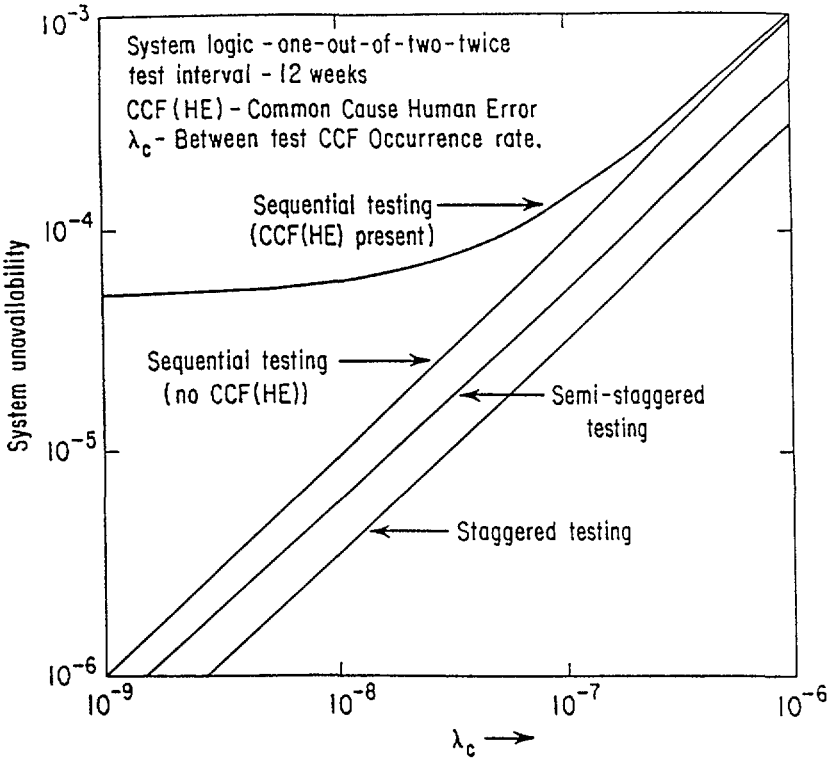


Figure 4.2. RPS average unavailability as a function of common-cause failure (occurring between tests) rate for different test strategies.

Table 4.2. Factor Decrease in RPS Average Unavailability Due to Staggered Testing for Changes in Common-Cause Failure Contribution (test interval = 12 weeks)

Common-Cause Failure Rate (Occurring Between Tests	Factor Decrease in RPS Average Unavailability (test interval = 12 weeks)			
	Evenly-Staggered		Semi-Staggered	
	CCF(HE)=0	CCF(HE)=5×10^{-5}	CCF(HE)=0	CCF(HE)=5×10^{-5}
4×10^{-9}	3.0	38.5	1.75	22.5
4×10^{-8}	3.0	6.7	1.75	4.0
2×10^{-7}	3.1	3.75	1.8	2.4
4×10^{-7}	3.1	3.28	1.8	2.1

contribution. Since staggered testing is assumed to eliminate the human error common-cause failure contribution, when this contribution dominates, the reduction is high and depends on the magnitude of human error common-cause failure probability.

4.4 Tradeoffs Between Surveillance Test Interval Increases and Staggered Testing Benefits

The system unavailability increases from surveillance test interval increases can be countered by system unavailability decreases from staggered testing. This implies that changes in surveillance requirements can be made to ob-

tain operational flexibility without changing the risk level in the plant. Where sequential testing is currently performed, increases in test interval can be obtained by trading off the risk increase using a staggered test strategy. The increase in test interval that can be obtained without affecting the risk level in the plant depends on the different risk contributors and the effect of staggered testing in reducing the contributions. Figure 4.3 presents a plot of change in the RPS average unavailability with staggered testing versus the increase in test interval. The intersection of the curve with the x-axis, which signifies no change in the system unavailability, determines the increase in test interval allowable with the staggered testing.

The analysis of RPS unavailability shows that the test interval can be increased by factors two to three, depending upon the type of staggered strategy used without affecting the current level of average system unavailability. When human error common-cause failure is a dominant contributor to system unavailability sequential testing, a much larger increase in the test interval can be obtained by staggered testing where probabilities of such failures are eliminated or significantly reduced.

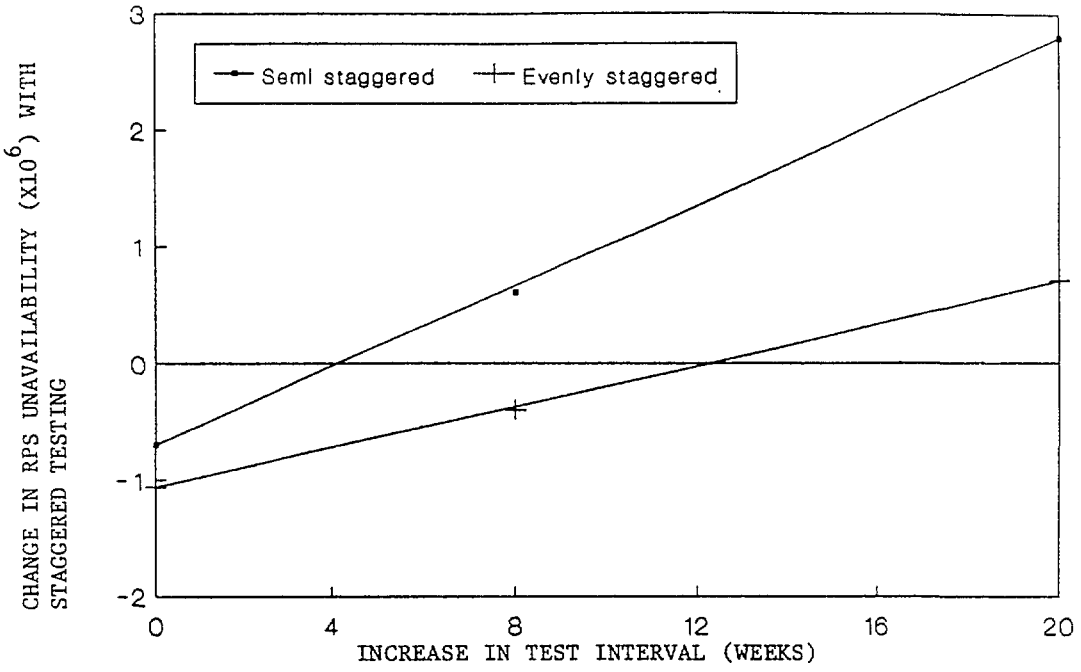


Figure 4.3. Tradeoffs between surveillance test internal increases and staggered testing benefits (human error common-cause failures in sequential testing assumed negligible).

5. SUMMARY AND CONCLUSIONS

The report presents an evaluation of the effect of test placement in system unavailability using GE Relay Plant RPS as an example. It provides a description of the various attributes in reliability evaluations that are affected by the test placements. The study focussed on the beneficial aspect on test placement. It did not attempt to quantify aspects associated with operational implementation that may have an adverse impact. A summary of the insights obtained from this study is presented below.

1. Adequacy of Tests

In deciding test intervals and test placements in standby safety systems to assure an acceptable level of system performance, the tests performed on the components or trains of the system should be adequate to detect the appropriate failure modes. The placement of the tests cannot improve the adequacy of the test procedure, and in this study, the tests are considered adequate and the improvement to be obtained by test placement is analyzed under that assumption.

2. Test Placement in a System Dominated by Common-Cause Failures

This study analyzed the benefit of test placement in a system dominated by common-cause failures. The example system chosen, GE Relay Plant RPS, is dominated by common-cause failures and a detailed evaluation of the common-cause failure contributors was performed. If human error related common-cause failure is present or dominant, a staggered test strategy can be used to eliminate or significantly reduce this contribution. For the RPS, the results show that a semi-staggered strategy, which is operationally more attractive than an evenly or perfect staggered strategy, would achieve most of the available benefits. A staggered strategy can also be used to reduce the effect of common-cause failure occurring between tests through early detection. The benefit depends on the type of staggering used; for the RPS with 1-out-of-2-twice logic, a factor of 3 reduction in average and peak unavailability can be achieved. The overall benefit in system unavailability dominated by common-cause failures, depends upon the relative contribution of the types of common-cause failures and given a test interval of 12 weeks for the RPS, the factor reduction in unavailability varies from 3 to 30.

3. Test Placement in Systems Dominated by Random Failures

System unavailability dominated by independent random failures of components can benefit significantly using a staggered test strategy. The improvement to be obtained depends on the system logic configuration and this aspect has been studied extensively in reliability literature (Ref. 1). In this study, the effect on system unavailability dominated by random failure contributions due to staggered strategy is explained (Chapter 2). The benefit to be gained in such situations can be significant, depending upon system logic.

4. Effect of Assumption in Common-Cause Failure Probability Estimation

Associated with the estimation of common-cause failure probability or rates, as applicable, is the uncertainty due to sparsity of data. Since test placements are considered in reducing the effect of these failures, the associated uncertainties in estimation of these failures should be considered. In this study, a sensitivity evaluation was performed to gain an understanding of this aspect. An approach in dealing with such issues is to perform bounding evaluation, i.e., using some upper bound estimate to check the implication obtained from the analysis using average estimates. For human error common-cause failures CCF(HE), a sensitivity evaluation that assumes a higher dependence among failures shows increased significance of a staggered test strategy. For time-related common-cause failure, CCF(T), the benefit of a staggered strategy compared to a sequential strategy remains the same under various estimation assumptions. In deciding on a test placement, one must clearly identify the potential of common-cause human failures that exist.

5. Consideration of Test Placement in Deciding Test Interval Extension

Current technical specifications are usually silent on test placements, but it is important to consider both the test interval and the test placements. In deciding on an increased test interval, the goal is to define adequate testing policy both from the operational and safety viewpoint. The results in this study indicate that test placement is as significant as the test interval. The

effect of test placement can even be higher than that of the interval between the tests. For example, in the GE RPS, the effect of increasing the test interval from 4 weeks to 12 weeks for a sequential test strategy is about a factor of 2.5 increase in average unavailability. Whereas for a 12-week test interval, a staggered test strategy can reduce the unavailability by factors of 3 to 30 depending on the type of common-cause failures present. One approach to defining an operationally attractive, at the same time appropriate from a safety viewpoint, technical specification requirement for a very reliable system like RPS, can be a large test interval with an appropriately defined test strategy.

6. Selection of an Appropriate Test Strategy

The selection of an appropriate test strategy for a system depends on the failure contributors present in the system and also on the acceptable level of unavailability for the system. In this study, the options or choices in the placement of tests are studied through an evaluation of sequential, evenly staggered, and semi-staggered strategies. As presented, a semi-staggered strategy for the GE RPS would eliminate or significantly reduce the human error common-cause potential. As discussed, because of the dominant failure modes associated with failures of scram contactors, staggering with respect to the channels is more important than staggering with respect to the variables for which the channels are tested. In the RPS, each of the four channels are tested for twelve variables. To obtain the benefit of test strategy through reduction of common-cause failures in the system, an effective strategy will be staggered testing with respect to the channels, but sequential testing for the variables for each of the channels. A sequential test strategy can also be applicable if the system unavailability remains within the acceptable level of unavailability. Current practice of testing the scram contactors in the GE RPS from the control panel using a staggered strategy at 7-day intervals and performing sequential testing of the channels during surveillance testing will result in RPS average unavailability below 4.2×10^{-6}.

REFERENCES

1. Green, A.E., and Bourne, A.J., Reliability Technology, John Wiley & Sons, 1978.

2. Vesely, W.E., et al., "Evaluation of Diesel Unavailability and Risk Effective Surveillance Test Intervals," NUREG/CR-4810, May 1987.

3. Sullivan, W.P., et al., "Technical Specification Improvement Analyses for BWR Reactor Protection System," NEDC-30851P, May 1985.

4. Letter from T. Pickens to H. Denton, "Staggered Testing of BWR Reactor Protection System Instrumentation Channels," January 1987.

5. Collins, B.L., and Wright, R.E., "A Review of the BWR Owners' Group Technical Specification Improvement Analysis for the BWR Reactor Protection System," EGG-EA-7105, Rev. 1, November 1986.

APPENDIX A

DETAILED RESULTS OF RPS SENSITIVITY EVALUATIONS

A.1 RPS Unavailability for Sequential Testing

The sequential test strategy for the RPS channel tests is considered in this analysis with the following assumptions:

1. The channels are tested sequentially in the order of A,C,B, and D at 12 week intervals.

2. If any channel is found failed at test, it is repaired before proceeding on to test the next channel. As discussed in Section 3.2, this assumption removes detectable human error common-cause failure during the test.

3. All instrumentation, including scram contractors, are tested only at the respective channel test.

4. The system is recovered from the common-cause failure of scram contactors, that may have occurred following the previous test or between test intervals, only after tests and repairs of at least A,C,B contactors in channel A,C, and B (this follows from the RPS fault tree). Thus, RPS unavailability due to common-cause failure of scram contactors is set to zero every 12 weeks.

Table A.1 presents the RPS average unavailability and peak unavailability in a sequential test strategy with a test interval of 12 weeks. Figure A.1 presents the time dependent plot of the unavailability. As evident from the results, the RPS unavailability is dominated by common-cause failure of the scram contactors (without this failure, the unavailability is of the order of 2.6×10^{-9}), and in the following, a brief description of various types of common-cause failures contributing to RPS scram contactor failure probability is presented. The scram contactor common-cause failure probability, CCFR1, is the sum of the following contributions.

1. Demand-related common-cause failure, CCF(Demand) - This failure is associated with a demand on the component and its probability is a constant. This contributor can be influenced by the number of demands due to the demand-caused wear out, but is not influenced by the test interval or the test strategy. Contribution of this failure mode to the RPS unavailability is of the order of 4×10^{-7} and reaches peak value of $\sim 8 \times 10^{-7}$ due to associated repair contributions.

2. Standby-time related common-cause failure, CCF(Time) - This type of common-cause failure of the contactors is detected at the test, but is associated with a common-cause human failure of detection, CCF(Non-Detection), as discussed in Section 3.2. A failure rate of 4.0×10^{-9} for CCF(Time) was used in the analysis based on the assumption in Ref. 3. CCF(Non-Detection) was incorporated in the FRANTIC model using the parameter p, which describes the probability of test inefficiency to detect standby-time related failure. CCF(ND) occurs due to operator failure to remove half-scram following the test of a channel.The CCF(Non-detection) probability is calculated to be 0.002, based on a probability of failure of 0.01 to remove half-scram after first channel (A) and a probability of failure of 0.1 and 1 respectively for successive failures following channel C and Channel D tests.

The average contribution to unavailability due to CCF(Time) and CCF-(Non-Detection) is of the order 3.8×10^{-6} and this contribution is influenced by the test interval and the test strategy.

3. Human Error Common-Cause Failure, CCF(HE) - This failure causes failure of all the contactors, but is not detected until the following test. This probability acts as a constant and directly adds to the RPS unavailability. The estimated probability was assumed to be 5.0×10^{-5} and is higher than that used in Ref. 3. The high RPS average and peak unavailability shown in Table 1 when all the different types of common-cause failures are considered is due to this error. When the potential of CCF(HE) does not exist or is so small that it is insignificant, then the RPS average unavailability is of the order of 4.2×10^{-6} and the peak unavailability reaches $\sim 8.9 \times 10^{-6}$ (Figure A.1).

Table A.1. RPS (MSIV Closure) Unavailability in a Sequential Test Strategy (12 Week Test Interval) for Various Common-Cause Contributors.

Common Cause Contributors	RPS Average Unavailability	RPS Peak Unavailability
CCFR1 = 0.0	2.6(-9)	5.0(-9)
CCF(D) = 4.0(-7) CCF(HE)= 0.0 λ,CCF(T) = 0.0 CCF(Non-Det.) = 0.0	4.0(-7)	8.0(-7)
CCF(D) = 0.0 CCF(HE)= 0.0 λ,CCF(T) = 4.0(-9) CCF(Non-Det.) = 2.0(-3)	3.8(-6)	8.5(-6)
CCF(D) = 0.0 CCF(HE)= 5.0(-5) λ,CCF(T) = 0.0 CCF(Non-Det.) = 0.0	5.0(-5)	1×10^{-4}
CCF(D) = 4.0(-7) CCF(HE)= 0.0 λ,CCF(T) = 4.0(-9) CCF(Non-Det.) = 2.0(-3)	4.2(-6)	8.9(-6)
CCF(D) = 4.0(-7) CCF(HE)= 5.0(-5) λ,CCF(T) = 4.0(-9) CCF(Non-Det.) = 2.0(-3)	5.4(-5)	1.1(-4)

CCF(D) - Common-Cause Demand Probability
CCF(HE)- Human Error Common-Cause Probability
λ,CCF(T) - Failure Rate of Time-Related Common Cause
CCF(Non-Det.) - Common-Cause Non-Detection Probability

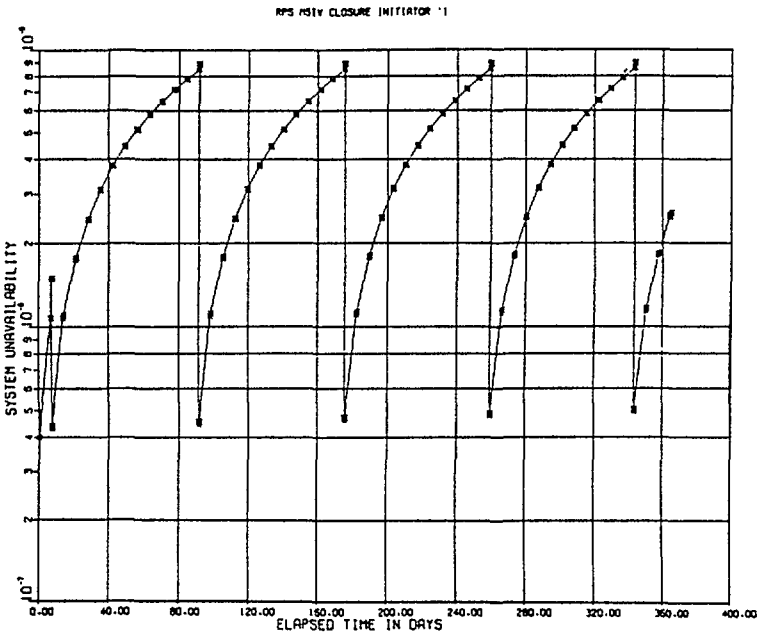


Figure A.1. Time-dependent plot of RPS (MSIV) unavailability for sequential testing (12 week test interval)

The results presented in Table A.1 show the relative contribution of different types of common-cause failures on the RPS unavailability. The separation is beneficial since the test placement affects some of these contributors thus allowing an estimate of the reduction that may be achieved.

A.2 RPS Unavailability for Staggered Testing

In this section, two alternatives to the sequential test strategy, evenly staggered and semi-staggered strategies, are considered. Although they have different maintenance and repair requirements, they both result in a shorter interval for detection of standby common-cause failures and they both decrease chances for common-cause failures due to human error. These two strategies and the associated assumptions in obtaining the RPS unavailabilities are presented below.

Evenly Staggered

1. Channel A,C,B, and D tests are evenly staggered; every channel test interval is 12 weeks, the interval between any two channel tests is 3 weeks.

2. Scram contactors and associated channel instrumentation are tested when a channel is tested.

3. If a channel is found to be unavailable during the test, the remaining channels are tested additionally after its repair.

4. The repair, if needed, always starts immediately after the test that detects the failure.

As follows from assumptions #3 and #4, the system can recover from being failed due to common-cause failure of scram contactors after each channel test, i.e., the RPS unavailability due to standby common-cause failures of scram contactors is set to zero every 3 weeks.

In this test strategy, common-cause human errors, CCF(HE) can occur only during additional testing, if a channel is found to be failed. But since channel failures occur with the low probability, the conditional contribution of RPS unavailability due to common-cause human errors is considered negligible in such a test strategy.

Semi-Staggered

1. Channels A and B are tested sequentially (channel test interval is 12 weeks); D and C Channels are tested sequentially but staggered with respect to Channel A and B tests.

2. The repair, if needed, always starts after the test and before proceeding on to test the other channel.

As follows from assumption 1 and the RPS system logic, the system can recover from being failed due to common-cause failures of scram contactors after test and repair of A,B or D,C contactors. Thus, the RPS unavailability due to standby common-cause failure of scram contactors could be set to zero every 6 weeks.

Channel B (or C) failure is not detected if the operator fails to remove the half scram position after the Channel A (or D) test resulting in non-detection. Then it will take another 6 weeks after repair of the A (or D) contactor to detect Contactor B (or C) failure. The probability of the event that omission error will not occur after the A (or D) contactor test is (1-0.01)-0.99. Thus, the probability that the RPS unavailability due to standby common-cause failure CCF(Time) will be set to zero every 6 weeks is 0.99.

The possibility of common-cause failure due to human error, CCF(HE), of simultaneously disabling all contactors is assumed negligible for this test strategy, since two groups of test i.e., A,B and D,C are performed independently of each other.

The common-cause failure of non-detection, CCF(Non-Detection), does not result in RPS failure in this strategy. The possibility of simultaneous failure of Channels A and B or Channels C and D due to non-detection does not exist; only Channels B and C can remain failed due to CCF(Non-Detection). But this will not prevent the RPS from generating the scram signal.

Table A.2 lists the RPS average and peak unavailabilities for these two test strategies are compared with the sequential strategy from Table A.1 and Figures A.2 and A.3, respectively present the time-dependent plots. Expectedly, RPS unavailability obtained for semi-staggered strategy is higher (70%) than that for evenly staggered strategy. The semi-staggered strategy provides much of the benefit of staggered testing from a reliability viewpoint by eliminating human error associated common causes, CCF(HE) and CCF(Non-Det.).

A.3 Effect of Increase in Test Interval

For each test strategy (sequential, evenly staggered, and semi-staggered) the RPS unavailability was evaluated, varying the channel test interval as shown in Table A.3.

The RPS unavailability shows an increase when test intervals are changed for any one of the three strategies. However, if CCF(HE) is included in the sequential strategy, the result will be dominated by this failure and the RPS unavailability for this strategy will show little variation. The results presented show the effect of other failure contributors. The primary effect is due to the standby-time related common-cause failures, CCF(Time).

Table A.2. RPS (MSIV) Average and Peak Unavailability for Different Test Strategies (Test Interval is 12 Weeks)

Test Strategy	RPS Average Unavailability	RPS Peak Unavailability
Evenly Staggered	1.4(-6)	2.8(-6)
Semi-Staggered	2.4(-6)	4.9(-6)
Sequential	4.2(-6)	8.9(-6)

Evenly Staggered: Channel A, C, B and D tests are equally staggered with 3 weeks interval. After detection of any channel failure, the remaining channels are tested additionally and repaired if needed.

Semi-Staggered: A and B channel tests are performed sequentially; D and C channel tests are performed sequentially and evenly staggered with the A and B channel tests. There is no additional testing after failure.

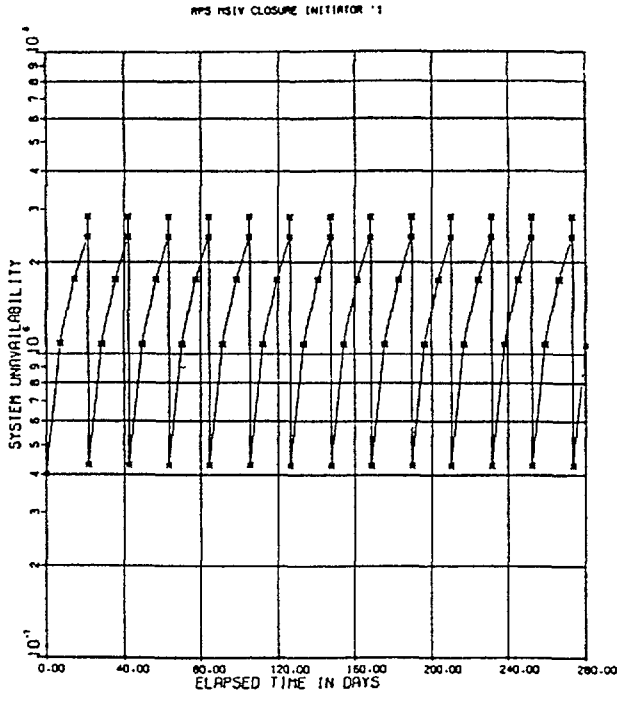


Figure A.2. Time-dependent plot of RPS (MSIV) unavailability for evenly staggered test strategy (12 week test interval)

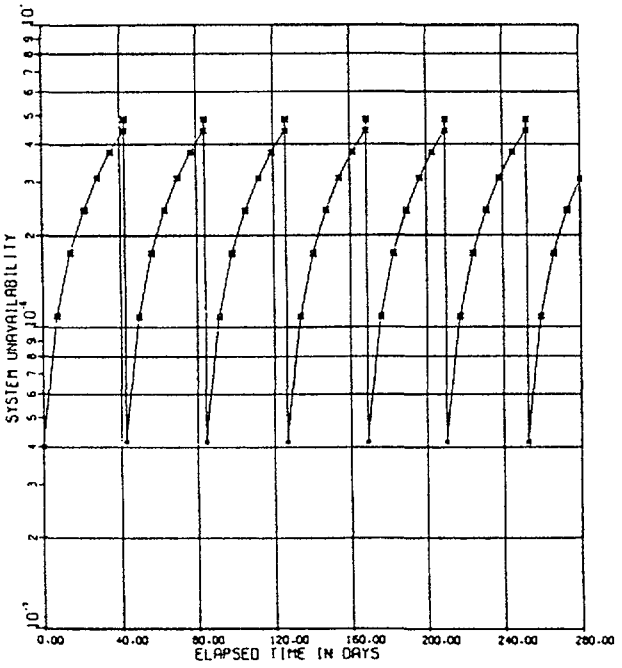


Figure A.3 Time-dependent plot of RPS (MSIV) unavailability for semi-staggered test strategy (12 week test interval)

The effect of an increased test interval on RPS unavailability for either of the three strategies is comparable. (Factor of 5 for sequential, factor of 4.2 for semi-staggered, and factor of 3.4 for evenly staggered). Another important point to note is that RPS unavailability for an evenly staggered or semi-staggered test strategy with 12 weeks test interval is comparable to RPS unavailability for sequential test strategy with 4 weeks test interval.

Table A.3. Effect of Increased Test Interval on RPS (MSIV) Unavailabilities for Different Test Strategies (CCF(Non.Det.)=2.0(-3), CCF(HE)=0)

	RPS Unavailability					
	Sequential Strategy*		Staggered Strategy			
			Evenly Staggered		Semi-Staggered	
Channel Test Interval	Average	Peak	Average	Peak	Average	Peak
4 Weeks	1.8(-6)	3.6(-6)	7.4(-7)	1.5(-6)	1.1(-6)	2.2(-6)
12 Weeks	4.2(-6)	8.9(-6)	1.4(-6)	2.8(-6)	2.4(-6)	4.9(-6)
1/2 Year	8.9(-6)	1.8(-5)	2.5(-6)	4.9(-6)	4.6(-6)	9.5(-6)

*Human error common cause, CCF(HE) for scram contactors was assumed not to be present (CCF(HE) = 0).

A.4 Effect of Increase in Test Time and Allowed Outage Time

The RPS unavailability was also studied for changes in the test time, τ and the allowed outage time (AOT) under two different testing strategies - sequential and semi-staggered. The results are presented in Table A.4 for different sets of values for τ and AOT.

The effect of change in τ and AOT on RPS unavailability for either of the test strategies is found to be insignificant. For the evenly staggered strategy, the impact is expected to be even lower.

Table A.4. Effect of Increased Test Time and Allowed Outage Time on RPS (MSIV) Unavailability for Sequential and Semi-Staggered Test Strategies

	RPS Unavailability			
	Sequential Strategy*		Semi-Staggered Strategy	
	Average	Peak	Average	Peak
τ = 2.0 hrs. AOT = 1.0 hrs.	4.2(-6)	8.9(-6)	2.4(-6)	4.9(-6)
τ = 6.0 hrs. AOT = 12.0 hrs.	4.4(-6)	9.1(-6)	2.5(-6)	4.9(-6)

τ: Test Duration

AOT: Allowed Outage Time

*CCF(HE) = 0

A.5 Sensitivity of RPS Unavailability to Common-Cause Failure Probability

The RPS unavailability was evaluated by varying the assumptions in the estimation of the common-cause failure contributors. The estimation of three types of common-cause failure of the scram contactors - CCF(Time), CCF(Non-Det.), and CCF(HE) are considered in a sequential test strategy. In general, since the RPS unavailability is dominated by these failures, the effect of assuming increased dependence among these failures significantly impacts the unavailability. Table A.5 summarizes the results obtained in this sensitivity evaluation.

The failure rate associated with CCF(Time) was increased from 4.0×10^{-9} to 4.0×10^{-7} where complete dependency (β=1.0) among the failures is assumed. The change in this failure rate linearly impacts the RPS unavailability, i.e., for a two order of magnitude change in this failure rate, the RPS unavailability also increases two orders of magnitude from 4.2×10^{-6} to 8.1×10^{-4}. The impact on RPS unavailability is even higher when this error is assumed in addition to a complete dependency (β=1.0) in CCF(Non-Det.).

Table A.5. Effect of Estimation Errors for the Common-Cause Failure Rate of Scram Contactors, and Common-Cause Non-Detection on RPS (MSIV Closure) Unavailability (Sequential Test Strategy, Channel Test Interval Equals 12 weeks)

	RPS Unavailability Sequential Testing, Test Interval = 12 Weeks							
	λ,CCF(Time) =							
	= 4.0(-9)		= 4.0(-8)		= 2.0(-7)		= 4.0(-7)	
	Average	Peak	Average	Peak	Average	Peak	Average	Peak
*CCF(ND)=2.0(-3) (β = .1)	4.2(-6)	8.9(-6)	3.9(-5)	8.2(-5)	1.9(-4)	4.1(-4)	3.8(-4)	8.1(-4)
CCF(ND)= 1.0(-2) (β = .5)	4.3(-6)	9.1(-6)	3.9(-5)	8.4(-5)	2.0(-4)	4.2(-4)	4.0(-4)	8.3(-4)
CCF(ND)= 2.0(-2) (β = 1.0)	4.5(-6)	9.4(-6)	4.1(-5)	8.7(-5)	2.0(-4)	4.3(-4)	4.1(-4)	8.6(-4)
CCF(HE)=5.0(-5)	5.4(-5)	1.1(-4)	8.7(-5)	1.8(-4)	2.4(-4)	5.0(-4)	4.2(-4)	9.1(-4)

* CCF(ND) = CCF(Non-Detection)

The effect of increased dependency on CCF(Non-Det.), i.e., β, changed from 0.1 to 1, is not significant. Comparing the values within a column in Table A.5, the increase in RPS unavailability is ~8% and remains more or less the same for different failure rates associated with CCF(Time).

The human error common cause CCF(HE), when included in the RPS unavailability calculation, is added to the other contributors and typically, dominates the unavailability. The dominance of this contributor decreases as the failure rate associated with CCF(Time) is increased, since then this term also becomes a significant contributor.

A.6 Comparison of Sequential vs Staggered Test Strategy

Table A.6 shows the values of average and peak RPS unavailability depending on the type of human error for three different test strategies: sequential, evenly staggered, and semi-staggered. A comparison of RPS unavailabilities for these three strategies is also obtained from Figures A.1 through A.3.

The RPS unavailability with sequential test strategy is obtained considering CCF(HE) that disables all contactors following a test and is detected only at the next test. In this case, the corresponding difference with an evenly staggered test strategy respectively for RPS average and peak unavailability is about a factor of 30. It is about a factor of 2 when evenly staggered and semi-staggered strategies are compared. When CCF(HE) is neglected, the average and peak system unavailabilities are about three (3) times higher for sequential strategy compared to corresponding values for a evenly staggered strategy and is about a factor of 1.8 higher compared to the semi-staggered strategy.

In the RPS system, or any similar system dominated by common-cause failures, the effect of a staggered strategy can become significant if CCF(HE) type of error is a dominant contributor. In that situation, any form of staggered strategy that eliminates or significantly reduces this error should be employed. Otherwise, the use of staggered strategy depends on the level of reduction being sought. In that case, some of the reduction is compensated by the increased risk due to an increase in the number of test-caused transients, if applicable. Other operational implementation aspects discussed in Chapter 2 should also be considered.

Table A.6. Comparison of Sequential vs Staggered Testing for RPS (MSIV Closure) Average and Peak Unavailabilities Depending on the Type of Human Errors; CHE or IC

Type of Human Error	Sequential Strategy		Staggered Strategy				Benefit of Staggered Testing			
	RPS Unavailability		RPS Unavailability				(Decrease in RPS Unavailability)			
			Evenly Staggered		Semi-Staggered		Evenly Staggered		Semi-Staggered	
	Average (a)	Peak (b)	Average (c)	Peak (d)	Average (e)	Peak (f)	Average (c-a)	Peak (d-b)	Average (e-a)	Peak (f-b)
CCF(HE) = 5.0(-5) CCF(D) = 4.0(-7) λCCF(T) = 4.0(-9) CCF(NonDet)=2.0(-3)	5.4(-5)	1.1(-4)	1.4(-6)	2.8(-6)	2.4(-6)	4.9(-6)	5.26(-5)	1.1(-4)	5.16(-5)	1.1(-4)
CCF(HE) = 0.0 CCF(D) = 4.0(-7) λCCT(T) = 4.0(-9) CCF(NonDet)=2.0(-3)	4.2(-6)	8.9(-6)	1.4(-6)	2.8(-6)	2.4(-6)	4.9(-6)	2.8(-6)	6.1(-6)	1.8(-6)	4.0(-6)

Next page(s) left blank

Appendix II

DECISION ON CONTINUED PLANT OPERATION OR SHUTDOWN IN FAILURE SITUATIONS OF STANDBY SAFETY SYSTEMS

Abbreviations

AOT	Allowed outage time (failure state of a component)
BD	Blowdown: reactor steam relief to condensation pool
CCF	Common cause failure
CO	Continued operation of the plant
ESD	Event sequence diagram
FW	Feedwater function
LCO	Limiting conditions for operation
MCS	Minimal cut set
RHR	Residual heat removal (plant safety function)
SC	Shutdown cooling (plant state or safety function = = RHR)
SD	Shutdown of the plant (used mainly for the decided state change of the plant)
TS	Technical specifications (TechSpecs)

Safety events

LoFW	Loss of feedwater
LoRHR	Loss of residual heat removal
LoPC	Loss of cooling of condensation pool
CoOPS	Containment overpressurization state
CoPRe	Containment pressure relief
CoreD	Reactor core damage

Notations used for event sequences are specified in Table 4.1

Notations used for system modules are specified in Table 4.1

Notations used for risk variables are specified in Section 5.1

1 INTRODUCTION

1.1 Background

Technical Specifications (TS) set forth limits and operating conditions for the safe operation of a nuclear power plant. As part of these rules, the Limiting Conditions of Operation (LCO) define the allowed power operation time, when a safety-related component or system is known to have failed. The allowed component/system outage times (AOT) depend on the safety functions affected, and the remaining degree of redundancy. If the failures cannot be repaired during the AOT, the plant needs to be brought to a safe state, which usually means cold shutdown state. So far the AOTs have mainly been based on deterministic analyses presented in the Final Safety Analysis Report, and on engineering judgement.

The probabilistic methods, this far mainly used for overall probabilistic risk assessments (PRA), provide a systematic approach to evaluate the additional risk during the presence of component failures in safety systems, and to compare the risk of continued power operation, over the expected repair time, with the decided shutdown of the plant. The risk in the shutdown alternative includes transient risks associated to plant state change. Furthermore, when failure situations of the residual heat removal (RHR) systems are considered, the decreased reliability of the remaining parts of the RHR systems to start and operate may contribute significantly to the disadvantage of the shutdown alternative.

It was of interest to know how the continued power operation and decided shutdown alternatives actually compare with each other as risks, which motivated the application and required method development presented here.

At the TVO power company, the first applications of probabilistic approach concerned optimisation of periodic tests and preventive maintenance during power operation. In the next stage, the LCO specifications of AOTs were undertaken for systematic treatment. A pilot study of the LCO problems was made for a comparison of the blackout risk between continued operation and decided shutdown alternatives in case of diesel generator failures. The TVO units have only one turbine generator each, with relatively large size as compared to the Finnish main grid. Dimensioning in this regard complies with the Nordic design specifications. Yet, the risk of inducing a loss of external grid in shutdown disturbance transient was expected to be a potentially significant risk contributor. The insights obtained in the pilot study encouraged us to continue with an analysis of the systems involved in the RHR function, as this function seemed important for shutdown related risk, and hence most interesting from the risk comparison point of view.

The experiences of the early applications and related method developments are described in Refs.[ExPSA_TVO86, AOT_PRA81, ETS_PSA85, DECET85, PM_IAEA85].

The study for AOT issue for RHR systems was in the first stage done at the RHR function level. This study was described in the technical report [ESumRepo88], and contributed as a practical case study for the Nordic research project NKA/RAS-450 on optimisation of technical specifications by the use of probabilistic methods [NKA/RAS-450].

In the final stage, the study was extended to plant risk level, mainly due to the installation of the containment relief venting system in 1989. This system influences substantially the plant risk profile [IAEA90_M]. In fact, the loss of RHR function in a restricted sense becomes less critical, as the steam relief from the containment can be used as a last resort for removing decay heat, assuming that sufficient feed water is available for reactor core cooling. However, the auxiliary feed water system and emergency injection systems are functionally dependent on the RHR systems. Consequently, even the results of the final stage showed that the decided shutdown constitutes a higher risk than continued power operation over usual repair times of less than one day. The recommended modifications of AOT rules and operating procedures are under way.

This report is intended to describe in detail the application as being completed in the final stage, extending the earlier publications about the case study [ESumRepo88, IAEA90_M].

1.2 New methodological features

The successful treatment of the AOT issue has called for the development of new methodological ideas in order to enhance modelling and quantification of the expected risk of operational decision alternatives - such as plant shutdown versus continued power operation in failure situations of standby safety systems - and how to take uncertainties into account in order to verify the confidence in conclusions. The main advances in the analysis methodology are concerned with:

- modelling of phased missions by using extended event sequence diagram
- consideration of recovery paths for safety functions
- implementation of time-dependent component models based on shared cause modelling of common cause failures

The methodological developments have been described in Refs.[ThesisM86, PhM_SRE86, PO_PSA89].

For the processing of event sequences and specific types of operational decision alternatives, a prototype computer program TeReLCO has been developed by Avaplan Oy with the support of TEKES Technology Development Centre of Finland and TVO power company [SRE_90PP].

1.3 Related work

This documentation is also intended to be used as underlying material, concerning further development and use of probabilistic methods in TS considerations, in the ongoing Nordic project NKS/SIK-1 "Safety Evaluation by the Use of Living PSA and Safety Indicators" (1990-93).

In the TVO application described here, there are many parallels with the TS developments done in other countries, specially in USA, in the research projects sponsored by NRC and EPRI, as well as to the recent developments in European countries and Japan. The related work is referred to in more detail in appropriate context. Some comparisons of the approaches will also be presented.

2 AOT PROBLEM SPECIFICATION

During the unavailability time of safety system components due to repairs or 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 power operation in such a situation is usually limited. For this purpose, the term Allowed Outage Time (AOT) has 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 occurrence
- possible CCF event
- repair need of functionally noncritical faults or
- intentional disconnection of equipment for preventive maintenance

The AOTs depend also on the system configuration, number and dimensioning of redundancies, and on the system's safety importance [TSB_Mad87]. It should be noted that the term AOT is associated with the unavailability periods of a component or system, but there is not necessarily any plant outage concerned.

In the study described here, the AOTs for RHR system trains are considered. The results apply to all unavailability modes listed above, assuming the unavailability of the train (or trains) is known to the operator.

2.1 TVO plant description, RHR systems

TVO nuclear power plant, located in Olkiluoto, Finland, is operated by Teollisuuden Voima Oy (TVO). The plant consists of two identical ABB Atom BWR units. The net electrical power of a single unit is 710 MW [TVO_Pros].

The primary safety-related systems are divided into four redundant subsystems, usually called trains. The capacities of these subsystems were designed to correspond with 4x50% configuration, which fulfils the single failure criterion also with one subsystem temporarily disconnected for maintenance. However, due to conservative design assumptions, the actual capacities correspond in most demand cases with 4x100% configuration.

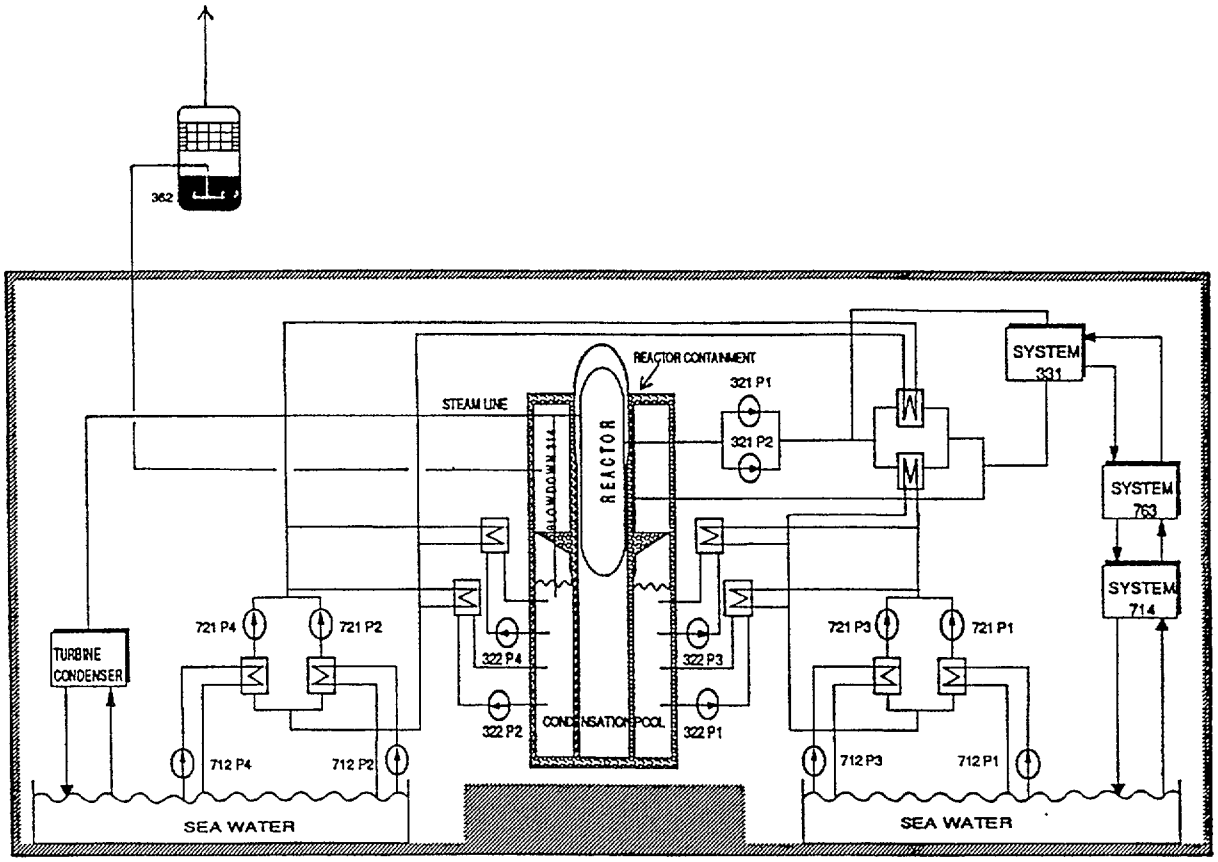
The four redundant subsystems are physically well separated, except that pairs of subsystems may share heat exchangers or other passive, piping components.

The systems that can be used for the RHR function are schematically presented in Fig.2.1. There are three diverse paths

321-721-712	Normal shutdown cooling path
322-721-712	Condensation pool cooling path
321-331-763-714	Backup shutdown cooling path

The normal shutdown cooling (SC) path is primarily used in cold the shutdown state, and during the refuelling outage. In this RHR mode, cooling water is circulated by system 321 pumps through the reactor core, and hence the feedwater function is not needed. Reactor pressure needs to be decreased below about 12 bar, in order to realign cooling flow through the 321/721 heat exchangers.

Pool cooling path is used in connection to blowdown transients, where steam is blown from reactor to condensation pool through the safety/relief system 314. This path can well be used for prolonged RHR by controlled blowdown through the regulating relief valves of system 314. In this RHR mode, steam released from the reactor to condensation pool need to be compensated,



314 = Relief system
321 = Shutdown cooling system
322 = Containment vessel spray system
331 = Reactor water clean-up system
362 = Containment filtered venting system
712 = Shutdown service water system
714 = Non-diesel backed normal operation service water system
721 = Shutdown secondary cooling system
763 = Heating system

Figure 2.1 Residual heat removal systems at the TVO plant (BWR).

i.e. some of the feedwater systems need to be operating. The primary system pressure can be kept at nominal full pressure of 70 bar, in order to minimize the heat release into condensation pool.

The backup SC path is actually the reactor water cleanup circuit. Its cooling capacity can be increased up to the level of decay heat production after about three hours from reactor shutdown. Up to this time, reactor steam can be dumped either to the turbine condenser or to the condensation pool, and feedwater is needed during that time. If steam is dumped to condensation pool during this initial reactor cooldown, pool temperature will increase during the three hours from nominal 20 °C up to about 40 °C, i.e. there is still a reasonable margin. After establishing backup RHR by the use of system 331, cooling water is circulated by system 321 pumps through the reactor core, i.e. the feedwater function is no longer needed. The reactor pressure can be kept up to full nominal pressure of 70 bar, as this is the normal operating pressure of the 321/331 heat exchangers.

The three paths have a specific order of operational preference, and interrelationships to feedwater function and primary system pressure control, which constitute important functional dependences to be taken into account in modelling.

2.2 Current AOTs for RHR systems

The current AOT rules for the four redundant RHR trains 721/712, which are representative for other modern 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

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 failure situations of system 721/712 trains (as in most other cases) this means cold shutdown of the reactor.

The 30 days AOT is also applied in the case of a disconnection for the repair of a random noncritical fault (concerns one subsystem at a time). It should be noted that according to operating experiences, the mean repair times of both the critical and noncritical faults of RHR train components are less than one day at the TVO plant [MiK_Dip, MTS_Dip].

Preventive maintenance is allowed to be performed during power operation within a total unavailability time of three days per subsystem per year [PM_IAEA_85].

2.3 Practical motivation to AOT reconsideration

Motivation to reconsideration of AOTs for RHR trains will be discussed in more detail in Section 3.6. It is, however, of high interest to notice that the current LCOs do not impose a shutdown requirement in case of system 321 being detected inoperable. LCOs just state that prompt measures should be undertaken in order to restore system 321. (In this case, the engineering judgement is well confirmed by risk analysis, which shows that shutdown of the plant with inoperable system 321 is not beneficial.) One of the principal motivations to the closer risk based study was the attention drawn by this discrepancy, as the LCO rules for the remaining part of the normal SC path, i.e. for system 721/712 trains seemed to be in a logical contradiction with the rules of system 321.

The RHR trains 721/712, however, also serve other cooling functions (pool cooling, AFWS component cooling, DG cooling etc.), and therefore it was not possible to deduce the actual risk aspects of the AOTs without a systematic modelling/ quantification approach.

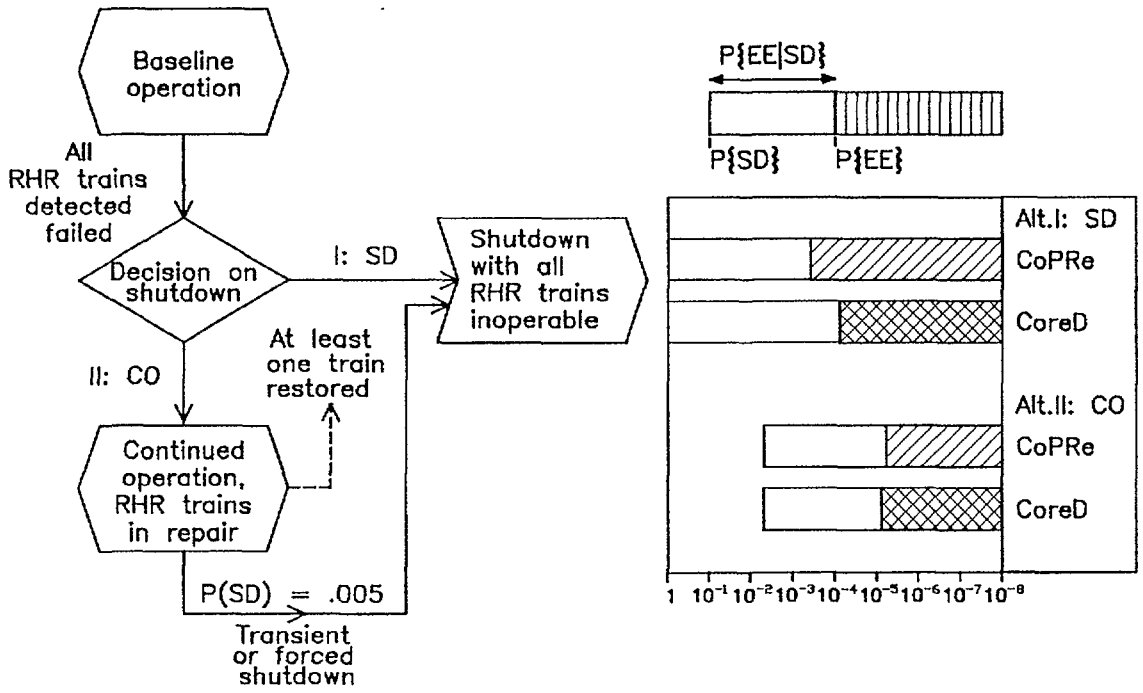
3 RESOLUTION STRUCTURE

In a nuclear power plant, the influence of a failure detected during power operation depends on the systems and safety functions affected. For most important systems, and in case of multiple failures, the risk level may be increased several orders of magnitude above the baseline. In such situations, it is a priority to find out the operational alternative of minimum risk until the baseline state is restored. The concept of baseline state is here used for the normal power operation state, where no failures or maintenance disconnections, of AOT concern and known by the operators, are present in the safety systems. This concept will be clarified and defined more precisely in Section 5.1.2.

3.1 Basic operational alternatives

The principal question is whether the plant should be shut down in a critical failure situation, or to continue power operation over the predicted repair time. These alternatives are illustrated by Event Sequence Diagram (ESD) in Fig.3.1, and will be discussed in more detail below. There are further alternatives such as

- Given a plant shutdown is needed, is it beneficial to test/startup the preferred residual heat removal (RHR) systems in advance prior to entering actual shutdown sequence as compared to startup in a late stage of shutdown? For example, the RHR systems should be operable at the time, when the main heat transfer system cannot be any longer used. The idea in performing the prior startup is the fact that it may be safer to postpone the plant shutdown, if the RHR systems are detected inoperable or degraded but can be repaired in a reasonably short time



Syntax

CO =	Continued operation of the plant over the repair time
SD =	Decided shutdown of the plant for the repairs
EE =	Undesired end event (CoPRe or CoreD)
CoPRe =	Containment pressure relief due to prevailing loss of RHR function
CoreD =	Core damage due to prevailing loss of feedwater/core cooling

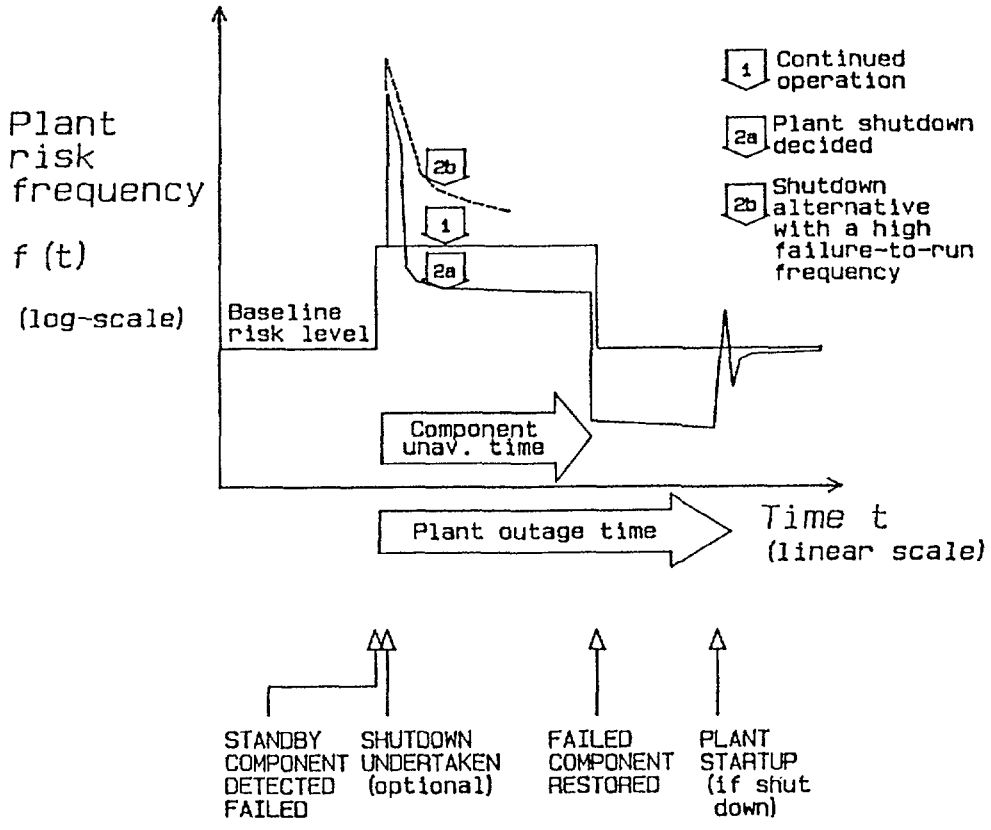
Figure 3.1 Modeling of operational decision alternatives by use of event sequence diagram, illustrated here in the case of all four RHR trains failed at the TVO plant. Likelihood of the plant shutdown with the associated challenge on RHR function, and the expected risk of undesired end events, are presented on the right hand side for the operational alternatives.

- Even when no plant shutdown requirement is actual, it can be questioned whether in case failures are detected in periodic tests, the operability of the remaining subsystems or redundant systems should be promptly checked? This question is specially relevant when the staggered testing scheme is used.

The benefits and risks of various alternatives may not be readily determined. The probabilistic methods can provide valuable aid in the problem resolution.

3.2 Continued plant operation versus shutdown

The increased risk level, known by the operator in a failure situation, is illustrated schematically in Fig.3.2. The operator faces alternative paths to proceed. The main decision to be made then is (compare also to Fig.3.1) whether to



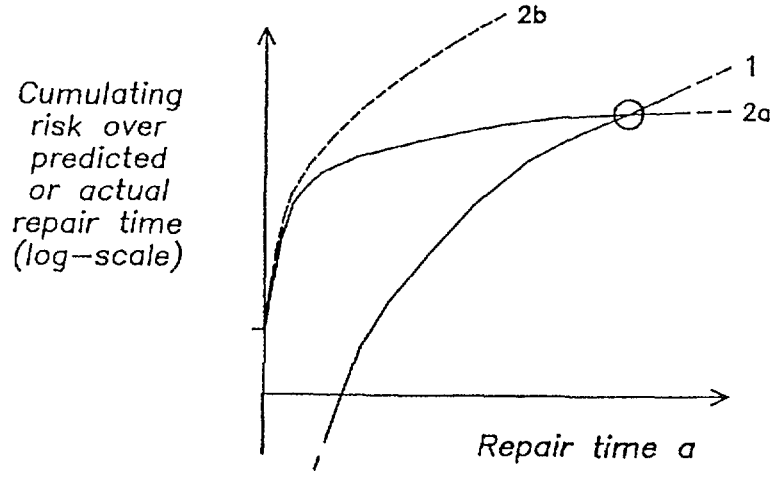


Figure 3.2 Conditional risk frequency in failure situation of a standby safety system with comparison between the operational decision of plant shutdown versus continued operation. The corresponding cumulative risks over prevailing failure state are presented in the lower part.

1) continue power operation over the repair time of the fault or

2) shut down the plant, which usually means to the cold shutdown state but may also mean some other low power state, where the faulted component's inoperability has a smaller influence.

As illustrated in Fig.3.2 (Curves 2a/b), the change of the operational state usually involves a risk peak arising from the

- unreliability of the systems, which are needed in the state change or 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 power grid, etc.)

In Fig.3.2, Curve 1 represents the case of continued power operation over the repair time. The risk associated with this alternative is the area below of Curve 1 and above the baseline.

In the case of decided shutdown, the risk frequency often decreases after the state change peak (Curve 2a), as the decay heat power decreases, which means lower capacity requirements on safety systems and longer available time for recovery if a critical safety function is lost.

3.3 Comparing risks over predicted repair time

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

The cumulative risk over predicted repair time is schematically illustrated in the lower part of Fig.3.2. The crossing point of Curves 1 and 2a represents the shortest repair, which, if exceeded, justifies the plant shutdown.

Achieving a lower risk level after plant shutdown, compared with the continued power operation, is the necessary precondition that the shutdown could at all be a safer state. In some cases the lower relative risk level may not be achievable. For example, if a part of the RHR systems is inoperable, the probability that the operable part fails to run in the plant shutdown state may be relatively so high, that the situation of Curve 2b, Fig.3.2, exists after shutdown. (The extreme example is the situation where the RHR systems are detected totally unavailable, in which case it is a trivial conclusion that the continued power operation with minimized disturbances is the safest state at least until a minimum residual heat removal capacity is restored.)

The relative risk constituted by continued operation and decided shutdown can be further clarified by the presentation of expected risk in the right part of Fig.3.1, where the

- left end of the bars represent the likelihood of RHR challenge, i.e. entering shutdown state with associated need to start up and operate RHR systems
- hatched subbars represent the risk of loss of RHR function including nonsuccessful recovery

- white area or band between these represents the conditional risk per shutdown, which can also be interpreted as remaining safety margin with the specified conditions (here the risks are presented in regard to two disjoint undesired end events, reactor core damage CoreD and containment pressure relief CoPRe, which will be defined and discussed in more detail in Section 5)

The first entity, likelihood of entering shutdown, is 100% for the decided shutdown, but relatively small in the continued operation alternative, as determined by the likelihood that some spontaneous transient or special forced shutdown need would occur during the repair time. In the TVO case, explained later in more detail, this likelihood is only about 0.5% over the average repair time of 12 hours for RHR system components, reflecting the low forced shutdown and plant trip rate. This is the main explanation to the results favouring continued operation as a safer alternative over usual repair times.

3.4 Influence of preset AOT

In the preceeding sections, the continued operation and shutdown were considered as operational alternatives in a failure situation, where some prediction can be made of the repair time. A preset AOT should reflect the crossing point after which the shutdown means smaller risk. The existence of AOT then influences the expected risk associated to failure situations - when considering them from the lifetime point of view - as this is composed of the contributions of repairs shorter than AOT with continued operation, and repairs exceeding AOT with plant shutdown. These contributions are schematically drafted in Fig.3.3.

The experiences show that if AOT is longer than the mean repair time, so a large part of faults will be repaired in a shorter time than AOT. This means that the expected contribution over component unavailability time while in power state saturates to a level corresponding to the risk over mean repair time. On the other hand, if AOT is short, the expected number of LCO shutdowns increases and also the associated risk contribution. This should be added to the previous contribution in order to achieve an objective correlation.

Finally, there exist also indirect influences, which are harder to evaluate. For example, it could be expected that an AOT shorter than normally needed to complete the repair, may result in negative side effects, if fault repairs are attempted hastily in order to avoid plant shutdown.

To conclude, considering the total influence of AOT on the long term risk, the schematic behaviour presented in Fig.3.3 can be drafted, with presumably broad minimum range but increase at small AOT values. Certainly, the actual sum curve may have different detailed forms depending on the plant specific features.

It should be noted, that in some other applications [EPRI5238, Wagner87], it is unrealistically assumed that given any AOT, it all will be used in every repair. This results in an erroneous

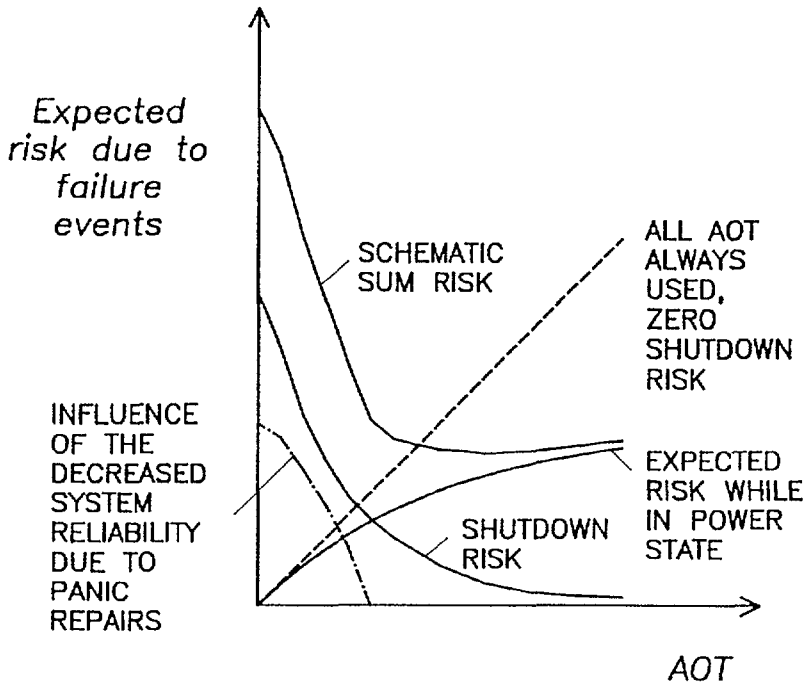


Figure 3.3 Schematic presentation of how a preset AOT influences lifetime expected risk (risk addition i.e. delta risk is presented).

correlation between the expected risk and AOT as illustrated in Fig.3.3. The stated assumption together with omitting shutdown risks means that the total risk would increase linearly as the function of AOT (dashed curve in Fig.3.3).

In recent publications [IAEA90_JP, PSA91_CS], the delta risk/AOT correlations of the form of Fig.3.3 are calculated for practical cases. As pointed out in more detail in Ref.[Te_dRAOT], the saturation of the expected contribution over component unavailability time while in power state is not properly taken into account. Furthermore, in practice a short AOT evidently influences the repair time, and this may affect substantially the likelihood of shutdown and thus the contribution of repairs exceeding AOT with plant shutdown, as shown by the sensitivity analysis for TVO/RHRS case in Ref.[Te_dRAOT]. Unfortunately, there are relatively few actual data about the influence of a short AOT on the component repair times. Also the uncertainties about the possible negative side effects of prompt repair attempts at short AOTs mean that the determination of the actual shape and the place of the eventual risk minimum of the delta risk/AOT correlation is quite difficult.

It should be emphasized that the influence of AOT on the expected lifetime risk is only one point of view. The instantaneous risk frequency and situation specific risk discussed earlier are other, and primary points of consideration for rare, high risk situations. Comparing risks over predicted repair time, for the continued operation versus decided shutdown alternatives, i.e. the placement of the

crossing point as illustrated in the lower part of Fig.3.2, should be regarded as the main guideline when determining a preset AOT. The delta risk/AOT correlation repeats the same information content in another form, but incorporates additional influences with associated increase of uncertainties. Therefore, the delta risk/AOT correlation curves are not included among the presentation of the results in this report.

The AOT criteria are discussed in more detail in [NKA/RAS-450], in many respects paralleling the scheme of Ref.[V&S_BNL89].

3.5 TS problem resolution strategy

The treatment of the AOT issue as a resolution problem is discussed here in light of the TVO/RHRS study, which extends significantly the scope of the analysis for the LCO issue. Principally, the minimum risk alternative is searched for the LCO rule (within specific constraints), in contrast to the considerations of acceptable risk increase over continued operation in the LCO state and the eventual trade-off between test interval changes, as has been done in some other applications [EPRI5238, Wagner87, V&S_BNL89].

In the resolution strategy structure proposed in [EPRI5238], the many kinds of constraints, which limit the possible resolution alternatives, are not considered as explicitly as their importance would necessitate. These should include

- technical constraints such as imposed by manufacturers for maintenance and test actions
- operational constraints, for example, dimensioning of personnel work load
- economical constraints: maintenance and test costs, power reduction or shutdown losses
- regulatory constraints

This has led to a restructured resolution flow diagram of Fig.3.4, where the constraints influence right at the beginning on the selection of resolution alternatives. This guarantees that practicable alternatives are selected for a deeper investigation.

Another important difference is the inclusion of a prestudy stage, because that is usually needed in order to clearly define the problem, outline possible resolution alternatives, and predict the analysis work required and expected benefits, prior to starting the actual, greater analytical effort.

Also the confinement of the analysis at the lowest (least resources consuming) level is structured in another way. In the original diagram, confinement of the work to the level at which the impact is acceptable is central. The emphasis should according to our view be placed on the search of

- "smallest risk alternative within the constraints"

compared to

- "acceptable risk increase".

The safety/cost justification of a probabilistic analysis should be understood in the broad meaning. All safety influences, expected operational or other practical benefits and disadvantages, as well as the analysis and modification costs shall be considered together.

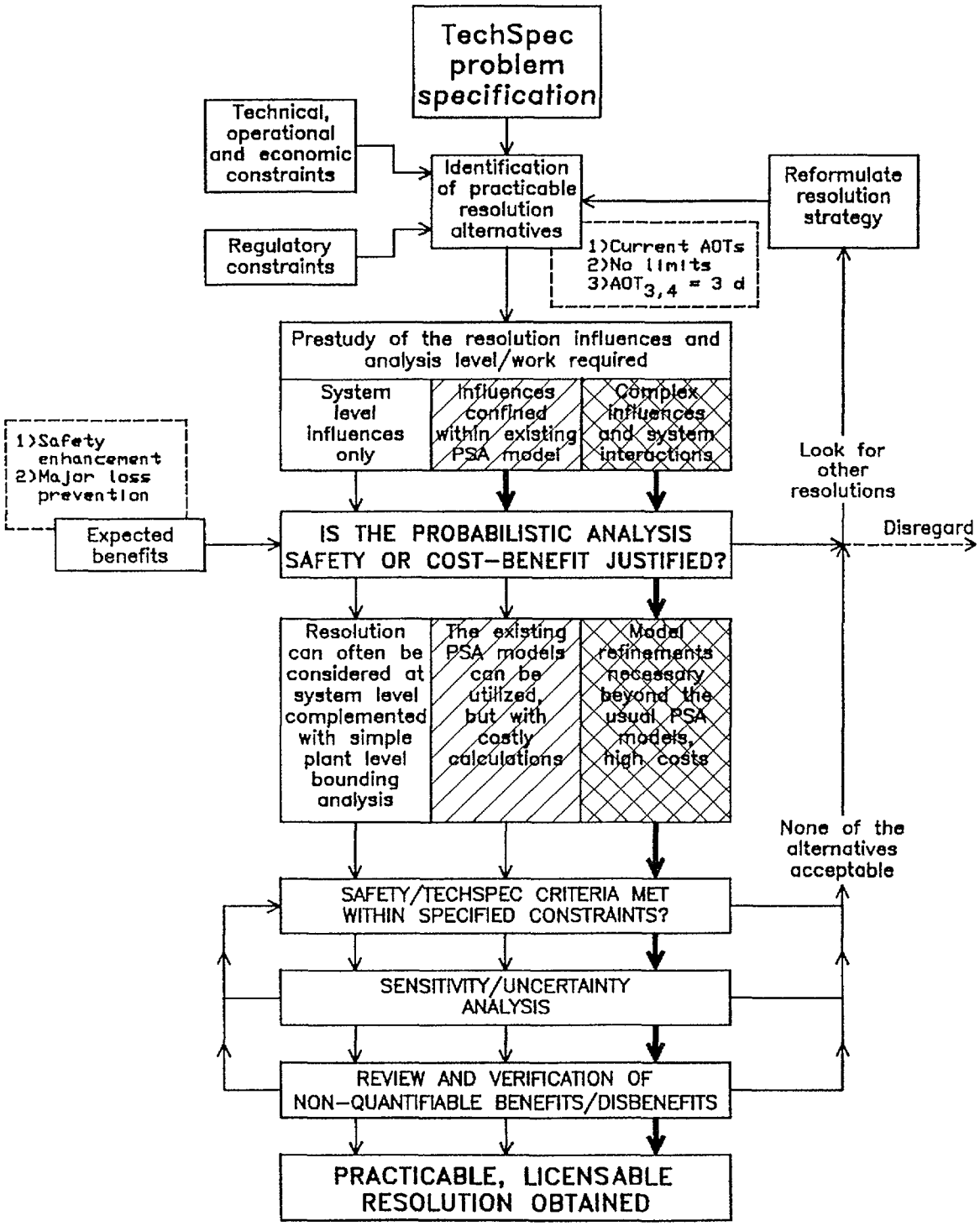


Figure 3.4 TS problem resolution strategy in the analysis of the AOT issue in the TVO/RHR system case.

3.6 Case study layout and phases

The resolution flow followed is presented in Fig.3.4. The background to the study was the general interest to compare LCO shutdown with continued operation in RHR system failure situations. Because RHR function is needed in shutdown state, the current LCOs were considered nonlogical, as they did not allow repair, in the cases of three or all four RHR trains 721/712 being inoperable during continued plant operation. This seemed contradictory also in comparison with system 321 LCOs, which do not include shutdown requirement as discussed in Section 2.3.

The expected benefits were potential safety enhancement and major loss prevention. It was estimated already in the beginning, that the influence in the production availability is minor due to the small likelihood of multiple failure situations.

Three principal LCO alternatives were specified

I Current AOTs (single failure 30 days, double failure 3 days, triple and quadruple failure no AOT)

II No LCOs (unlimited continued operation)

III AOT of 3 days extended to cases of three or four trains failed.

These will be discussed in more detail in Section 7 in connection to deduction of recommendable AOT modifications. Compare also to Table 7.1.

In the first stages, the analysis was started at the RHR function level. It became gradually evident that the analysis needs to be extended to plant risk level (corresponding to so called PRA Level 1) in order to properly take into account the functional dependences of other safety functions on the RHR function, i.e. cooling support provided by system 721/712 trains for the auxiliary feedwater system and diesel generators, and the dependence of the core spray system on the containment pool cooling path 322-721-712.

During the early stages of the study, no plant PRA was available. Furthermore, because in part of the modelling, more advanced methods were needed than is standard in PRAs, special effort had to be put in the confinement of the analysis within reasonable amount of resources. Fortunately, the study could be combined with preparation work for TVO/PRA, and later stages have been accomplished parallel to and benefiting from the PRA.

As many complex influences and system interactions have been covered, the need for a very careful treatment of the uncertainties was understood right from the beginning. Sensitivity analyses of different kind have been done extensively.

4 MODELLING OF SHUTDOWN COOLING MISSION

During the study, the modelling approach evolved from the conventional fault tree/event tree methods first applied, into a plant state/process oriented approach. The methodological developments are described in more detail in Refs.[PM_SRE86, PO_PSA89]. Here most essential features and application specific details are only outlined.

The notations and abbreviations used for the system modules, and basic events in sequence models are collected into Table 4.1.

4.1 Plant shutdown transient diagram

The modelling procedure applied can be characterised as a top-down approach. At the highest level of hierarchy, the decision/event sequence diagram is used. It describes the principal operational alternatives in a failure situation as relevant for AOT considerations, Fig.3.1.

At the next highest level of hierarchy, SD transient diagram is used to model initiating events, Fig.4.1. The initiating events represent beginning of failure paths, which may lead from the normal state or path of operation, through intermediate branches/states into undesired end events.

SD transient diagram includes initiating events at two levels. Firstly, there are modelled initiating transient events (ITR), which represent exit ways from the normal power operation state of the plant. The subdiagram for the first exit from the normal power operation - decided shutdown (DecSD) - stands in a special position for the comparison of operational alternatives in AOT considerations, as will be discussed in more detail in Section 4.3. The other exit events from the normal power operation include automated plant trip, or a need to manually trip the plant for a prompt shutdown.

SD transient diagram ends at transfer events, SC cooling initiating events (ISC). These are grouped in disjoint event classes representing most essential situations, where the RHR function is challenged.

SD transient diagram represents first phase of the shutdown mission. In a normal decided shutdown, proceeding in a planned way, this phase includes first about 3 hours up to the changeover of starting to use the normal SC path 321-721-712. In the transients with an automated plant trip, the first phase modelled by SD transient diagram is shorter.

4.2 Screening of initiating events

Selecting and grouping of initiating transient events is analogous to the approach established in PRA studies. SD transient diagram has similarities to the so called master event tree [PRA_PGuide]. The SC initiating events correspond with transfer events often used in order to structure large event trees onto different levels of hierarchy.

Table 4.1 Module and event notations.

System modules

M321	Module of shutdown cooling system 321
VA,VO	Containment isolation valves of system 321
PA	Pumps of system 321
M331	Module of reactor water cleanup system 331 including also heating system 763 and normal operation service water system 714 (non-diesel-backed)
Iisol	I isolation event (protections for leakage inside containment)
Yisol	Y isolation event (protections for leakage in interfacing safety systems)
VB	Flow arrangement for shutdown cooling via 321-721-712, including heat exchangers and manually operated valves
PU	Pump line of shutdown secondary cooling system 721
PM	Pump line of shutdown service water system 712
PL	PU + PM
316	Relief system
314	Condensation pool
PC	Pump line of containment vessel spray system 322
MFWS	Main feedwater system
TC	Turbine condenser
M733	Demineralized water distribution system
EWS	External water supply
AF	Pump line of auxiliary feedwater system 327
CS	Pump line of core spray system 323
TB	Automatic/manual depressurization of reactor
EB	Power supply of each sub (AC/DC)
AC	AC bus
DC	DC bus
AD	AC + DC
BI	Battery operation at loss of EPS
DG	Diesel generator
DP	DG + BI
DGX	Diesel generator of the other reactor block
EPS	External power supply

Shutdown cooling initiating events

0	Smooth	Gradual cooldown with steam dumping to turbine condenser
1	InitBD	Plant trip with initial blowdown to pool
2	Yisol	Y isolation event
3	IisBD	Spurious I isolation event
4	LePCi	Leakage of primary coolant inside containment (relevant I isolation)
5	UnMF	Unavailable main feedwater
6	LoEPS	Loss of external power supply
7	CCImAC	Common cause initiator affecting m out of 4 AC subs
8	CCImDC	Common cause initiator affecting m out of 4 DC subs

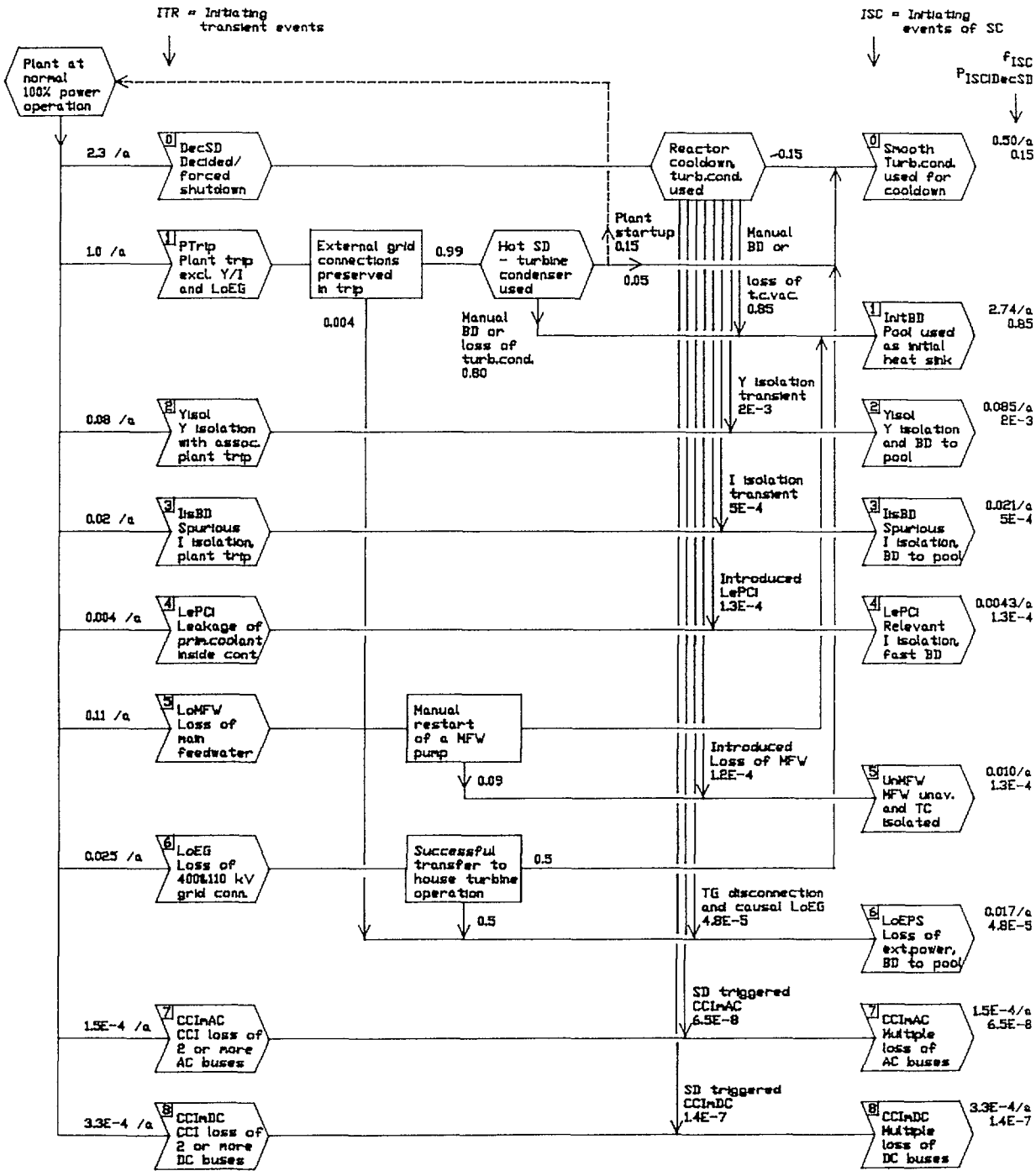


Figure 4.1 Shutdown transient diagram. Event notations are defined in Table 4.1.

In a failure situation of RHR systems, the relative importance of initiating events may substantially differ from the average contributions analysed in a PRA study. In general, those initiating events for which RHR function is an essential part of the plant response increase in importance.

Specially, such initiating events which are Common Cause Initiators (CCI) in regard to RHR function, i.e. both directly challenge RHR and render a part of the RHR systems unavailable, may increase drastically in relative importance, given that some part of the RHR systems is known to be failed initially. Very obvious CCIs in this regard are the

- loss of turbine condenser and
- loss of external power sources,

as these imply unavailability of the normal heat transfer system. Other potentially important CCIs may be global/local protections associated with RHR equipment (Y and I isolation at TVO I/II) or multiple failures of AC/DC supply system.

AOT considerations are aimed at comparison of the relative risks associated with a failure situation, especially the risk of continued operation over repair time versus decided plant shutdown. Therefore, different types of simplifications, often stronger than in a PRA, are motivated and acceptable.

It should be noticed that modelling here excludes those accident scenarios, such as ATWS events, where core damage may be caused prior to the time point when the use of RHR function would be relevant. Those risk contributions can be considered constant with respect to the consideration of AOT issue for RHR systems, and may hence be neglected from the relative risk considerations. Furthermore, in multiple failure situations of RHR trains, those risk contributions are small.

This study is also limited to so called internal initiators, which means that fire and flood initiators, for example, are not included in the considerations. The implications of this limitation will be further discussed in Chapter 6.

4.3 Relationship to operational alternatives

It is of special importance to notice that the SD transient diagram, specific for an AOT consideration, describes both

- continued power operation alternative: then initial plant state of full power operation is assumed, and it may be exited due to different initiating transients with associated frequencies (i.e. rate = probability per unit of time). The possible exits include also a decided shutdown forced by special circumstances (which may occur in addition to the failures of RHR systems assumed here as an initial condition for the consideration). During the plant state change when shutting down, additional branching of event sequences may occur until SC initiation transfer events. For example, loss of external grid may occur during continued power operation with a rate of 0.025/a. The corresponding exit event LoEG may branch with the chances

of about 50% just in Smooth SC initiating state, if automatic transfer to house turbine operation succeeds. Otherwise, it results in the loss of external power source state LoEPS in regard to SC initiation.

- decided shutdown alternative: then it is assumed that the normal power operation state is exited with a likelihood of 1 through the DecSD path. During reactor cooldown, disturbance transients may result in branching. For example, abrupt turbine generator disconnection may cause loss of external grid connections. The conditional probability of this is estimated to be 4.8E-5, including the likelihood of disturbance transient in power reduction phase, abrupt opening of generator breaker and introduced fall down of external grid.

The key idea of using SD transient diagram in this way is the benefit, that both operational alternatives are reduced into the same scheme with respect to more detailed and laborious modelling of system response. Modelling of the following phases of SC mission is done at the next level of hierarchy by event sequence diagrams for each disjoint SC initiating event, i.e. for the transfer events ending the SD transient diagram. The quantification results from that level can then be associated into SD transient diagram scheme through multiplication by

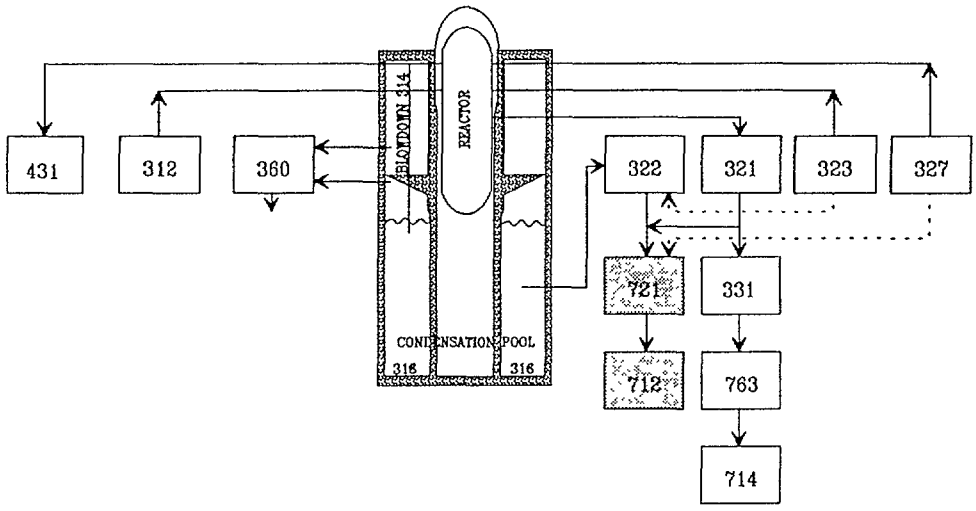
- SC initiating event frequencies f_{ISC} in order to sum up risk frequency for continued power operation alternative
- SC initiating event probabilities $P_{ISC|DecSD}$ in order to sum up risk for decided shutdown alternative

as will be explained in more detail, and by the use of mathematical expressions in Section 5.2.

4.4 RHR paths, modelling of shutdown cooling phases

The RHR paths as specified in Section 2.1 are presented with simplified flow/block diagram in Fig.4.2. Here, also feedwater paths are shown. These paths and associated systems are functionally interrelated. The auxiliary feed water system (AFWS), system 327 requires component cooling by RHR trains 721/712. The core spray system (CSS), system 323 presupposes pool cooling (path 322-721-712 operating) to preserve suction water temperature below 95 °C. In addition, there are important functional dependences for AC/DC power supply and protection isolations as will be discussed in more detail in the next section.

In the early stages of the analyses, performed at RHR systems and function level, several remarkable boundary conditions were assumed [ESumRepo88], specially in regard to feedwater systems. After installing the containment filtered venting system in 1989, the relative risk importance of RHR systems substantially decreased. Furthermore, due to the functional relationships with feedwater systems, it became evident that the modelling scope need to be extended to fully cover feedwater function in order to properly infer risk influences of failure situations of RHR trains 721/712.



System notations

312	Main feed water system
314	Reactor relief system
316	Condensation pool system
321	Shutdown cooling systems
322	Containment vessel spray/pool cooling system
323	Core spray system
327	Auxiliary feed water system
331	Reactor water cleanup system
360	Containment overpressure protection/filtered venting system
431	Condenser and vacuum system
712	Shutdown service water system
714	Non-diesel backed, normal operation service water system
721	Shutdown secondary cooling system
763	Heating system

Figure 4.2 RHR and FW systems, and their support systems at TVO I/II. This study is concerned with AOTs for RHR trains of systems 712 and 721.

As a principal boundary condition, there still remains the fact, that a prolonged steam dump or restoration of turbine condenser is not taken into account as RHR sink in later SC phase. This is mainly due to the fact that this kind of operation is not planned at TVO I/II. It would presuppose complex operations, which are not verified in practice. Operating experiences also show that dumping of steam to the turbine condenser is very unstable at low steam production rates. With regard to possible credit of turbine condenser, a sensitivity analysis was made using judged availability estimates for the recovery of turbine condenser, specific in different SC initiating events. This showed that the relative results between the operational alternatives would not be significantly affected.

4.5 Modelling of RHR, power supply and auxiliary systems

In system modelling, extended reliability block diagram is used, Fig.4.3.a-b. The extensions concern description of the functional dependences on support systems such as AC/DC power supply and component cooling. These are noted by arrows at the side of front line system modules, which makes the models intuitively simple and reasonably compact. This idea comes from the GO modelling approach [EPRI_GO].

The block diagrams serve well to describe the system configurations and so called hard wired functional dependences, but they are not full substitutes for system fault trees. There

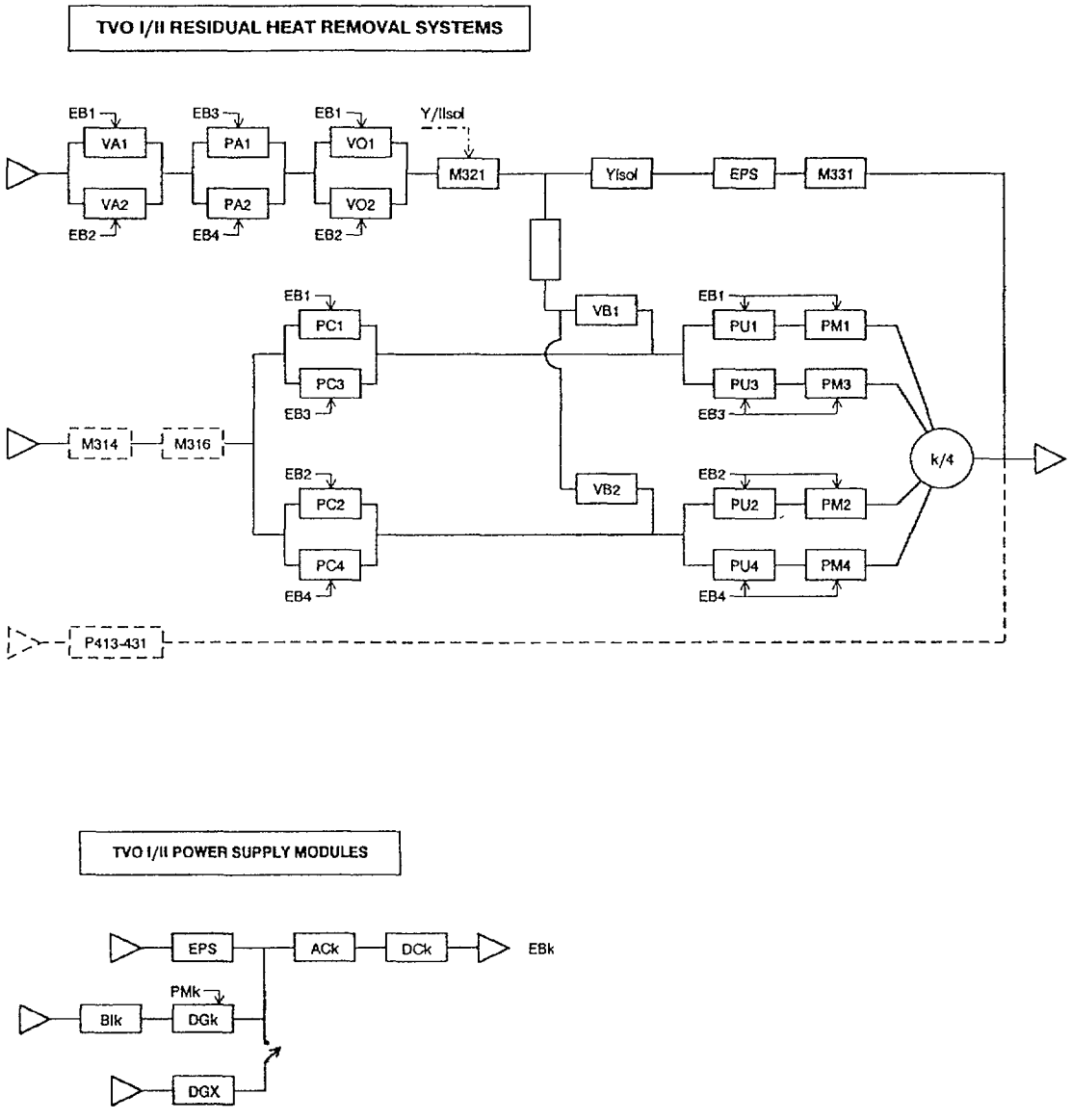


Figure 4.3a Reduced, modularised block diagrams for RHR systems and AC/DC buses. Module notations are defined in Table 4.1.

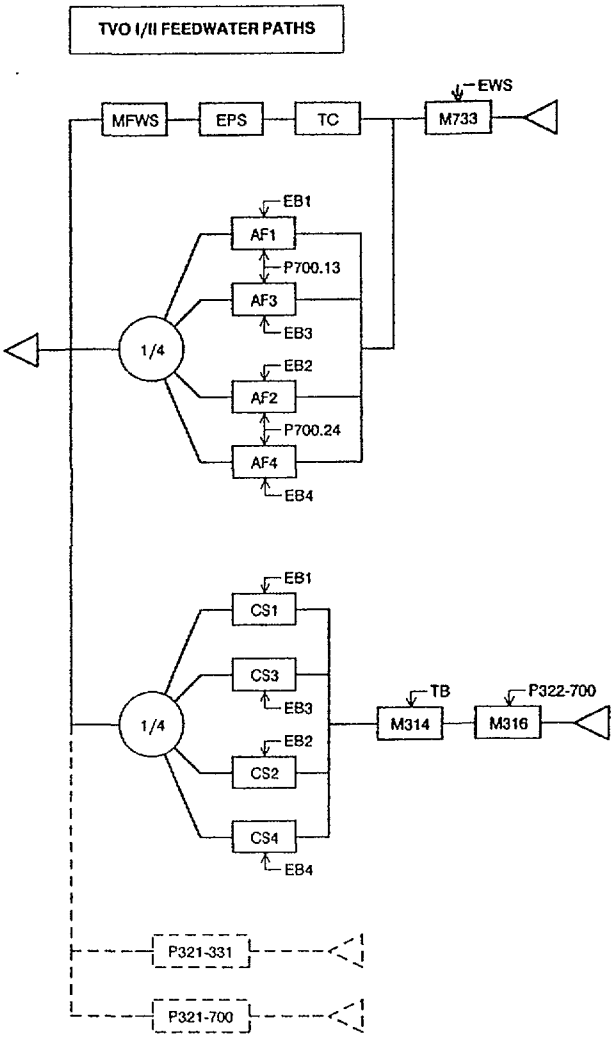


Figure 4.3b Reduced, modularised block diagram for feedwater systems. Module notations are defined in Table 4.1.

exist often special kind of system and component failure modes and their combinations, whose reduction to a block diagram presentation would be too cumbersome, but can be conveniently described by the fault tree logic [NKA/SAK-1]. In our study, several complex modelling issues were handled at the detailed level by Boolean expressions, which are equivalent to (graphical) fault tree models.

In order to facilitate computerised risk quantification by timedependent component and sequence models, it is necessary to reduce less significant details from the system models. The main reduction principle was modularization, for example by combining a pump train, constituted of a pump, associated valves and local instrumentation, into one functional block.

In the early stages of the study, rather detailed component block diagrams were first generated and quantified with timeindependent components models, using the task-oriented RELVEC program developed at VTT [RELVEC]. The simplifications done in the modularization were then successively verified by

the help of MCS list and importance measure information. In the later stages of the study, evolving detailed PRA study models could be used in a similar way as guidance and for verification.

It should be noticed, that in the modularization, detailed, component level information is lost, and also low-order contributors may be neglected. This sacrifice is, however, well motivated in order to be able to use more developed quantification methods concerning operational priorities, recovery possibilities and other timedependent phenomena. These aspects are essential in order to adequately quantify the SD state change related risks, as well as long term SC mission reliability. If desired, the system details could be selectively added, for example, in order to consider the influence of some components more explicitly.

Specially, the AC/DC supply as well as protection system dependences are still modelled in a crude way. This area has been an unresolved issue in the PRA studies as well, requiring further development work. In the TVO/PRA, lot of effort was put into the detailed analysis and modelling of AC/DC systems, which could then be benefited when tailoring the models for the AOT considerations.

4.6 Operator interactions

Operator actions are explicitly considered only to a limited extent. The capacity increase of the reactor water cleanup system 331 has been analysed in detail. Also restoration on tripped pumps or blocked valves in connection to isolation events have been selectively covered. In other cases it is mostly assumed that operators either succeed in planned operations or that the failures of operation are implicitly included in the frequency or probability data for the initiating events or other basic events.

4.7 Phased missions, event sequence modelling

The most essential methodological feature in the developed approach is the use of Event Sequence Diagram (ESD) for the detailed description of plant/systems response. The modelling elements are presented in Fig.4.4, and an example model in Fig.4.5. Also the SD transient diagram, Fig.4.1, follows this scheme.

The new, essential extension is the use of embedded state submodels [PM_SRE86, PO_PSA89] in the modelling of operational and transient scenarios, as compared to the earlier uses of ESD [Seabrook]. The rectangular block is here reserved for the activation events, whose failure exit is quantified by a conditional probability. The state block is used for intermediate and stable states, whose failure exits are quantified by conditional failure rates. The time lag between enter and exit events of a state block may be substantial and is generally stochastically distributed, whereas in an activation block this time difference can be assumed negligible.

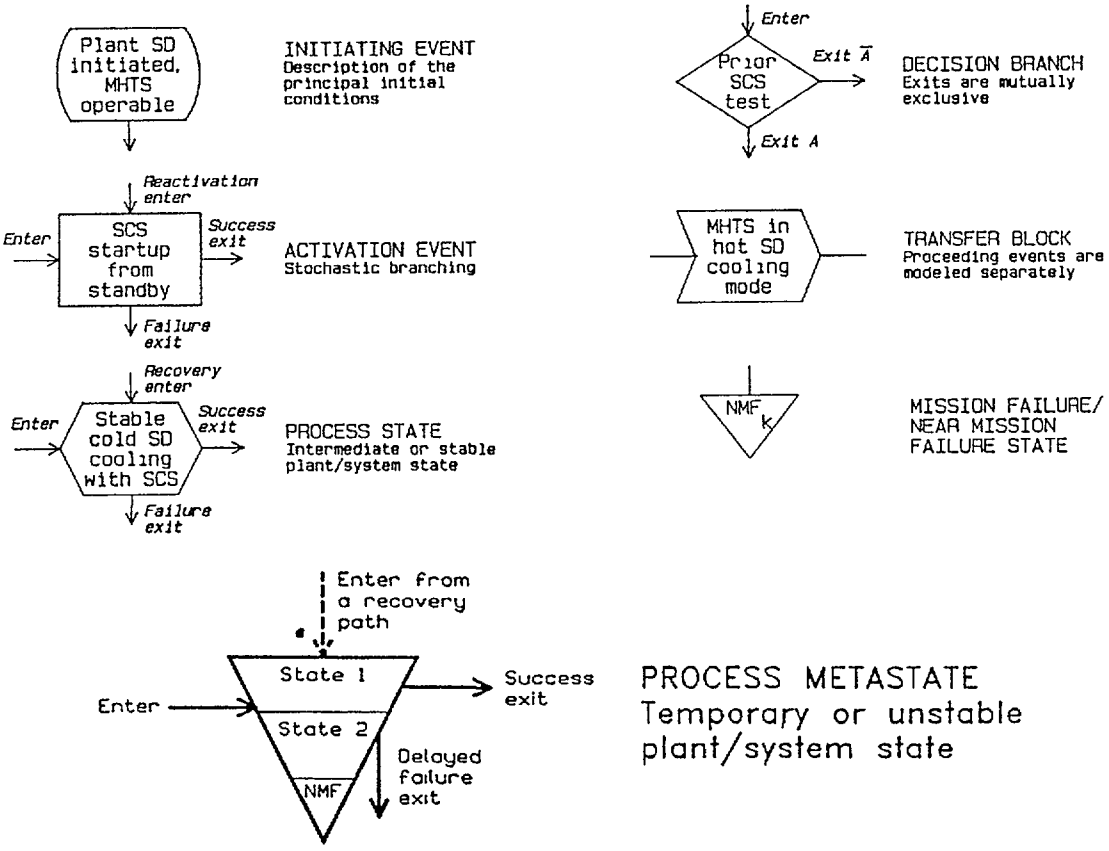


Figure 4.4 Symbols used in the extended Event Sequence Diagram (ESD).

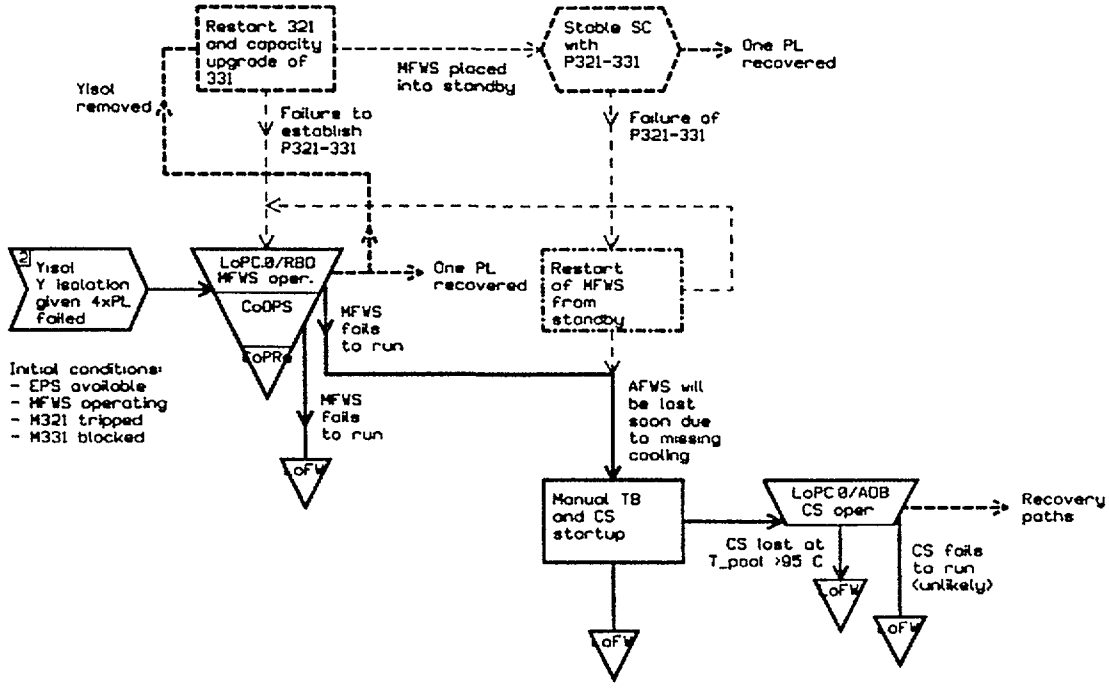


Figure 4.5 Example Event Sequence Diagram (ESD).

A critical plant condition is represented by a near mission failure (NMF) state. The NMF states are handled separately from the "normal" plant states due to differences in recovery modelling. The concept of NMF will be defined and discussed in more detail in Section 4.8.

A distinct metastate block is used for temporary or unstable process states, which develop into a NMF state without an active operator intervention (for example, due to pool heatup). Within a metastate, different substates can be distinguished.

The new approach allows process oriented modelling of phased missions and flexible modelling of the recovery paths from failure states. This also enhances the structured consideration of time dependences in process conditions, and specific scenario of events. As an example in Fig.4.5, the Y isolation initiating condition (with all 721/712 trains assumed failed) means a plant state where regulated blowdown of steam to pool will be used without heat transfer away (LoPC.0/RBD). Reactor water inventory is controlled by the initially operating MFWS. Without the recovery of RHR function, the pool heatup in metastate LoPC.0/RBD results in CoPRe condition, i.e. actuation of filtered steam release from the containment. Successful operation of MFWS is critical up to the recovery of RHR function. If MFWS fails prior to pool temperature 95 °C, manual depressurization and successful startup of core spray system still allows time for recovery measures, but only up to the pool temperature 95 °C, because CS pumps render then inoperable. On the other hand, if MFWS fails during CoOPS, i.e. pool temperature above 95 °C, the loss of feedwater condition is directly entered. It should be noticed, that AFWS can not be credited, because the assumed total failure of RHR trains 721/712 means, that AFWS pumps lack cooling, and would soon be lost if operated.

In connection with the inclusion of plant/system state modelling, the primary variable is transition frequency. This contrasts to the conventional event tree/fault tree quantification, which is based on simplified probability calculation of branching events and system demand failures.

The construction of ESDs was facilitated by PRA event trees. In more complex cases, the contributing failure combinations were verified by reliability block diagrams or fault trees for safety functions with listings of minimal cut sets (MCS). Available PRA models were found for this purpose useful and mostly sufficient.

It is important to emphasise that the ESD model layout is made according to the following rules (compare to Fig.4.5)

- paths of normal operation and success paths flow from left to right and are drawn in solid lines
- failure paths flow downwards and are also drawn in solid lines
- recovery paths flow upwards/leftwards, i.e. in the opposite direction as compared to failure (and success) paths, and are drawn for proper distinction in dashed lines

This layout implies that generally the plant states are ordered by mission time from left to right, and more critical states are placed downwards in the diagram. The NMF states are thus placed most downwards.

In the example model, Fig.4.5, only a part of the recovery paths are shown for simplicity. The primary recovery with removal of Y isolation illustrates, however, how efficiently things of this kind are coped with in the ESD approach.

4.8 Recovery paths, available time scenarios

Component repairs and other types of recoveries are systematically taken into account during the SC phases. This is necessary for an adequate comparison of operational alternatives of the AOT issue.

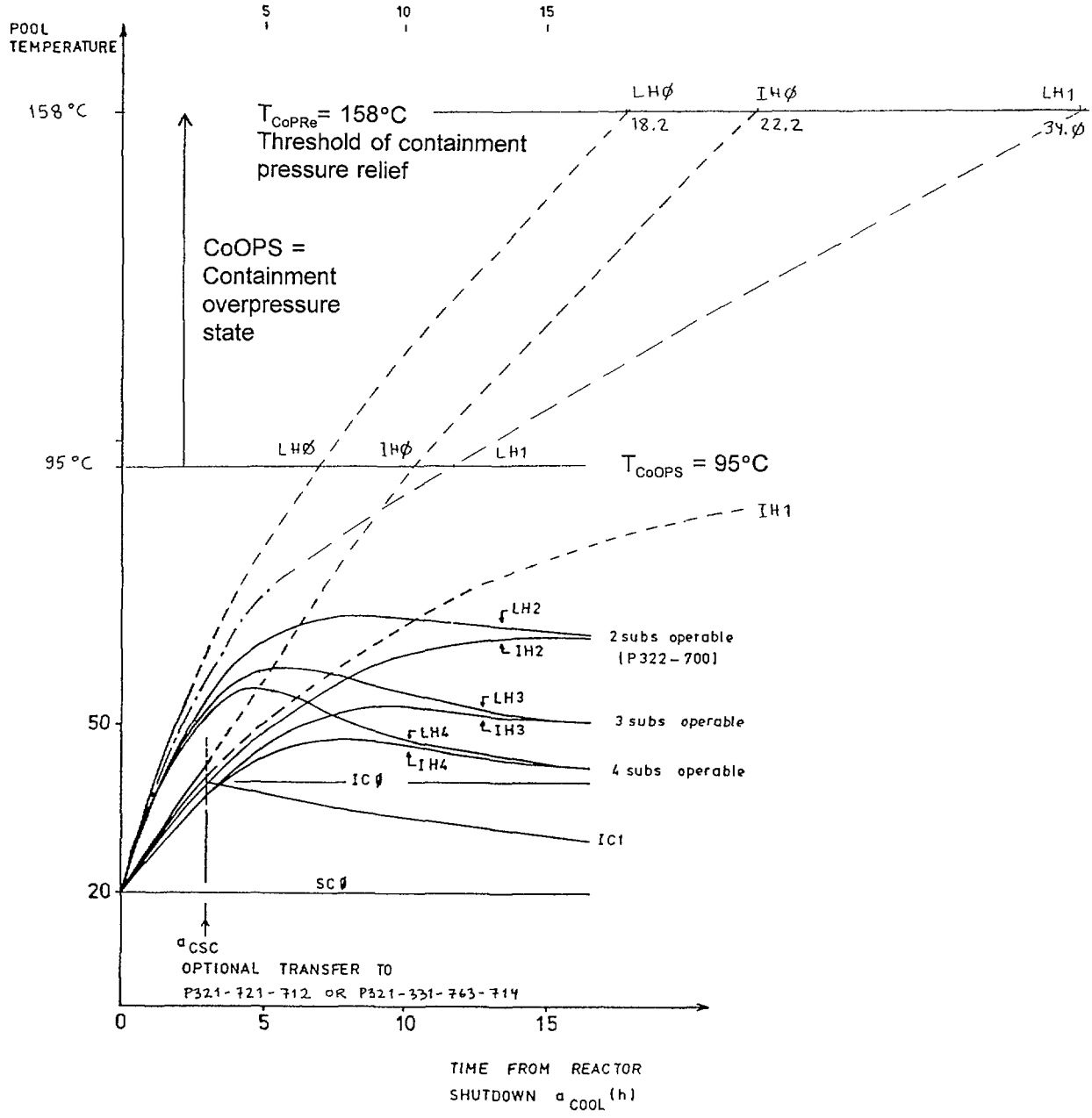
A new concept of Near Mission Failure (NMF) state was introduced for a near miss situation, where a critical safety function is lost, but there still remains time margin for recovery. In TVO/RHRS considerations, NMF states are associated to two kind of situations

- LoRHR: loss of RHR function in the narrow meaning, i.e. heat transfer away from the containment and suppression pool is lost, but reactor water inventory is retained (feedwater to the reactor and, if needed, also steam relief from the reactor are operating). Without recovery, LoRHR condition results in the containment pressurisation and need to undertake filtered venting.
- LoFW: loss of feed water function in the broad meaning, i.e. reactor water inventory control. Without recovery, reactor core will be uncovered with subsequent core damage.

Event sequences are grouped into disjoint scenarios according to the time margin for restoration, given by the pool heatup time or water level decrease in the reactor core, depending on which one is sooner critical in the various NMF states. In the case of a partial station blackout, the duration time of about 3 hours of battery supply to the instrumentation may become most critical, because a multiple loss of DC buses causes a variety of safety system interlocks.

Selected pool heatup scenarios are presented in Fig.4.6. Both the total loss of pool cooling and partial loss with only one train out of four operating are considered. In LOCA sequences, one train in the pool cooling path is not sufficient to prevent water heatup above the limit of 95 °C, which is considered critical for the operation of core spray system 323. In most scenarios the heatup speed is rather low giving substantial time margin for restorations.

The quantification of nonrecovery from the NMF states will be discussed in Section 5.5.



ASk	Coding	
| | |		
| | k	= Number of operable 322-721-712 trains	
| S	= Reactor shutdown state:	H = Hot SD
|		C = Cold SD
A	= SC initiation state:	S = Smooth
		B = InitBD
		I = Yisol, IisBD, LoEPS
		L = LePCi

Figure 4.6 Primary scenarios of containment pool heatup.

5 QUANTIFICATION

The following undesired end events are considered, representing the influence of multiple RHR train failures on the plant risk

CoPRe|LoRHR = Containment pressure relief due to prevailing loss of RHR function

CoreD|LoFW = Core damage due to prevailing loss of feedwater/core cooling

The CoPRe|LoRHR event is concerned with failure to transport heat to the ultimate heat sink - sea, by use of the three alternative RHR paths described in Section 4.2, but assuming that makeup water to reactor core is available in order to retain reactor water inventory and adequate core cooling by boiling. Release of steam and suppression in the pool are assumed to operate. A prevailing LoRHR situation results in pool heatup and containment pressurisation, compare with Fig.4.6. Restoration possibilities are taken into account up to the nominal threshold of the containment relief pressure, corresponding with pool temperature of 158 °C. This undesired end event means steam relief from containment to atmosphere via filtered venting system 362, compare to Figs.2.1 and 4.2.

The CoreD|LoFW event is concerned with loss of reactor makeup water as a result of losing feedwater paths described in Section 4.2. The consequence of the failures is water level decrease in reactor vessel. Restoration possibilities are taken into account until water level reaches the top of the core. This undesired end event means endangering core cooling with possible core damage.

The CoreD|LoFW end event corresponds to the usual core damage end event as specified in Level 1 PRA studies. In contrast, the CoPRe|LoRHR is less severe in regard to the safety consequences. Prevailing high temperature in containment may cause degradation, with need of lengthy inspections and repairs, and may hence result in substantial economic losses.

The CoreD|LoFW is the primary end event to be considered in risk comparisons. CoPRe|LoRHR was considered parallel for completeness. There is also the historical background to this. Prior to installing containment filtered venting system, the containment overpressurisation state was outside the design conditions, and therefore it was conservatively included in "general" core damage risk in the early stages of the study, although that is not quite correct. In the final stage of the analysis, a proper distinction of these end events was made.

It should still be emphasised that CoreD|LoFW end event is not a monolithic simple thing, but instead the actual consequences may have a wide spectrum depending of the specific event sequence occurring, and containment response. This same problem concerns Level 1 PRA generally. In our case the potential implications for the results and conclusions have been considered by engineering judgement.

5.1 Specification of risk variables

The basic concepts are shortly defined here following the scheme presented in Ref.[NKA/RAS-450].

5.1.1 Risk frequency

The risk frequency is the basic concept. It is associated with the probability of 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 undesired end event (UndEnd) is associated with the containment pressure relief (CoPRe) or core damage (CoreD), as explained in the beginning of this chapter

$$f_{UndEnd} = \text{Probability of undesired end event per unit of time} \qquad (5.1)$$

The risk frequency is usually given in units [1/year]. In the actual calculations in this study, units [1/hour] are used in analogy to component failure rates. However, in the plant level result presentations using units [1/year] is convenient as it allows comparison with the PRA output for the average annual risk level.

It need to be emphasised at this point that in the context of conventional PRA studies, the averaged risk over various component and system states is derived (and usually presented as annual risk). In the context of an LCO analysis, the actual dependence on time, component and system states, and operational scenarios are of interest. I.e. we are here concerned with the "instantaneous" risk frequency. This concept and its meaning were schematically illustrated in Fig.3.2, while Fig.5.1 shows how f_{LoRHR} behaves in the double failure state of RHR trains 712 [ESumRepo88].

5.1.2 Baseline risk

The baseline risk (compare to Fig.3.2) will be used in the continuation to refer to the risk level in case the safety systems are in their nominal state. For most safety systems this means standby state without any components known to be inoperable. The latent failures of these components are only detected by surveillance tests or at demand situations. Their likelihood is the prime ingredient of the baseline risk. For some safety systems or components, the nominal state may also be the operating state. Consequently failures of those components are usually directly revealed by instrumentation or process symptoms. If an initiating event occurs during the baseline state, the instantaneous unavailability is initially zero for these components, but they may fail during the mission period, and contribute in that way also to the baseline risk.

Disconnections for testing or maintenance, and detection of critical faults in surveillance testing of standby components or failure to run of operating components, etc., are deviations from the baseline state.

When considering AOT situations for a safety system, it is important carefully to exclude from the baseline state all unavailability states of safety system components which would interfere with the LCO rules for the considered systems. Such interfering combination cases should be considered explicitly as distinct AOT situations, not included "implicitly" as in PRA studies is normally done for repair and maintenance downtimes.

The long term risk is composed of the integrated baseline risk plus the expected value of the increments due to all kinds of deviations from the baseline.

5.1.3 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 is derived as:

$$C_{ALT}(a|X) = \int_{t=t_0}^{t_0+a} dt.f_{UndEnd|ALT}(t \mid X(t_0)) \qquad (5.2)$$

where ALT stands for the operational alternative, and X for the failure situation considered, detected at t_0. (This is illustrated in Figs.6.1 and 6.4 for the TVO/RHRS case.)

5.1.4 Expected risk per failure event

Next, the expected risk over the failure situation X, for an operational alternative ALT, is the integral of the risk frequency (here f_{UndEnd})

$$R_{ALT}(X) = \int_{t=t_0}^{\infty} dt.F\hat{}_X(t-t_0).f_{UndEnd|ALT}(t \mid X(t_0)) \qquad (5.3)$$

where $F\hat{}_X(a)$ is the complement $1-F_X(a)$ of the repair time distribution $F_X(a)$ for the failure state X. As compared with 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, i.e. it is the mean risk per repair.

For the TVO/RHRS case, the expected risks per failure event are illustrated in Figs.6.2 and 6.5. They are calculated, from the risk frequencies, Figs.6.1 and 6.4, 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 interpret and become less sensitive to a part of input data.

Also the expected number of system failure situations NF (compare to Figs.6.2 and 6.5) is more meaningful to be presented in the perspective of the whole lifetime, as the likelihood of multiple failures is so small per test cycle, and

even per year. It should be noted that the cumulative and expected risks can also be given an interpretation as the expected number of undesired end events per operational alternative/scenario [TM_Thesis].

5.1.5 Addition in lifetime risk

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

$$dR_{ALT}(X) = NF_X.R_{ALT}(X). \quad (5.4.a)$$

For the TVO/RHRS case these are presented in Figs.6.3 and 6.6, again normalised by the lifetime baseline risk. Alternatively, the addition to the average risk frequency *fav* could be presented as

$$dfav_{ALT}(X) = dR_{ALT}(X)/LT = \lambda_X.R_{ALT}(X). \quad (5.4.b)$$

where

LT = Plant lifetime

λ_X. = Frequency of failure situations X

5.2 Event sequence quantification

5.2.1 Calculating total expected risk

The highest level of modelling/quantification is based of SD transient diagram, as explained in Section 4.1. This interfaces to the detailed sequence models via transfer frequencies/ probabilities of SC initiating events, which are quantified by mission failure risk (probability)

$$R(in) = P\{\text{Mission failure} \mid \text{SC initiation via in}\} \quad (5.5)$$

In overall quantification, the risk frequency of CO alternative is obtained from these by

$$f_{CO} = \sum_{in=0}^{in\_max} f_{ISC}(in)*R(in) \quad (5.6)$$

The expected risk of CO alternative is derived through multiplication by mean repair time

$$R_{CO} = f_{CO}*a_{mean} \quad (5.7)$$

Analogously, the total risk of SD alternative in obtained as

$$RSD = \sum_{in=0}^{in\_max} PISC \mid DecSD(in)*R(in) \quad (5.8)$$

The total mission failure probability for a SC initiating event *in* is schematically obtained from two parts (in many cases the initiating event interacts with repair states of failures at the start or during the mission period, and these repair dependencies are considered in actual cut sequence quantification algorithm):

$$R(in) = pch\_t(in) + \int_{a=0}^{oo} da*fsc\_t(in,a)*pnr(in,a) \qquad (5.9)$$

where

pch_t(in) = Probability of mission failure at SC start
fsc_t(in,a) = Frequency of mission failure during SC period
pnr(in,a) = Probability of nonrecovery from initiating event during SC period up to time a

5.2.2 Visualisation of instantaneous risk frequency

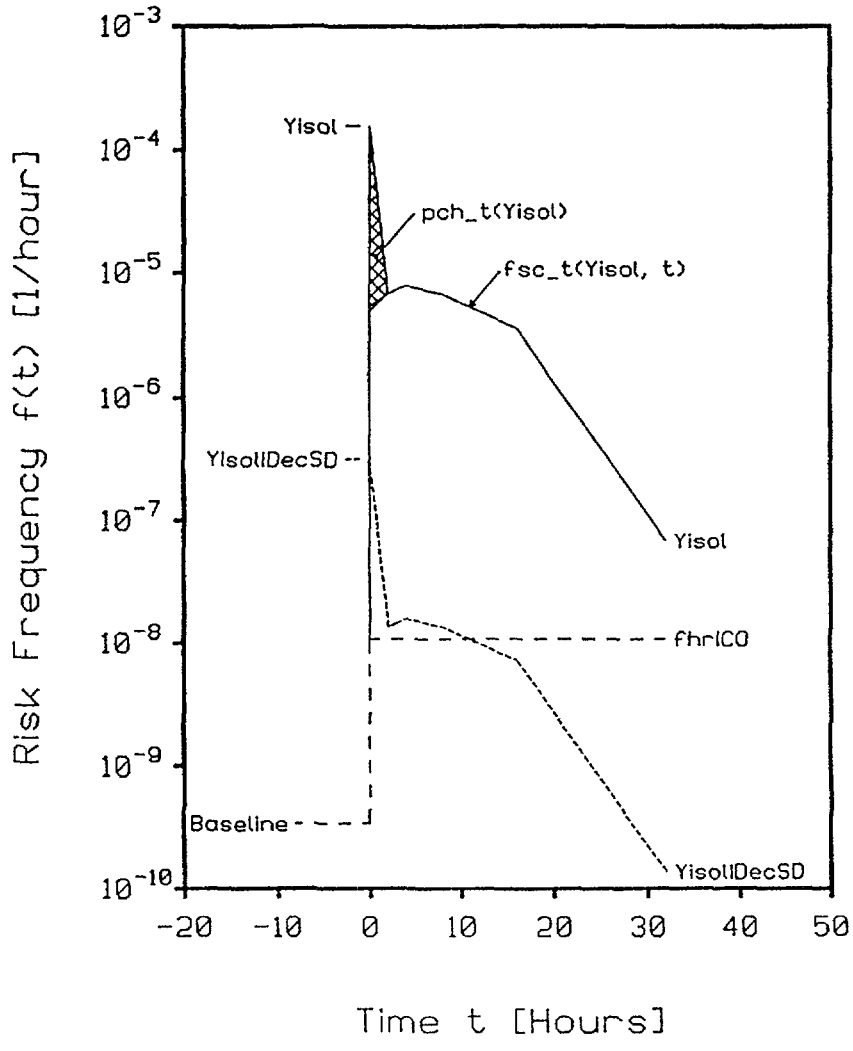
For a given *in*, the associated cut sequences are quantified in the first stage and then summed up to produce the basic entities and *fsc_t(in,a)*, compare with Eq.(5.9). It should be emphasised that the first one of these is a sole probability entity, while the second is a frequency entity and a function of time *a* elapsed from the initiating event occurrence (start of SC mission). For drawing the instantaneous risk frequency, for illustrating purposes, such as shown in Figs.5.1.a-b, the probability entity *pch_t(in)* can mathematically be considered as a Dirac delta function, and drawn as a peak. For practical purposes it is motivated to draw this delta peak with a nonzero width, comparable with the duration of the reactor power reduction/cooldown, or startup phase of standby safety systems, depending on which one of these is contributing most to the total probability of mission failure at SC start. In fact, the delta peak can be considered as a superposition of narrower peaks related to different contributors, at specific time points during the initial reactor shutdown phase, before a more stable SC mission period is reached.

In this study, a triangle shape with a base width of *ach = 2 hours* for the delta peak is consistently applied for all SC initiating events, Fig.5.1.a. Consequently, the height of the delta peak is derived as equality for integration area:

$$fch = \frac{pch}{½.ach} = \frac{pch}{1\ hour} \qquad (5.10)$$

and the triangle shape contribution is then overlaid above the *fch_t(in, a)* contribution. The probability mass *pch* is thus effectively divided over one hour, which is convenient for the numerical relationship. It should be noted, that in some SC initiating events, the actual spread may be larger, and in some cases shorter.

It need to be still emphasised, that the delta peaks corresponding with *pch* entity are drawn just for illustration purposes, being visually a well motivated way of representing the risk vulnerability of the initial reactor shutdown phase. However, the actual risk variables for comparison, as discussed in the preceeding section, are directly derived from the basic



Legend

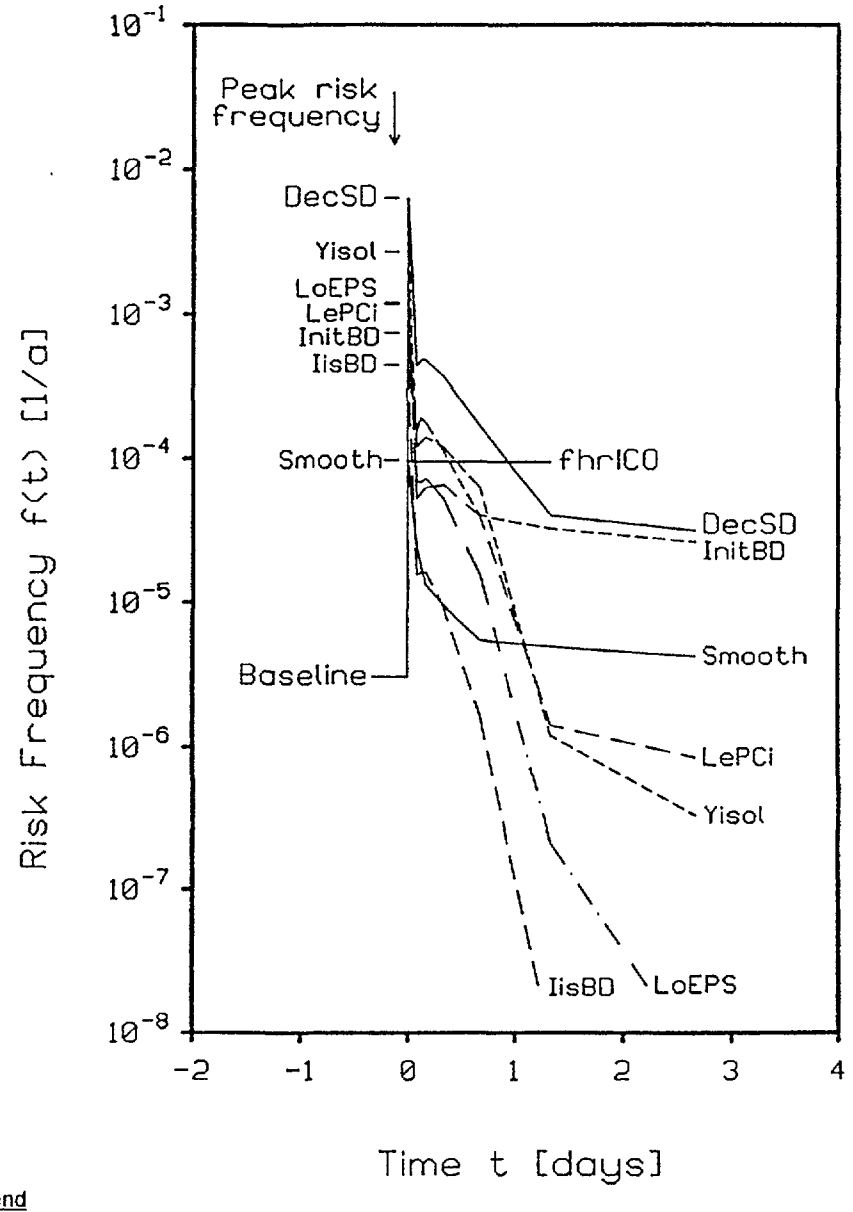
Yisol = Y isolation, results in isolation of the normal shutdown cooling path, the instantaneous risk frequency is calculated assuming Yisol occurred at time point zero

YisolIDecSD = Y isolation scenario normalised as conditional for a decided shutdown of the plant; Yisol occurs with a specific likelihood during reactor shutdown/cooldown process (in the beginning of the SC mission)

fhrICO = Risk frequency in continued power operation state for the assumed initial failure situation

Baseline = Risk frequency while in baseline power operation state

Figure 5.1.a Constructing the visual presentation of instantaneous risk frequency. (RHR function level considerations, two out of four RHR trains 712 (PM) detected failed during power operation. Based on early stage results [ESumRepo88].)



Legend

Smooth =	Smoothly proceeding decided shutdown of the plant
InitBD =	Shutdown disturbance trip, initiates blowdown to condensation pool
IisBD =	I isolation with blowdown to condensation pool, excluding actual LOCAs
Yisol =	Y isolation, results in isolation of the normal shutdown cooling path
LePCi =	Leakage of primary coolant inside containment, i.e. actual LOCAs
LoEPS =	Loss of external power supply
DecSD =	Decided shutdown of the plant, sum over all initiating event scenarios listed above (normalized as conditional for a decided shutdown)
fhr|CO =	Risk frequency in continued power operation state

Figure 5.1.b Example risk frequency diagram. (RHR function level considerations, two out of four RHR trains 712 (PM) detected failed during power operation. Based on early stage results [ESumRepo88].)

entities *{pch_t(in),fch_t(in, a)}*, being thus independent of the details how the graphical risk frequency presentation is being made. (With the above scheme, the same results would nevertheless be obtained if the expectation values were integrated from the "total visual" instantaneous risk frequency curves.)

5.2.3 Detailed shape of risk frequency curves

The risk frequency diagrams, Figs.5.1.a-b, also include other fundamental features. Firstly, the instantaneous risk frequency of Y isolation scenario is shown in Fig.5.1.a, when being in a double failure situation of RHR trains 712. (Effectively, $P_{Yisol} = 1$ at zero time point, while no other initiating event being present.)

In the beginning of the SC mission, shortly after the initial risk peak, the risk frequency increases a bit because of increasing projected unavailability of MFWS and EPS, being in operating state and available (which means zero unavailability) in the beginning. Also the initial blowdown to pool decreases heatup margin in the period of about 3-6 hours. However, thereafter the two still intact RHR trains are likely to succeed in pool cooling, restoring larger heatup margin. Besides, the diminishing decay heat level begins to effectively increase heatup margin, allowing more time to make recoveries if a critical failure combination occurs later during the SC mission period. This is the main reason for the strong decrease of the risk frequency in long term.

In Fig.5.1.a, the dashed curve Yisol|DecSD shows the conditional risk frequency of Yisol, per decided shutdown in a double failure situation of RHR trains 712. This is derived from the Yisol risk frequency by multiplying by the probability $P_{Yisol|DecSD} = 2E\text{-}3$, compare with the corresponding branch in the SD transient diagram, Fig.4.1.

In Fig.5.1.b, the contributions to the total risk frequency of DecSD is shown, one being the contribution Yisol|DecSD shown firstly in Fig.5.1.a. It should be noticed that the scales in the diagrams are different. Specially, the vertical scale in Fig.5.1.a is [1/hour] in order to enhance numerical comparability of basic timedependent entities, while in Fig.5.1.b it is [1/year] in order to enhance comparability with the annual average risk level - as discussed in the preceeding section.

Looking more closely, also the risk frequency of CO alternative f_{CO}, in Eq.(5.6) is a timedependent entity, because in fine details, the initiating event frequencies $f_{ISC}(in)$, are actually fluctuating by time, and on the other hand, also the total mission failure probability $R(in)$ possesses second order timedependence specially due to the dependence on actual test time points of standby equipment. These kind of fine details on timedependent factors are neglected in this study, because of their minor role for AOT risk comparisons. The dependence of actual test time points for some most contributing components was included in the early stages of the study, but then averaged, because their small influence was understood [ESumRepo88].

5.3 Risk profiles and importance measures

The risk entities defined above are presented in the form of risk profiles in Figs.5.2.a-d, arranged in such a way, that Figs.5.2.a/c represent risks of CO alternative and Figs.5.2.b/d of SD alternative in regard to CoPRe and CoreD end events respectively.

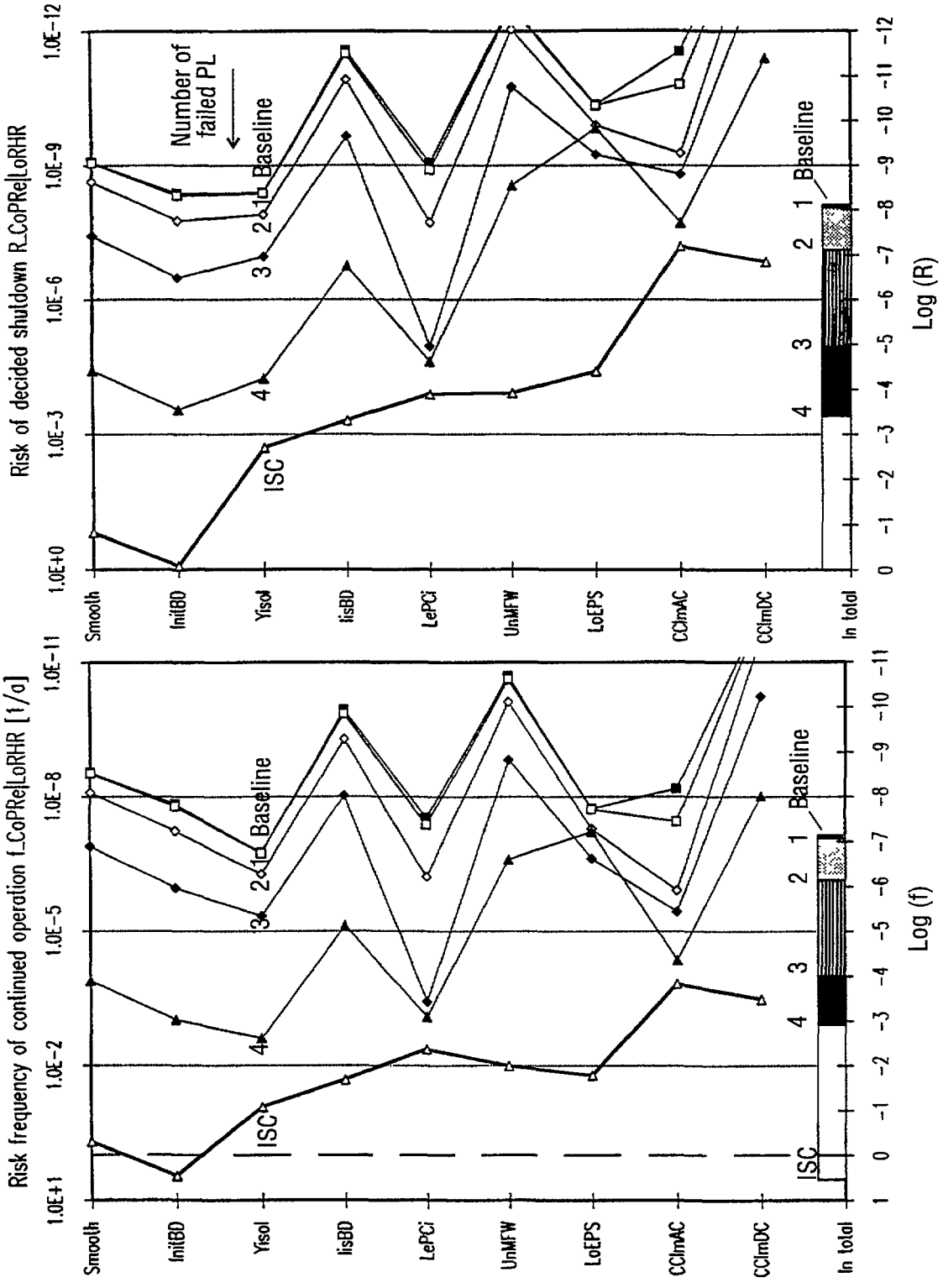


Fig.5.2.a-b. Copre|LoRHR risk profiles for CO/SD alternatives.

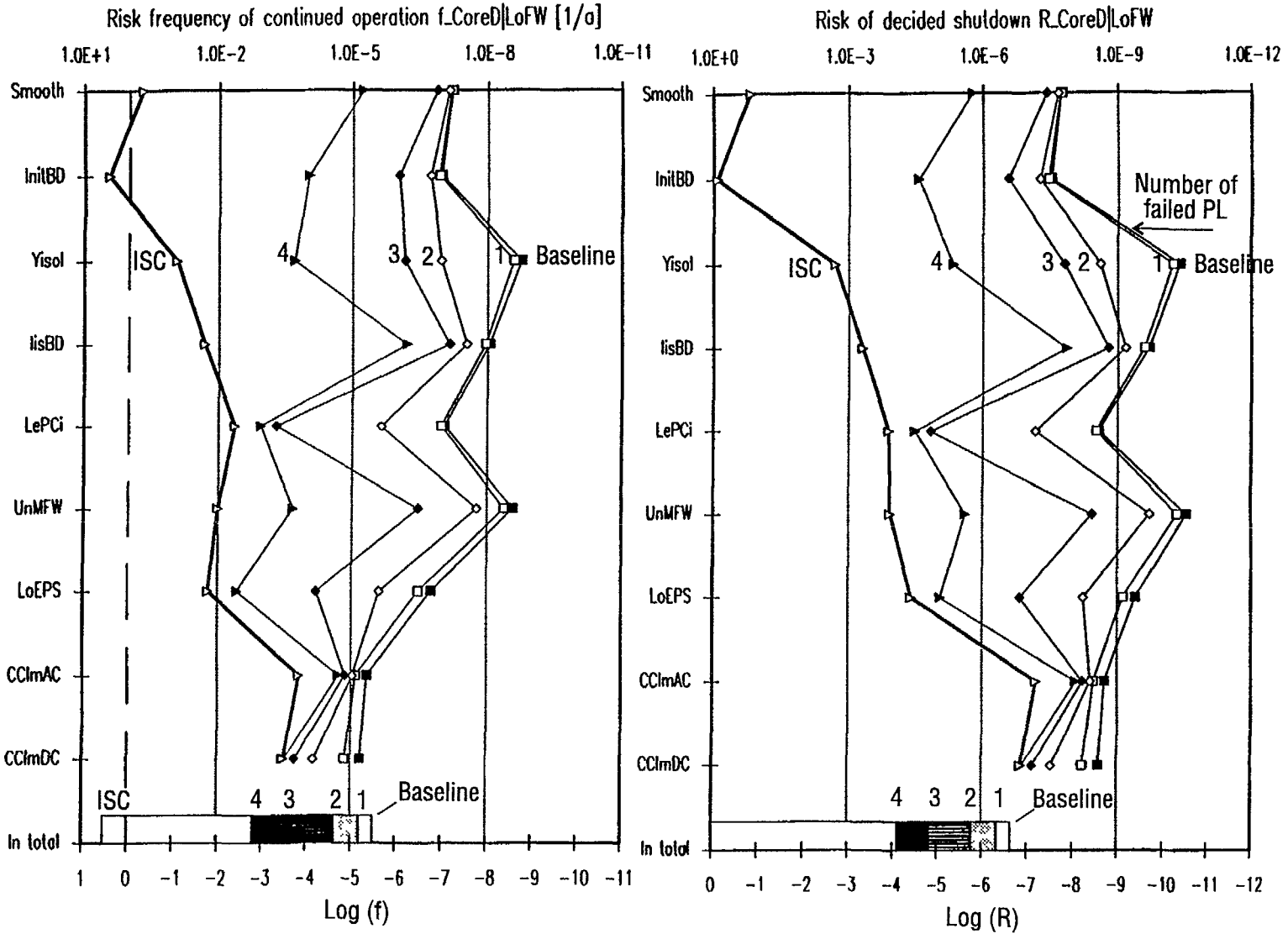


Fig.5.2.c-d. CoreD|LoFW risk profiles for CO/SD alternatives.

In the risk profile of CO alternative, Figs.5.2.a and 5.2.c, the first curve represents the frequencies $f_{ISC}(in)$ of SC initiating events *in*, and the other curves the corresponding risk frequency contribution, given initial state of different failure multiplicities of RHR trains 712/721. Failure multiplicity 0 corresponds with the baseline state. The margin between $f_{ISC}(in)$ and the corresponding risk frequency contribution equals $R(in)$, compare with Eq.(5.6). This margin is naturally dependent of the initial failure state, decreasing monotonically as the function of failure multiplicity.

Risk profiles tell a lot of plant design features. In CO alternative with respect to CoPRe risk, it can be concluded, that the dominant contributors are Y isolation events and primary coolant leakage LePCi, Fig.5.2.a. In multiple failure situations of RHR trains, the plant becomes the susceptible also for mere plant trips (InitBD), because then the RHR function is dependent on the successful capacity increase of the cleaning water system 331.

The CoPRe risk profile of SD alternative, Fig.5.2.b, is in many respect similar to CO alternative, but the contribution of plant trip type SC initiating events (InitBD) is pronounced, as this is the most likely transfer event to SC period in SD alternative (about 85%). Correspondingly, the contribution of the more severe transients remains small.

Analogous profiles for CoreD|LoFW risk are presented in Figs.5.2.c-d. The baseline risk is strongly dominated by CCI events of AC/DC buses, but in triple/quadruple failure states of RHR trains, primary coolant leakage LePCi and loss of external power sources LoEPS become most important. In SD alternative, plant trip type SC initiating events (InitBD) are also among dominant contributors.

Risk importance measures, as calculated with respect to baseline risk for system modules and other primary basic events are presented in Figs.5.3.a-b. The importance measure definitions and presentations follow the scheme of Ref.[Imp_TeRe]. The risk increase factors are in this study calculated by tailored models for the cases of given system functions known unavailable, in order to properly take into account operational implications. The risk increase factors are produced only for selected systems, because corresponding laborious tailoring of the failure situation specific models for other systems was not undertaken within the study.

The importance measures are presented for both alternatives CO/SD in Figs.5.3.a-b. These show differences, which are related to specific details of plant design. First of all, it can be concluded, that the risk increase factors for RHR trains 712/721, i.e. modules PM/PU are specially high, proving that the consideration of their AOTs is essential. It is also interesting to notice, that the importances of electric power supply modules EPS, DG, DGX are small for CoPRe|LoRHR risk but significant for CoreD|LoFW risk.

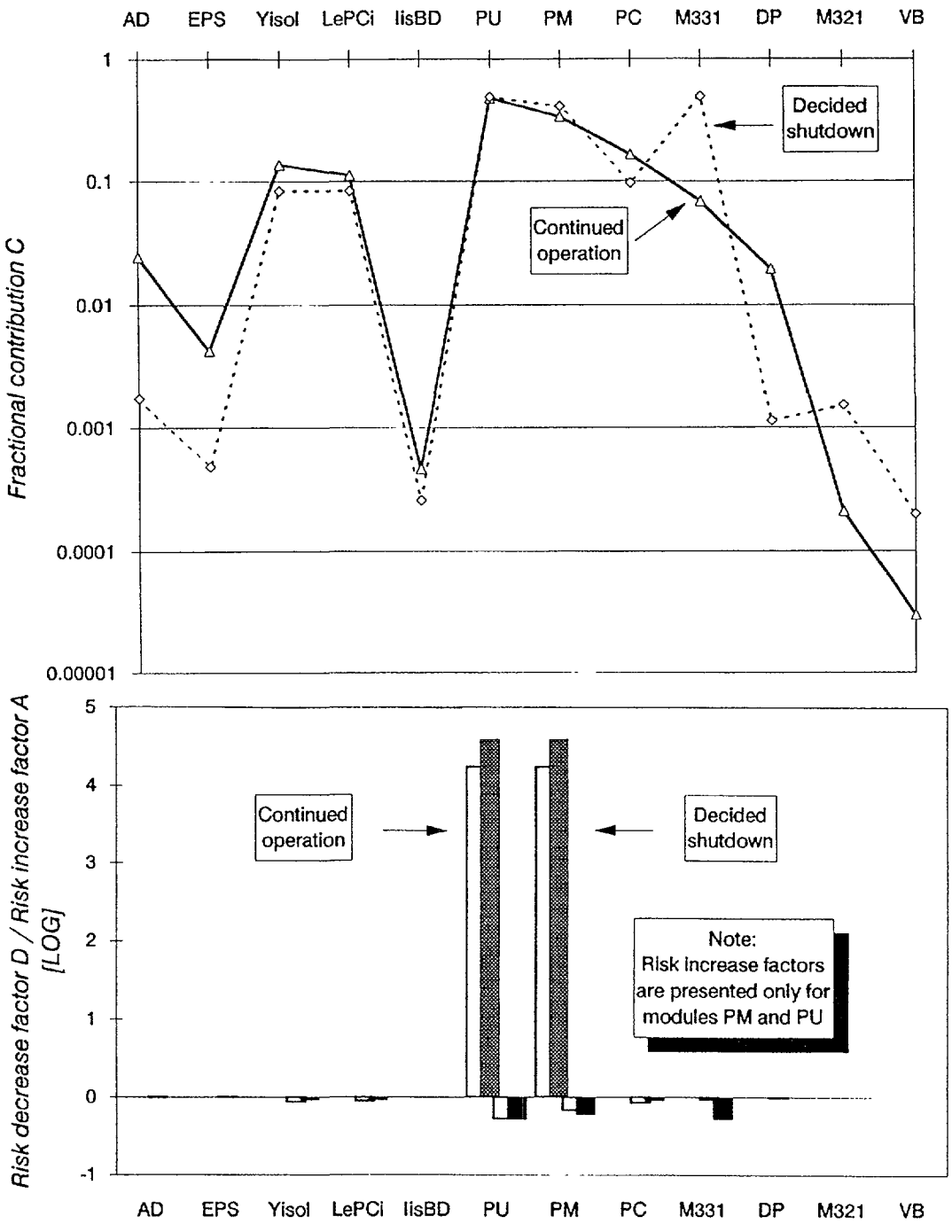


Figure 5.3.a. Risk importance measures in regard to baseline CoPRe|LoRHR risk level. Module definitions are presented in Table 4.1.

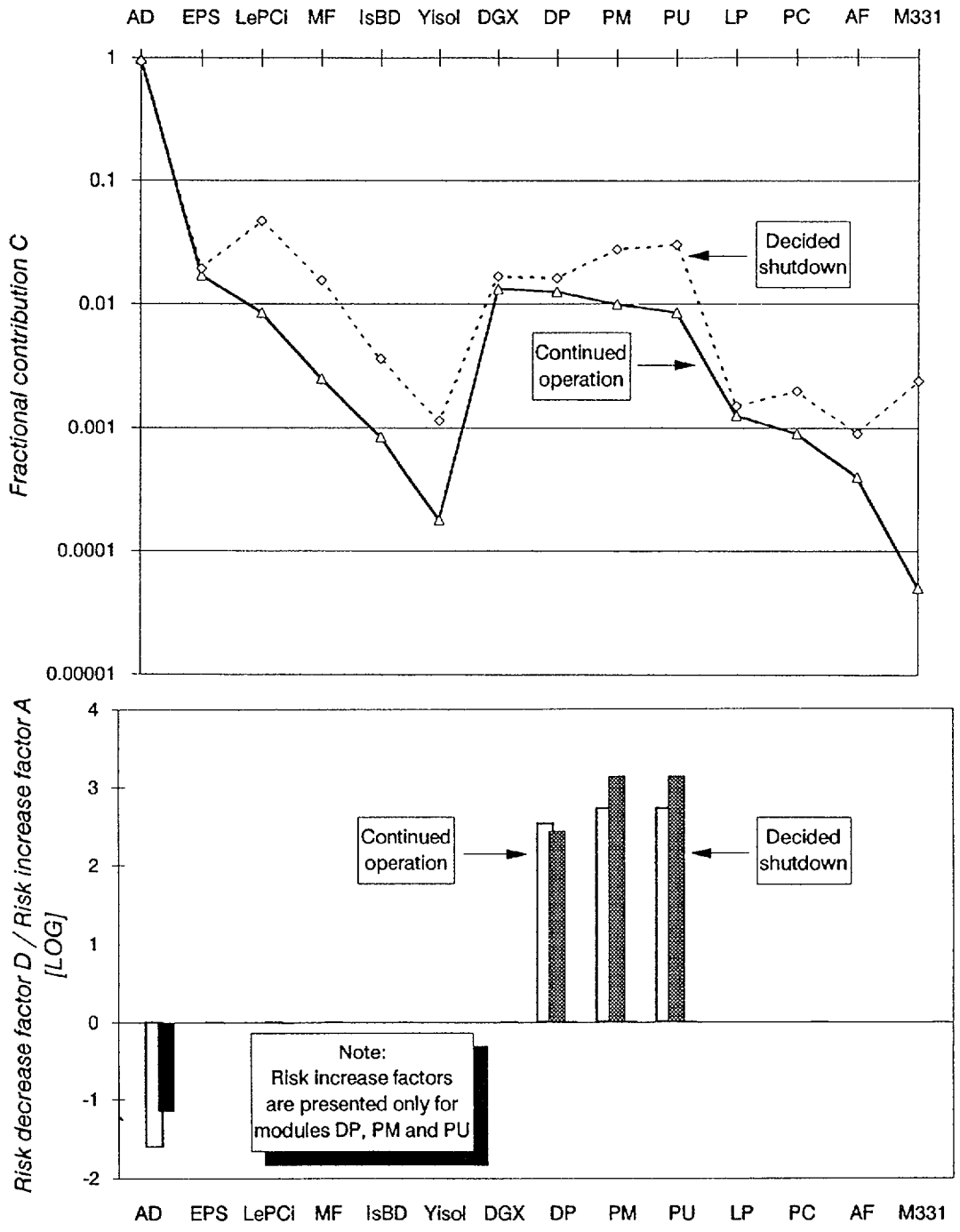


Figure 5.3.b. Risk importance measures in regard to baseline CoreD|LoFW risk level. Module definitions are presented in Table 4.1.

5.4 Repair/recovery time distributions

The repair and other recovery time distributions are modelled by multipart exponential distributions:

$$pnr(a) = \sum_k pnr^{(k)}(a) \qquad (5.11)$$

$$pnr^{(k)}(a) = z^{(k)} \cdot e^{-\frac{a - d^{(k)}}{a^{(k)}}}$$

$$= 1, \text{ if } a < d^{(k)}$$

where the sum of the fractions $z^{(k)}$ is 1. The (active) repair time constants $a^{(k)}$ and repair delay time $d^{(k)}$ are positive constants. This model gives a reasonably good fit to actual empirical distributions, and is very convenient due to mathematical simplicity: consideration of recovery paths is reduced to the application of well established methods of Markow process analysis [PO_PSA89].

The distribution parts can be interpreted as failure types of different repair classes of increasing severity and required repair time, such as electrical/mechanical/catastrophic failures. An example of repair time distribution with this background is presented for 721 train modules PM in Table 5.2.

It should be noticed, that usually the same distribution is applied to both modes of failure to start and failure to run, when there is not evidence showing a difference between these in regard to repair time distributions. Operating experiences also showed, that at the TVO plant, the repair delay times were not pronounced. They effectively were covered by the exponential distribution parts with zero $d^{(k)}$ parameters. This contrasts to a more usual situation, where remarkable repair delay times are evident, and need to be explicitly taken into account.

5.5 Recovery from NMF states

As pointed out in Section 4.8, the NMF states are in central role for considering event specific recovery possibilities.

5.5.1 Recovery time distributions

For the recovery from NMF states, module repair time distributions are mostly used as such. This may be pessimistic, because in a critical situation, repair actions can be undertaken more promptly as compared to normal, routine repair arrangements (background to the statistical distributions used). On the other hand, in a complex emergency situation, there may interfere many delaying factors. Thus, as the first approximation, the normal repair time distribution for component failures was used also for recovery model of NMF states.

Operator actions for recovery were considered case by case, in order to take into account situation specific factors consistently. For this purpose standard time curves for operation action were applied [UCLA_83]. Quantitative estimates are partly based on PRA study analyses, partly on additional engineering judgements.

5.5.2 Heatup time margins

Time available for restoration from a NMF state is obtained by the use of heatup scenarios, as illustrated in Fig.5.4 for the case of pool heatup scenario LH2, compare to Fig.4.6. The cases of total safety function failures and partial failures, where one pool cooling train with a capacity less than 100% only remains operable, are handled separately, by strictly defining them as mutually disjoint cases.

In LH2 scenario, the primary coolant leakage LePCi initiates SC, which means, that the normal SC cooling system 321 is automatically blocked. In LH2, two trains in the pool cooling path 322-721-712 are assumed successfully started and operating (also reactor water inventory is assumed to be maintained by successful operation of the emergency core cooling systems). The potential failures of the two, initially intact pool cooling trains are considered at discrete time points defined for use as quantification steps.

Fig.5.4 shows pool temperature behaviour, when one or both trains, initially operating in the pool cooling path 322-721-712 in LH2 scenario, failed at time point 2 hours from reactor shutdown.

In the total failure case (such as CCF occurrence), CoOPS threshold of 95 °C is reached at time point 7.6 hours. This gives an available restoration time of 5.6 hours. Entering CoOPS may be critical in such event sequences, where the core cooling relies on containment spray system 323, whose pumps become inoperable at the CoOPS threshold. In other sequences CoPRe threshold at 158 °C may be critical. Up to that point there is 17 hours time available to recovery (from the failure of the remaining 322-721-712 trains at two hours time point). In LOCA cases the abrupt pressure drop in containment, when relief is initiated will cause boiling in reactor water level measurement tubes, which is assumed to cause instability of level control and result in the loss of feedwater function.

In the partial failure cases, where one 322-721-712 train remains operating, temperature increase is rather slow. The maximum pool temperature remains in these situations below 100 °C.

5.5.3 Quantification of recovery paths

The quantification of cut sequences is based on discretising the time axis. At each time step, the possible recovery paths are considered for a given initial failure situation and initiating event, and eventual later events of the specific sequence. In case of multiple recovery options, a model of

"shortest repair first" is applied, in order to derive the net distribution. This approach will be discussed in Section 5.6. From the net distribution, the probability of nonsuccessful recovery is then obtained using the situation and time specific margin available for recovery.

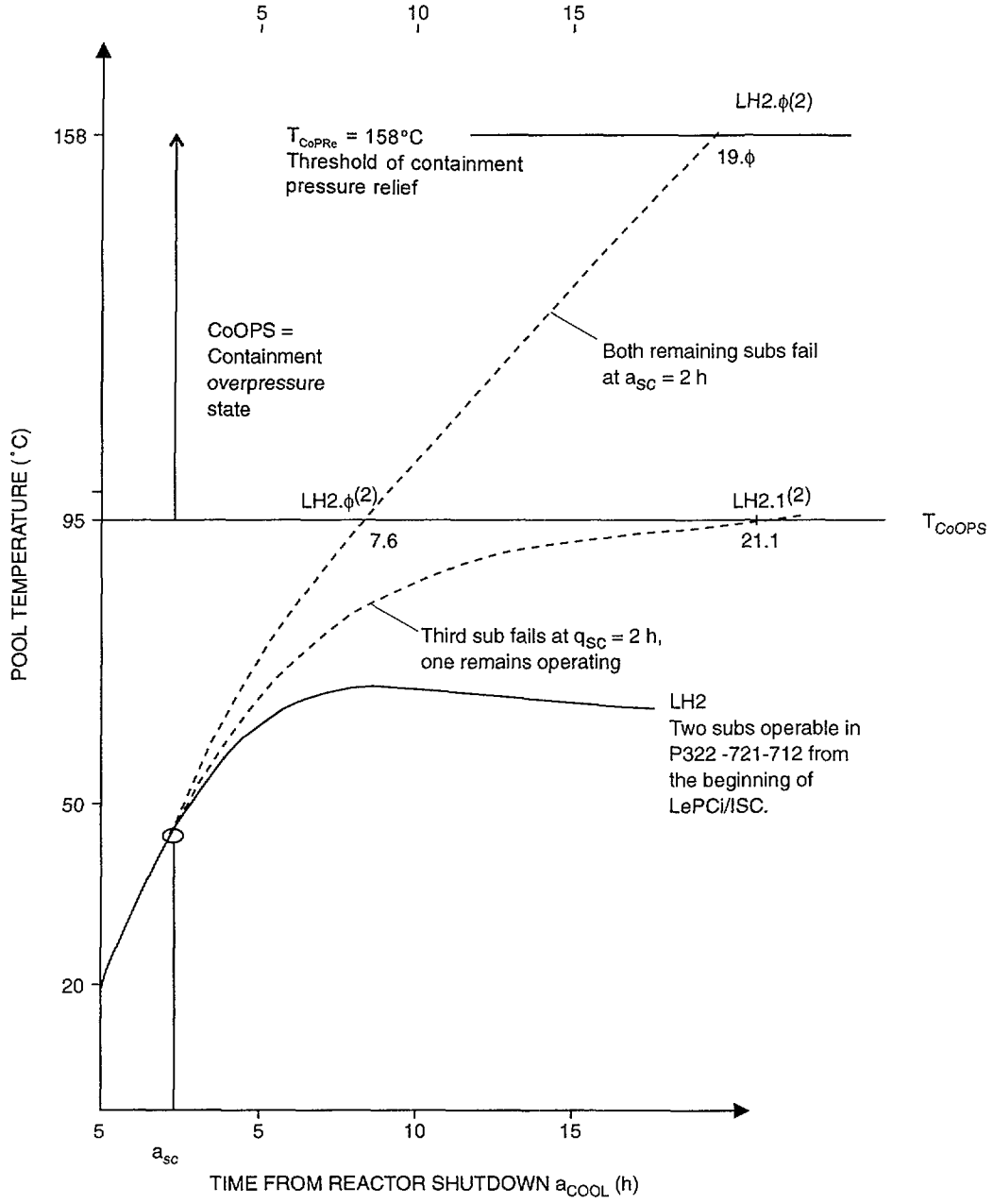


Figure 5.4 Example of available time to restoration as allowed by condensation pool heatup time: In the initiating event scenario of LePCi, with two pool cooling trains started, one or both operating trains fail at the time point of 2 hours.

5.6 Treatment of multiple repairs

In a multiple failure, the components are often assumed to be repaired independently of each other. This means that equal repair resources are assumed to be available for each failed component without regard to the number of simultaneously existing repair states. This assumption may be too optimistic due to limitations on suitable personnel and other practical boundaries. Furthermore, in complex emergency conditions, applicable to recovery from NMF states, it may be difficult to focus interest on several objectives parallel.

It is more reasonable to adopt such a model, that in multiple failure situations, the repair priority is given to the component whose expected recovery time is assessed shortest. When using repair time distributions, which are multipart exponential, this can be interpreted in the following way:

- repair class of a fault can be identified quite soon after detection
- highest repair priority is put on the component with shortest expected repair time, i.e. smallest repair class constant.

Yet, the repair time of the highest priority is exponentially distributed, which adequately reflects the uncertainties. This approach, "Shortest Repair Class First" model (SRCF), results in a distribution, which is still multipart exponential [PO_PSA89], with all consequential benefits. This model was systematically applied in the quantification of multiple failure recoveries.

5.7 Component unavailability model

The simple $q + \lambda t$ model is implemented as timedependent unavailability model of standby components [TI_Opt88]. For diesel generators, the model was supplemented by a contribution q_hid of latent failures not detectable in normal surveillance tests but only in annual overhaul test or actual demand.

For system modules, $q + \lambda t$ model is applied using the straightforward superposition principle for combining q and λ parameters, as well as repair time distributions.

5.8 Common Cause Failure model

Shared cause model of dependencies [SHACAM] - a variant of MGL/Alpha factor method - is used as the parametric CCF model for "hidden dependencies" of identical redundant components. This parametrisation fulfils the desired property of subgroup invariance, which among other benefits greatly enhances the treatment of conditional probabilities in multiple failure situations.

For latent failure modes, the shared cause basic events are described again by use of $q + \lambda t$ model. For example, for k redundant components out of n, the CCF part of instantaneous unavailability is expressed by

$$ce_{k|n}(t) = dq_{k|n}.q + ds_{k|n}.fs.(t - t_{LastTestSk}), \qquad (5.12)$$

where

$dq_{k|n}$ = Dependence coefficient of the timeindependent part (q)
$ds_{k|n}$ = Dependence coefficient with regard to latent standby failure rate fs and timedependent part (fs.t = λ.t)

and $t_{LastTestSk}$ is the test time point of the component tested last in the subgroup Sk prior to the time point of consideration, compare to Fig.5.5.

In a symmetric CCF group with sequential test scheme, the dependence coefficients of the two unavailability parts are assumed equal, ie $dq_{k|n} = ds_{k|n}$. In case of pairwise separated four train systems and/or pairwise staggered test scheme, the dependence coefficients are adapted accordingly. For this purpose, the subgroup invariant SHACAM parametrisation, where parameters have the intuitively clear interpretation as

y(k) = Probability of next specific component failing, due to a shared cause, with k-1 specific components already failed (5.13)

proved to provide a workable, consistent framework.

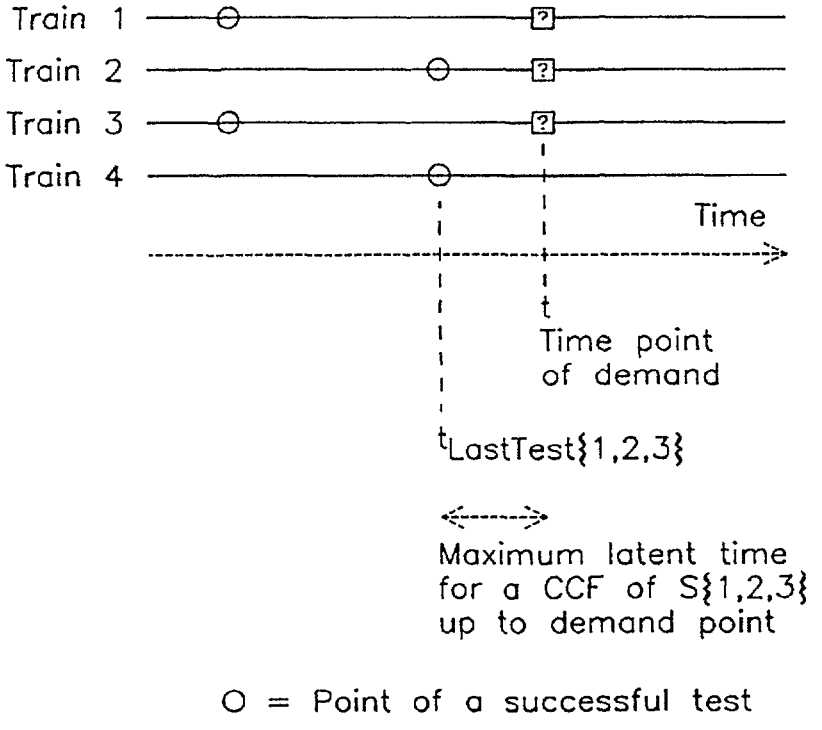


Figure 5.5 Illustration of how the latent time for timedependent CCF model is constituted in case of pairwise staggered test scheme. Prior to example demand point, train 2 is tested last, and determines the maximum latent time for CCFs shared by the considered subgroup of trains 1, 2 and 3.

The symmetric CCF model was applied also to the failure to run mode, using equivalent dependence parameters as compared to the unavailability part, as there lacks evidence to make distinction between dependence level of these different failure modes. However, proper distinction is made in total unavailability and failure rate expressions for combination terms in regard to the multiplicity in cause events. This is necessary in order to consistently apply the multiple repair model to the combination events.

5.9 Data base elaboration

Data types needed are listed in Table 5.1. The main part of the data could be inferred from TVO's own operating experience (about 20 reactor years). As primary supporting information, the compiled data for ABB Atom BWRs were used [T-book85], as well as the other data from Swedish BWRs for rare initiating events and transient probabilities. Also international data were reviewed and utilised as supporting information [PTRSD_90]. In later stages of the analysis, PRA data analysis task could be utilised.

Table 5.1 Data types required and applicable to BWR/RHR systems TS analyses.

ENTITY	DATA PARAMETERS
INITIATING EVENTS	Frequency while in power operation state Transient probabilities in shutdown changes Frequency while in hot/cold shutdown state Dependence data for CCI events Recovery time distributions
SYSTEM MODULE DATA	Standby unavailability parameters Test interval and scheme for standby modules Failure rate during mission time Dependence parameters for CCF groups Repair time distributions
MANUAL OPERATIONS	Error probabilities Recovery time distributions
PLANT RESPONSE Available time for repairs or other recoveries, when critical safety function fails (applicable to BWR/RHR TS analysis cases)	Decrease of water level in reactor given loss of feedwater Condensation pool heatup given loss of RHR Depleting battery backup for vital AC/DC given blackout situation

SD transient diagram event data could be based for the more frequent basic events, up to isolation events and main feedwater losses, on plant specific experience, supplemented by Swedish BWR experience. For primary coolant leakages, generic PRA data, and SD related data from PTS studies were utilised [PTS_HB85]. The data for CCI events of AC/DC buses are based on single failure probability information combined with dependence level judged on the basis of fault detectability and worldwide experiences of this kind of (very rare) events.

During the preparation process of this report, the reliability data for EPS were updated after a fire event at TVO II in April 1991, causing total loss of EPS. The pooled, more recent data gave somewhat higher frequency estimate for LoEPS, but a duration distribution with overall shorter recovery times. The grid connections and alternative power supply paths were also modelled in more detail. The net influence on the relative results was however small, and the conclusions of the study remained as earlier.

A module data example is presented in Table 5.2 for the most central system module of the study, system 712 pump line module PM, compare to Fig.4.3.a. There are four redundant identical PM modules, each consisting of the components listed in the data table. In the train, components are in series as a reliability structure, therefore the main reliability variables *{qs, fs, fo}* of the module are direct sums over the component variables. Repair time distributions are constructed as superpositions from the components' distributions, using mean projected unavailabilities as weights.

An example of module reliability characteristics is presented in in Fig. 5.6. It illustrates the strong influence of the state knowledge, compare with more detailed discussion about the concept of projected unavailability in Ref.[PM_SRE86].

Dependence parameters are estimated for the whole trains, and are mainly based on generic CCF data for type components.

6 EVALUATION OF RESULTS

The main results of event sequence quantifications are presented here for both undesired end events separately. Risk variables were shortly defined in Section 5.1, while a more detailed description for them is included in Ref.[NKA/RAS-450].

6.1 Main results for CoPRe|LoRHR

Instantaneous risk frequency and cumulative risk over predicted repair time are presented in Fig.6.1 for the end event CoPre|LoRHR, i.e. for the need to use filtered steam venting from the containment due to prevailing failure of RHR systems. For each failure state of RHR trains 712/721, the risk variables of the two operational alternative, continued operation (CO) and decided shutdown (SD), are presented parallel.

Table 5.2 Example description of module data for RHR train 712 module PM.

MODULE SETUP: EXAMPLE

Module	No redun- dances	Description Included components
PM	4	Pump line of shutdown service water system
		712P00# Centrifugal pump
		712K00# Flow measurement
		711V00# Suction valve
		712V#01 Nonreturn valve

MODULE DATA TABLE: EXTRACT FOR PM

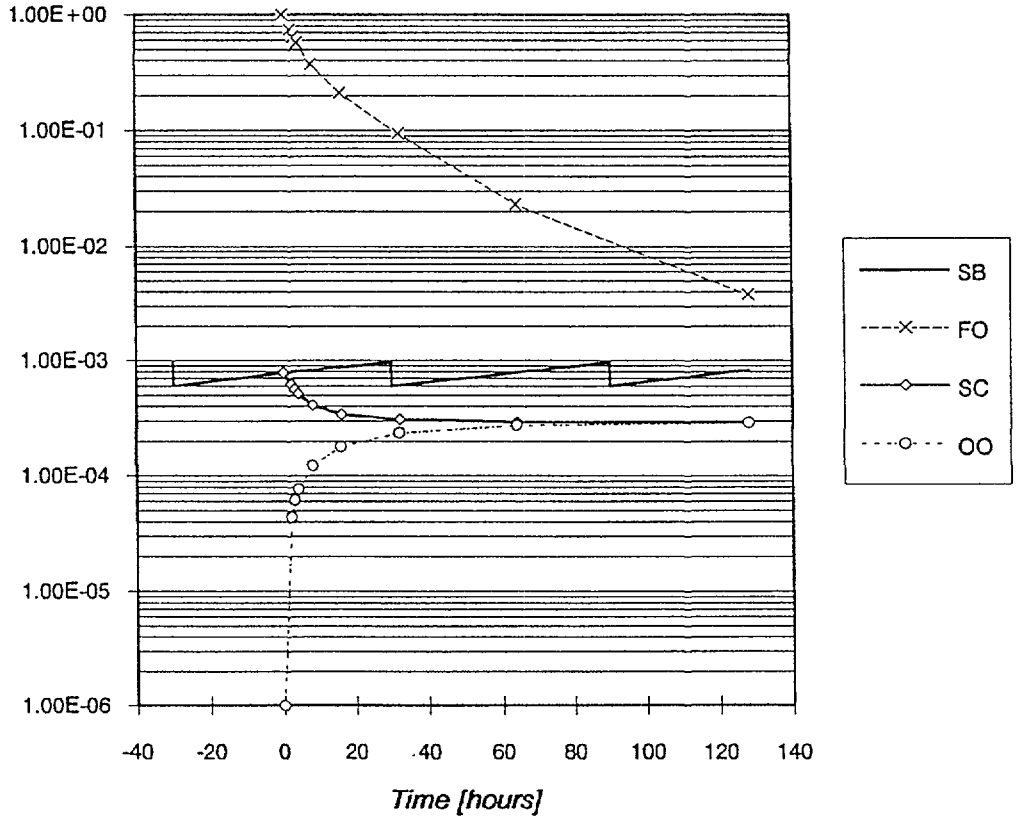
		Reliability variables			Rep.time distr.		i_tsc	Dep.par
		qs	fs	fo	zr	ar	test_int	y2..4
k_typ	m_typ$	q_hid	[1/h]	[1/h]		[h]	[h]	
1	PM				zn=1	am=11.8		
		6.0E-4	6.0E-6	2.5E-5	0.56	4	1	0.05
					0.43	20	60	0.25
					0.01	100	0	0.60

$$zn = \sum_k zr^{(k)}$$

$$am = \sum_k zr^{(k)} . ar^{(k)}$$

DATA PARAMETERS

Symbol	Unit	Description
qs		Timeindependent part of standby unavailability
fs	[1/h]	Standby failure rate
q_hid		Unvailability hidden in periodic tests
fo	[1/h]	Failure rate during mission period
zr		Fractions of multipart exponential recovery time distribution
ar	[h]	Time constants "
i_tsc		Test scheme index = 0 Timeindependent model used 1 Sequential scheme 2 Pairwise staggered scheme
test_int	[h]	Test interval
test.1	[h]	Test scheme anchor point (sub 1)
y2,y3,y4		Dependence parameters [SHACAM]

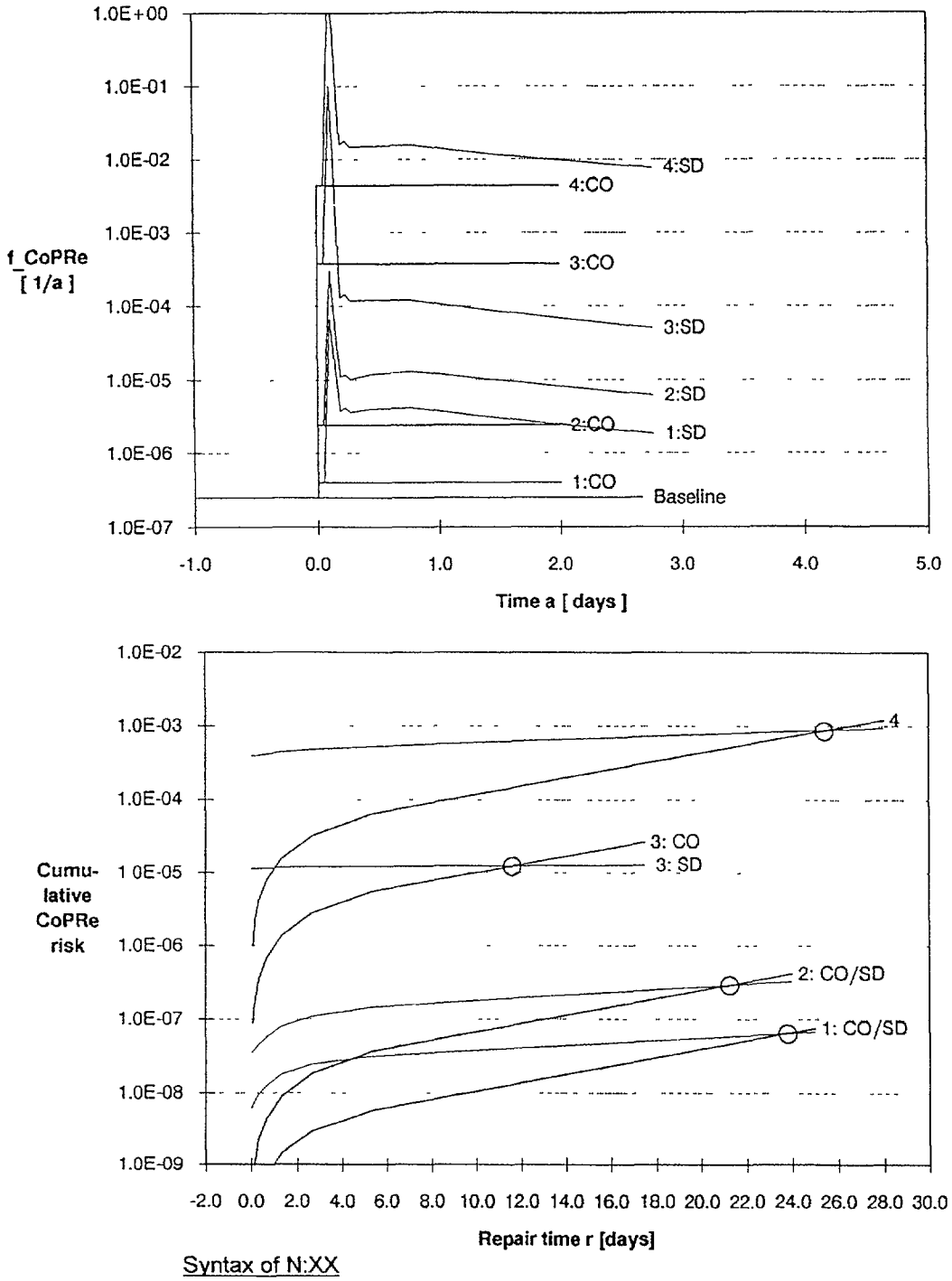


Legend

SB =	Standby state, instantaneous unavailability (latent failures possible, but no known failures or maintence downtime or other unavailability present)
FO =	Failed at demand, projected unavailability
SC =	Challenged from standby, projected unavailability, equals in the beginning with the instantaneous unavailability of standby state
OO =	Successfully started from standby, projected unavailability

Figure 5.6 Example of module reliability characteristics for system 712 train (PM): instantaneous unavailability over standby period, as well over mission time given a random demand and different assumptions about the initial operational state.

For CoPre|LoRHR, the baseline risk level is rather low, which is mainly explained by good chances of recovery during the reasonably long pool heatup time to reach containment pressure relief threshold. But in multiple failure states the risk level increases drastically. Except the triple failure state, the risk frequency decreases rather slowly in SD alternative. The triple failure state deviates qualitatively from the other ones, because the relative credit of one remaining train is highest in this case. After about 10 hours from reactor shutdown, one RHR train is in all event scenarios sufficient for decay heat removal. In single and double failure states this credit is masked by the CCF influence, which implies that it is more likely to lose all remaining RHR trains than to enter triple failure state. In quadruple failure state, this influence of partial LoRHR is not present.



Syntax of N:XX

N = Number of failed RHR trains

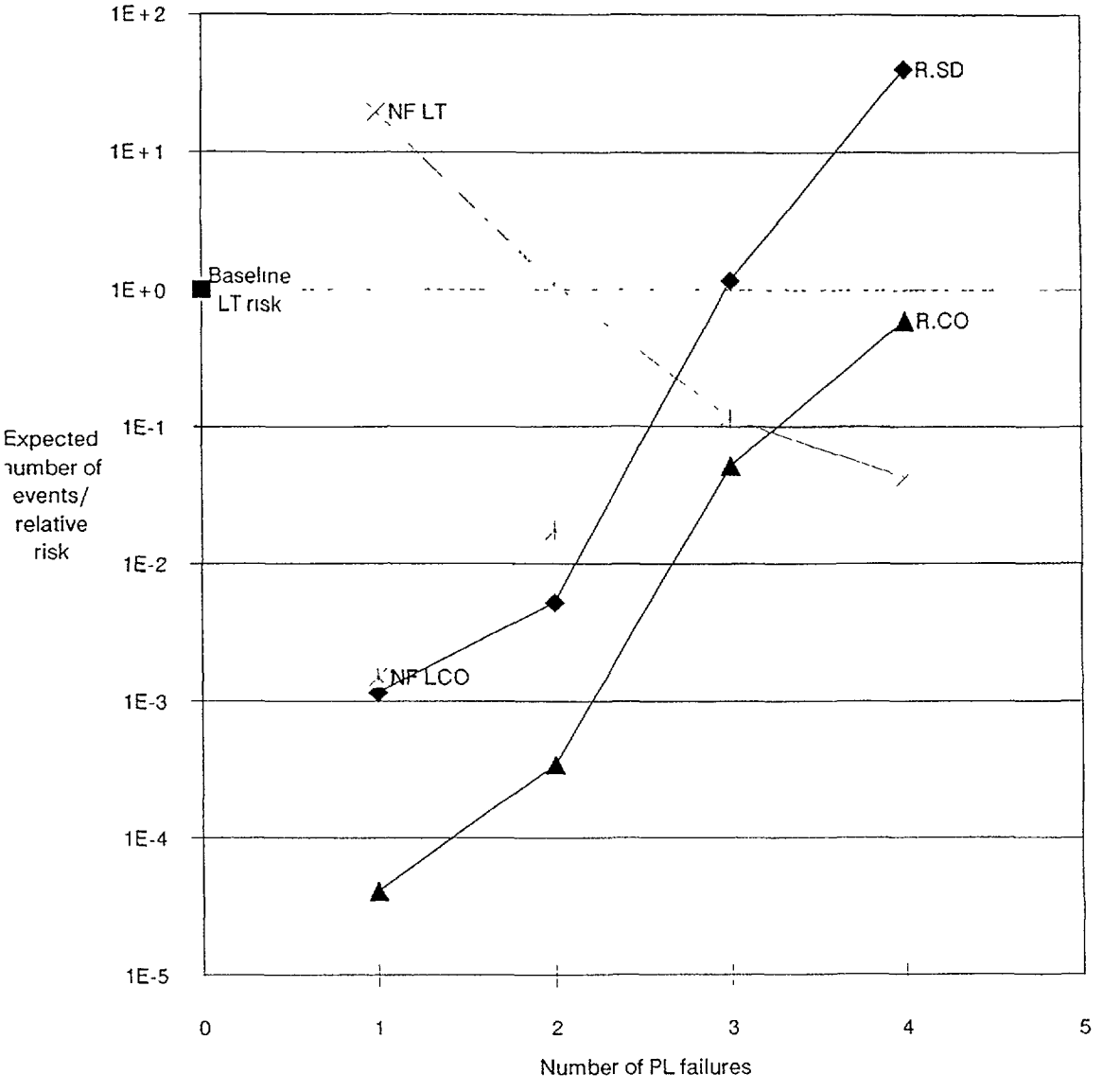
XX = CO = Continued power operation of the plant

SD = Decided shutdown of the plant

Figure 6.1 Risk frequency and cumulative risk over predicted repair time for the CoPRe|LoRHR risk.

The influence of partial LoRHR explains also the behaviour of cumulative risk over predicted repair time for different failure situations in Fig.6.1. The crossing point for CO/SD risk predictions is at shortest time for triple failure case, but even then it is at rather long time. This long threshold time is due to the increasing SD state change risk (risk peak) as the function of failure multiplicity.

The expected risk per failure event is presented in Fig.6.2, normalised with respect to baseline lifetime risk, as explained in Section 5.1. It can be concluded that with respect to CoPRe|LoRHR risk, the SD alternative is clearly disbeneficial in case of usual failures (mean repair time 12 hours).



Syntax of curve labels

NF LT = Expected number of failure situations during plant lifetime

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

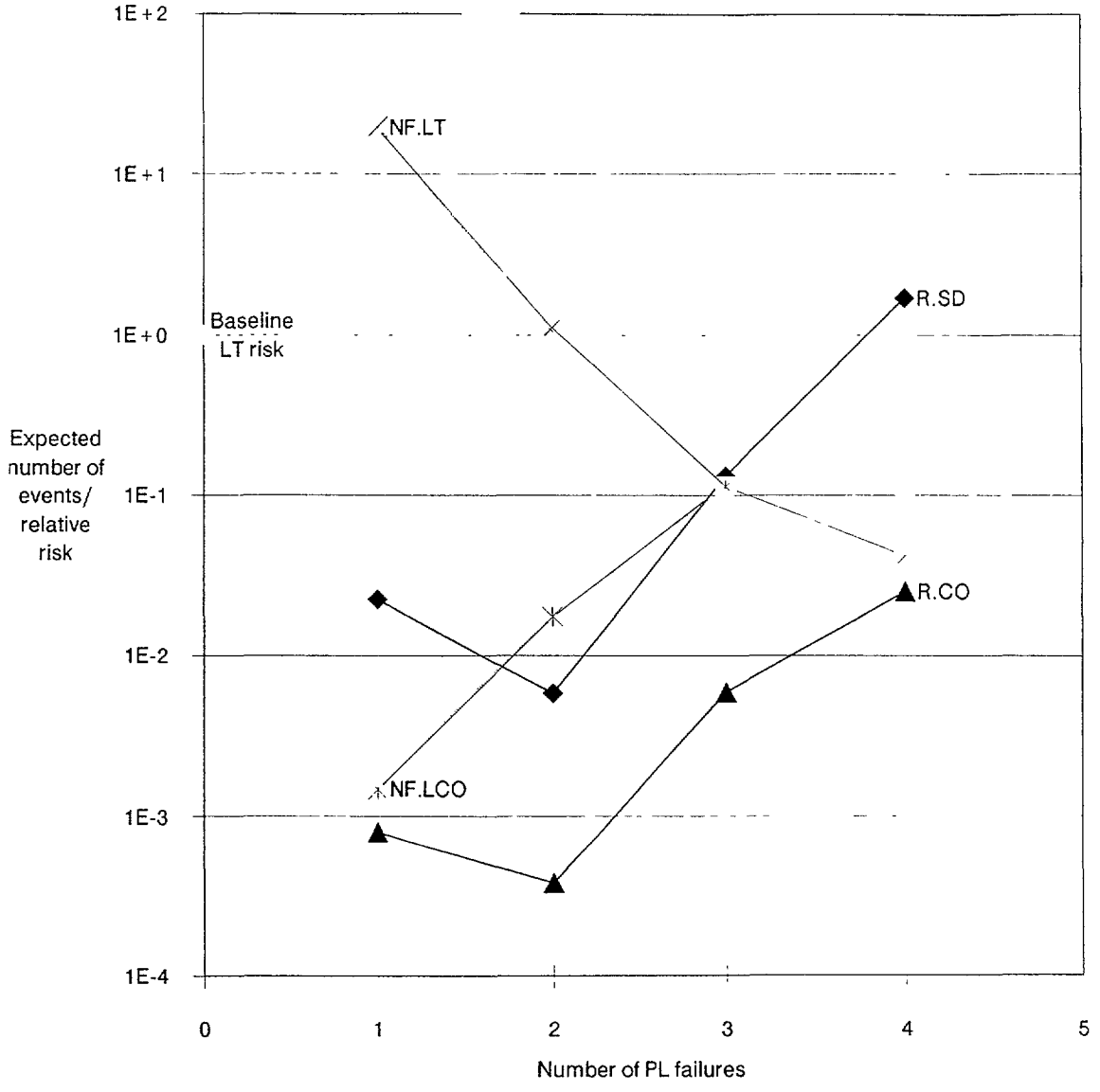
R.CO = Expected risk per failure situation assuming continued plant operation, normalised by the baseline risk over plant lifetime

R SD = Expected risk per failure situation assuming plant shutdown, normalised by the baseline risk over plant lifetime

Figure 6.2 Expected risk per failure situation, normalized with respect to lifetime baseline CoPRe|LoRHR risk.

Curve NF.LT in Fig.6.2 shows the expected number of RHR train 712 failures over plant lifetime (40 years). Curve NF.LCO indicates expected number of failure situations exceeding current AOTs and necessitating a plant shutdown. It can be concluded, that the triple and quadruple failure situations, with high risk per failure event, are not very likely to occur.

The expected risk addition of all failure situations of RHR trains 712 over plant lifetime is presented in Fig.6.3. These are obtained from the risks per failure event, in Fig.6.2, through multiplication by the expected number of failure events NF.LT, as explained in Section 5.1.5, Eq.(5.4).



Syntax of curve labels

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

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

R.CO = Lifetime risk addition for failure situations assuming continued plant operation, normalised by the baseline risk over plant lifetime

R.SD = Lifetime risk addition for failure situations assuming plant shutdown, normalised by the baseline risk over plant lifetime

Figure 6.3 Expected lifetime risk additions of failure situations, normalized with respect to lifetime baseline CoPRe|LoRHR risk.

It can be concluded, that the risk addition for CoPRe|LoRHR of triple and quadruple failure states makes about double as much as baseline risk, for current AOTs requiring SD in these failure states. Giving about 3 days AOT for these would effectively diminish the risk addition by factor 10, i.e. the relative benefit is substantial. It should be noted that in absolute terms the benefit is small, because CoPRe|LoRHR risk is at low level (compare to baseline risk frequency in Fig.6.1)

6.2 Main results for CoreD|LoFW

In a similar way, the results are presented for the other, more severe end event CoreD|LoFW, i.e. core damage due to prevailing loss feedwater/core cooling.

Fig.6.4 shows the risk frequency and cumulative risk over predicted repair time. The patterns over different failure multiplicity are somewhat different as compared to CoPRe|LoRHR. This is on one hand due to higher baseline risk level dominated by other contributions than RHR system failures, and on the other hand due smaller relative SD state change risk peak, which however here also increases as the function of failure multiplicity. As a net influence, the crossing points for cumulative risk of SD/CO alternatives over predicted repair times are relatively short for single and double failures, but substantially long for triple and quadruple failures.

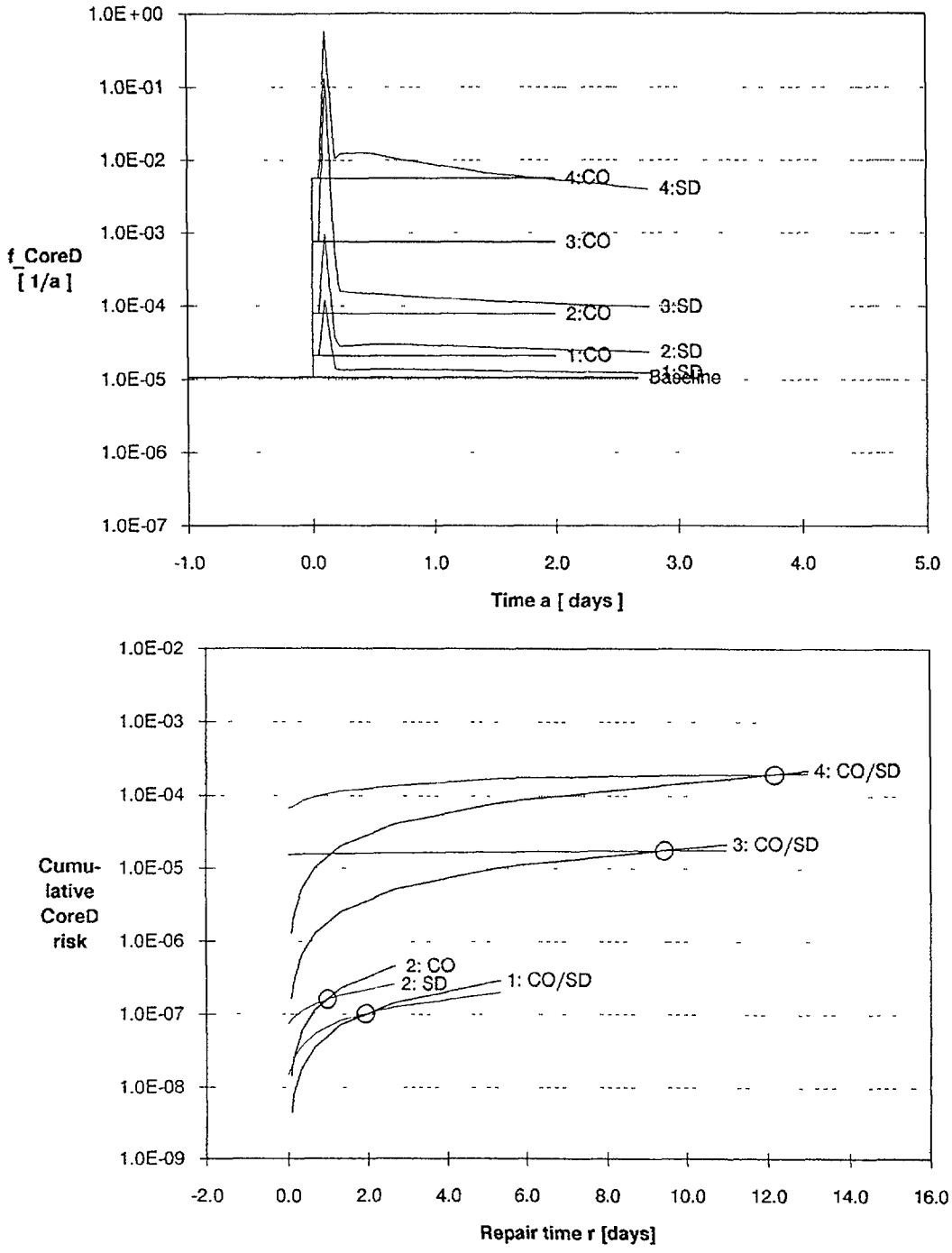
It can be concluded that the degraded capability of the RHR function severely affects the operability of the feed water function only in triple and quadruple failure situations of RHR trains. In single and double failure states the impact on CoreD|LoFW risk is small, and hence the SD related risk is then also relatively small.

Consequently, the expected risk per failure event for CoreD|LoFW are closer for low order failure states, but clearly disbeneficial for SD in triple and quadruple failure states, Fig.6.5. This pattern combined with relatively high baseline risk means that the expected lifetime risk additions of failure situations remain relatively small, as shown in Fig.6.6. Hence, the conclusions about AOTs for triple and quadruple failures can be mainly based on the comparison of the high situation specific risks and crossing point for the cumulative risk of SD/CO alternatives over predicted repair times, Fig.6.4.

6.3 Interpretation of predictions, resolution criteria

The results show that in relative comparison, SD alternative is clearly disbeneficial over usual repair times, as compared to CO alternative in triple and quadruple failure states of RHR trains 721/712. This is valid for all risk viewpoints:

1) Instantaneous risk frequency
2) Cumulative risk over predicted repair time
3) Expected risk per failure situation
4) Expected risk additions of failure situations in long term total risk



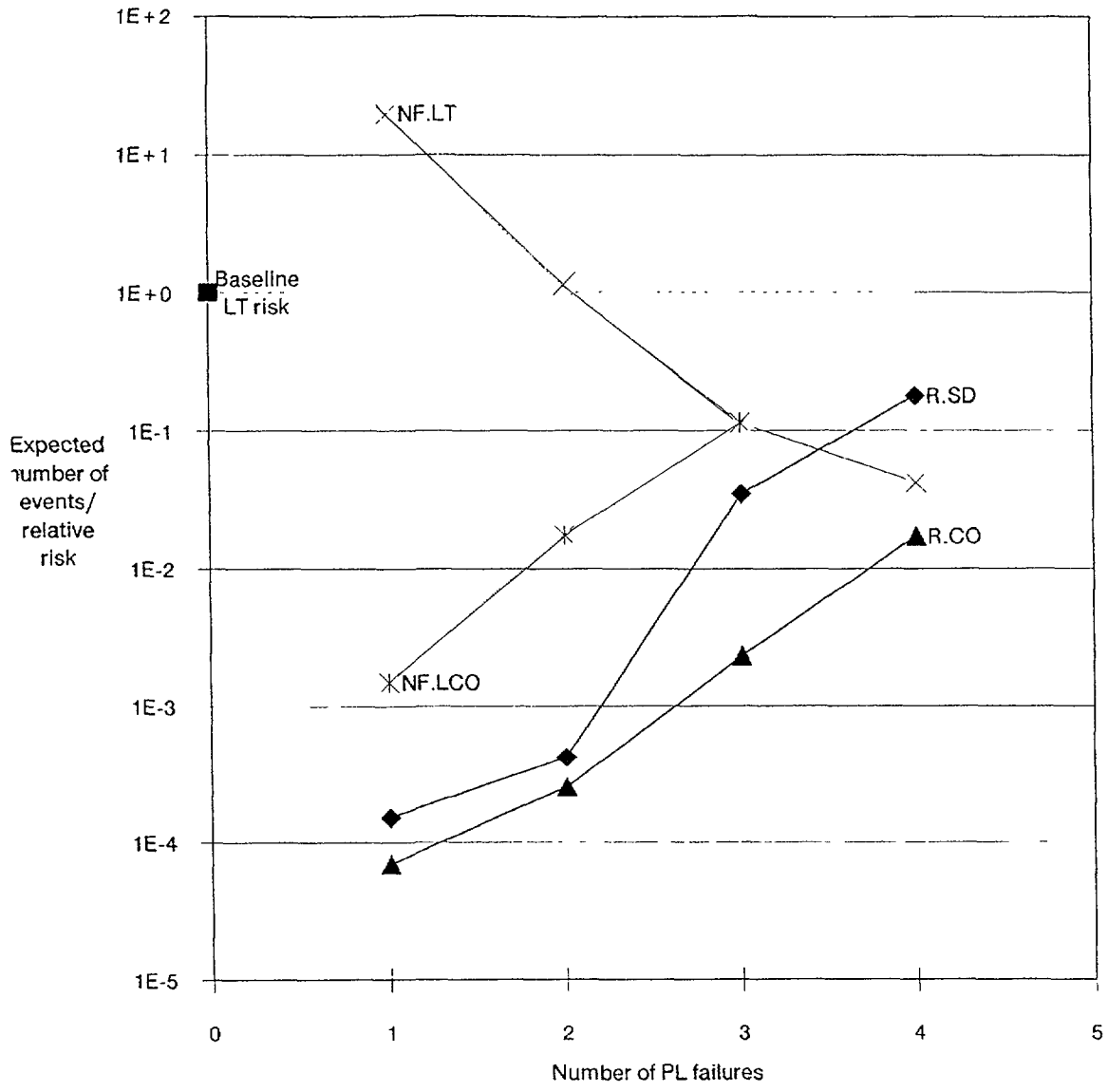
Syntax of N:XX

N = Number of failed RHR trains

XX = CO = Continued power operation of the plant

SD = Decided shutdown of the plant

Figure 6.4 Risk frequency and cumulative risk over predicted repair time for the CoreD|LoFW risk.



Syntax of curve labels

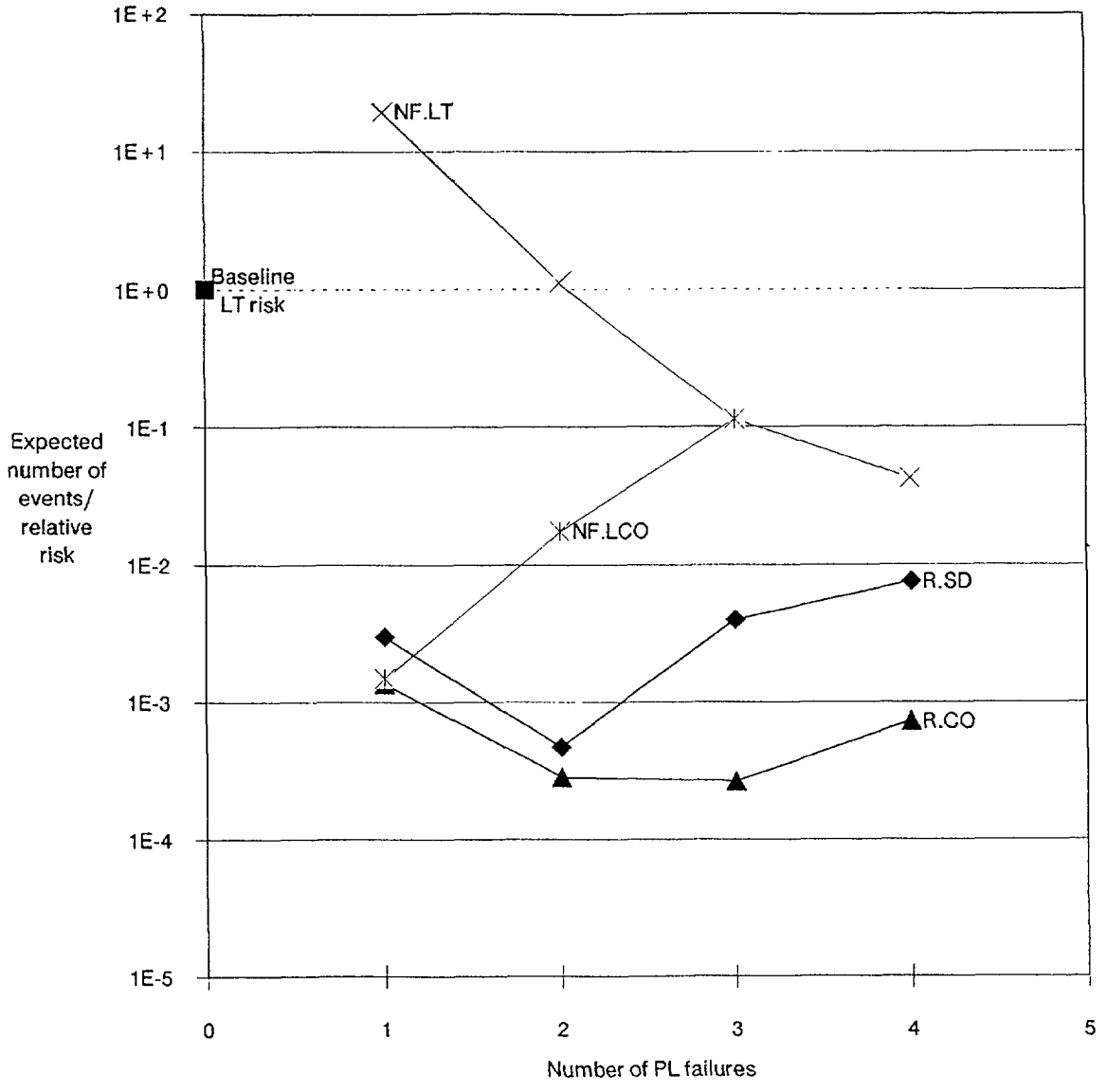
NF.LT = Expected number of failure situations during plant lifetime

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

R.CO = Expected risk per failure situation assuming continued plant operation, normalised by the baseline risk over plant lifetime

R.SD = Expected risk per failure situation assuming plant shutdown, normalised by the baseline risk over plant lifetime

Figure 6.5 Expected risk per failure situation, normalized with respect to lifetime baseline CoreD|LoFW risk.



Syntax of curve labels

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

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

R.CO = Lifetime risk addition for failure situations assuming continued plant operation, normalised by the baseline risk over plant lifetime

R.SD = Lifetime risk addition for failure situations assuming plant shutdown, normalised by the baseline risk over plant lifetime

Figure 6.6 Expected lifetime risk additions of failure situations, normalized with respect to lifetime baseline CoreD|LoFW risk.

For low order failure states, specially for the primary risk end event CoreD|LoFW, the alternatives SD/CO are close to each other. The degraded RHR function has then still only a relatively small impact on the operability of reactor core cooling, which means that the SD related risk is also small. Furthermore, the contribution of the low order failure situations is rather small relative to the baseline risk level and total average risk. Hence flexible AOTs, and the current rules in particular, are motivated by the risk analysis results for single and double failures.

Due to the specific risk profile for the TVO I/II plant, specially due to the small likelihood of entering high risk situation of triple or quadruple failure state of RHR trains 712/721, the conclusions about AOTs could mainly be based on the comparison of cumulative risk over predicted repair time and expected risk per failure situation (points 2-3 above). The other risk viewpoints just confirmed the conclusions.

6.4 Identification of uncertainties, sensitivity analyses

Similarly as in PRA studies, this kind of risk analysis is made under different kinds of uncertainties related to boundary conditions, modelling simplifications, and sparse or judgmental data.

The most important boundary condition was considering risks by the use of two undesired end events, need for filtered venting from containment and reactor core damage. An additional consideration was, however made, to confirm that a more refined consequence classification would not significantly affect the conclusions.

Another primary limitation was that internal initiators only were considered. During the preparation process of this report, additional work was done in order to evaluate the influence of fire and flood initiators, based on corresponding extensions of TVO PRA study in 1991. Among the fire and flood initiators, those which render inoperable both MFWS and reactor water cleanup path 321-331 for RHR, proved to contribute significantly, somewhat more to the continued operation alternative than to the plant shutdown alternative, given a failure situation of RHR trains 712/721. Still the relative results were not affected so much. The earlier conclusions thus remain valid.

Going to more detailed features, the following modelling assumptions and simplifications were identified and considered most important in the study:

- Restoration of turbine condenser to be used as a steam sink, when the ordinary RHR paths are failed
- Manual opening of isolation valves (by use of local operations with portable high pressure equipment) of the normal SC system 321 when they are blocked in a blackout situation
- Partial plugging of system 322/323 suction filters in the condensation pool, and manual recovery by flushing, in a LOCA situation

- Critical temperature thresholds and assumption about water mixing in the condensation pool heatup model, and uncertain local recovery possibilities after entering pressurised state in the containment

For the data uncertainties, the following parts were considered most significant:

- Likelihood of errors in the capacity increase of the cleaning water system 331, when needed as the last resort for RHR function
- Reliability of external power supply and distribution of the restoration time
- Likelihood of Y isolation transients in the course of decided shutdown
- Likelihood of CCFs, and CCIs due to multiple failures AC/DC buses

During the course of the study, systematic sensitivity analyses were made for the identified uncertainty items as listed above. Two examples are presented in Figs.6.7-8. They show the usual finding that the relative results, i.e. risk ratio of SD/CO alternatives, is in many cases quite insensitive with respect to uncertainties.

The results for quadruple failure case were also checked by manual calculations for the most dominant contributions, in order to verify the calculation program.

Despite many modelling and quantification uncertainties included in this kind of analysis, it can be concluded, that the qualitative and quantitative results provide much improved information for the AOT issue, and reduce thus effectively the general uncertainty of making decisions about AOT rules.

7 PROPOSED MODIFICATION OF AOT AND OPERATING INSTRUCTIONS

During the course of the study, the principal resolution alternatives were specified as shown in Table 7.1, including their qualitative benefits and drawbacks.

7.1 Principal justifications, consideration of influences

To summarize the risk analysis results, following conclusions about AOT resolution alternatives for RHR trains 712/721 can be made:

1) In case of single failures, the risk frequency increase is small and also the risk over expected repair times is small. The current 30 days AOT is deemed suitable.

2) In case of double failures, the risk frequency increase is moderate, but the predicted risk over usual repair times (of less than one day) for continued operation is still lower than the risk of shutdown alternative. The current 3 days AOT is deemed suitable. It should be emphasized that the TVO experience shows that the mean repair time of RHR train componens is 12 hours.

3) In case of triple or quadruple failures, the immediate shutdown constitutes a significantly higher risk than continued operation over usual repair times.

Because the advantage of the continued operation for usual repair times in triple or quadruple failure situations is so obvious, the requirement in the current TS to reach cold shutdown in 24 hours is recommended to be changed to allow maximum of 3 days AOT.

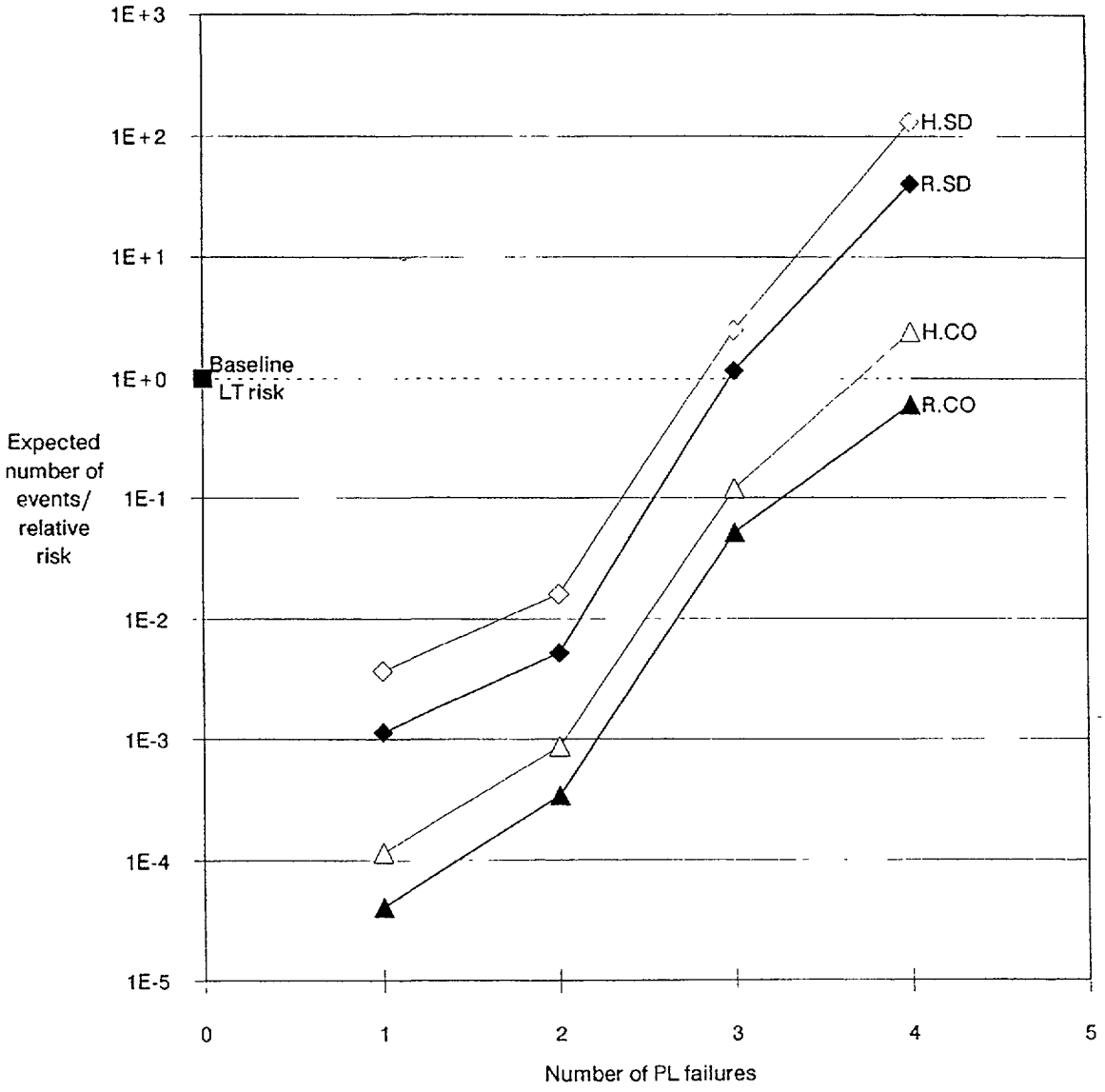


Figure 6.7 Sensitivity of the CoPRe|LoRHR risk per failure situation, with respect to the recovery during CoOPS. The expected risk per failure situation H.XX is calculated without any recovery during CoOPS after T = 95 °C. Compare with Fig.6.2.

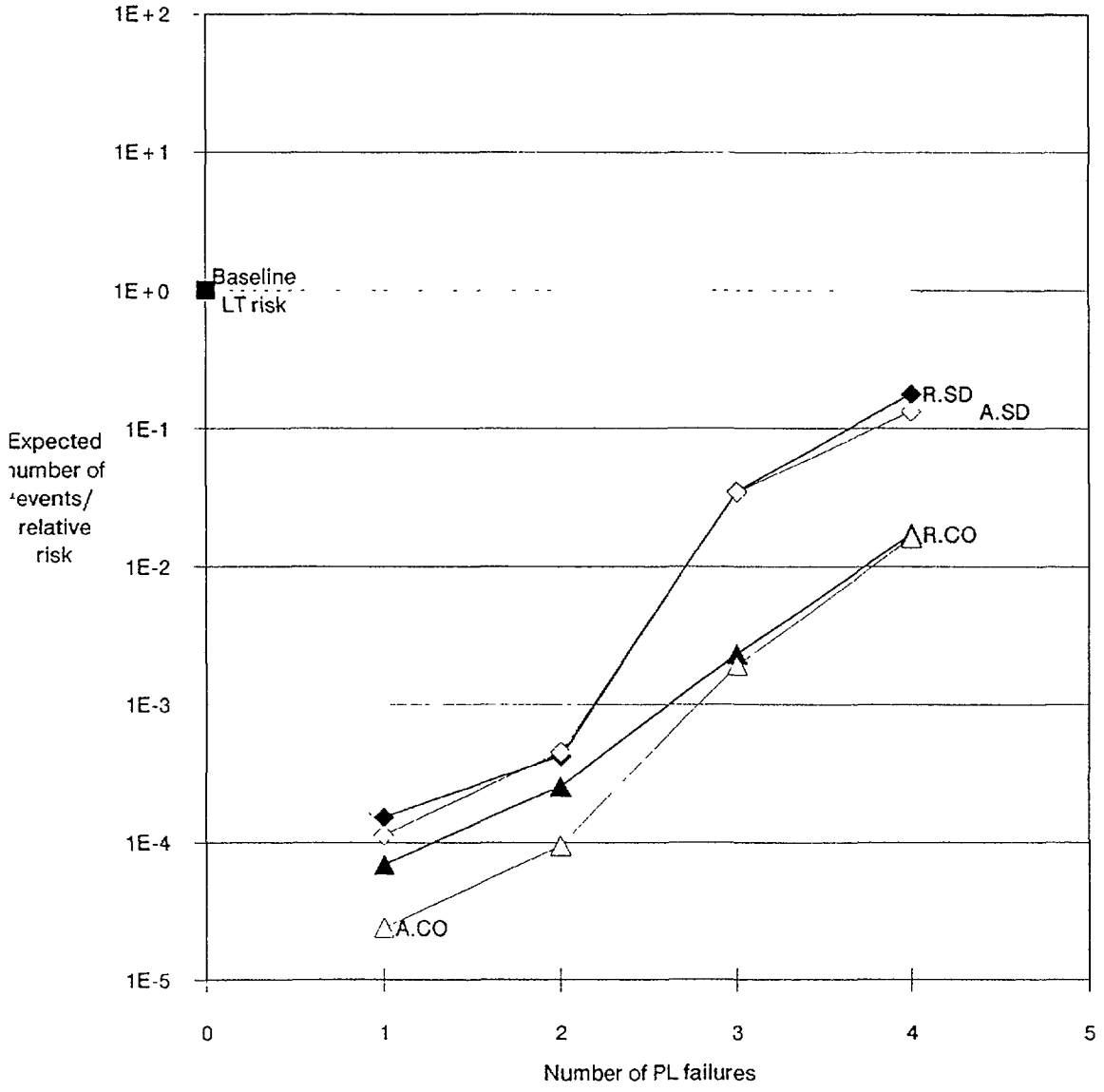


Figure 6.8 Sensitivity of the CoreD|LoFW risk per failure situation, with respect to the latent unavailability of AC/DC bus faults. In cases A.XX, the latent part has been increased from 10% to 30%, in relation to spontaneously revealing faults. Compare with Fig.6.5.

The plant level risk influences of the proposed AOT modification is shown in Fig.7.1 with respect to long term average risk. It can be concluded, that the expected overall risk impact is negligible, and therefore decision making can be based on the relative results for the risk ratio of SD/CO alternatives.

7.2 Operation scheme in multiple failure situations

The detailed specification of modified AOT rules appeared to be a complicated matter. Firstly, it was noticed that it was necessary to eliminate chaining of failures. It was considered

Table 7.1 Specification of benefits and drawbacks of the AOT alternatives for RHR trains 721/712. If not otherwise explicitely stated, the common rules are (1) startup RHR trains prior to actual SD operations, and (2) in case of additional failures detected, postpone SD, if possible within the specifications, aiming to get at least two trains restored into operation before SD.

	ALTERNATIVE	BENEFITS	DRAWBACKS
I	No time constraints specified, prompt repair measures emphasized	Very clear rule	In case of 3..4 failures the risk frequency is high, which is in principle difficult to accept for an unlimited time
II	AOT of 30 days for single failure, 3 days for multiple failure counted from the last failure detection	Still relatively simple rule, restricts already efficiently long term power operation in 3..4 failure states	Chaining of failure states possible, although unlikely to result in power operation longer than 6..9 days in 3..4 failure states.
III	AOT of 30 days for single failure, 3 days for multiple failure counted from the second failure detection, however, at least 1 day from the last failure	Restricts efficiently long term power operation in 3..4 failure states, eliminates chaining possibility of failure states	Moderately complex rule
IV	AOT of 30 days for single failure, 3 days for multiple failure counted from the second failure detection. In double failure state when 3 days' AOT is predicted to be exceeded, and in triple failure state, the remaining intact trains should be tested, preferably at 1 day point of elapsed AOT. SD should be undertaken if two trains are operable or no trains are expected to be repaired during the remaining AOT time. Otherwise SD is still postponed with aim to get more RHR trains operable so that SD could be done preferably with two trains, or at least one train operating. In any case SD shall be undertaken at the prefixed three days maximum AOT.	Eliminates chaining problem	Complex rule

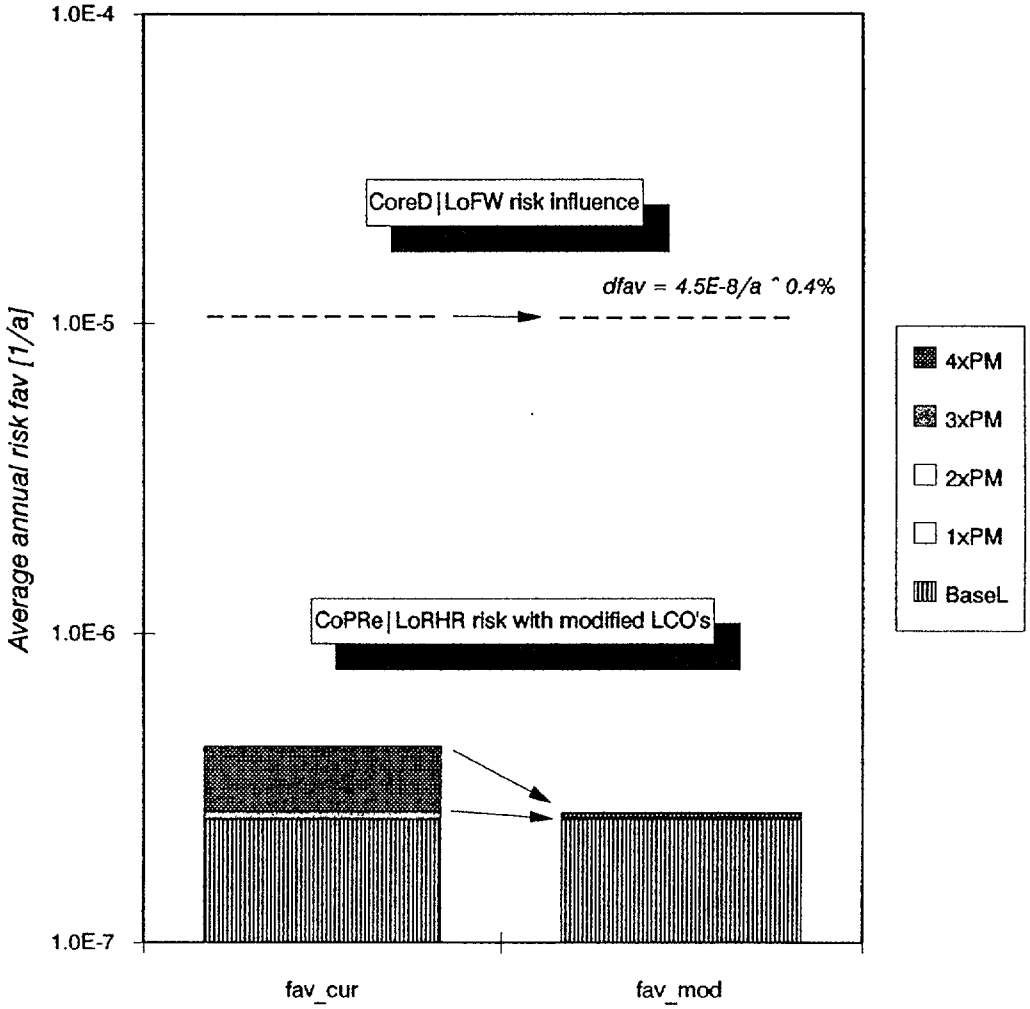


Figure 7.1 Influence of allowing 3 days AOT for triple and quadruple failure situations of RHR trains 712 (PM modules). The failure situations of RHR trains 721 (PU modules) have approximately the same contribution.

undesirable that the rule would give extension to AOT, if additional RHR train failures would be detected when preparing LCO shutdown and starting those trains. This problem finally led to the fourth resolution alternative in Table 7.1 with a prefixed maximum AOT limit of 3 days applicable to a multiple failure state as a whole.

Because the detailled specification of the proposed AOT rule became rather complex, a procedure diagram was developed using the recently developed scheme of emergency procedures [TVO_EmP].

The procedure diagram is presented in Fig.7.2. It gives guidance how to proceed when multiple failure is detected in the RHR trains 721/712 during power operation. In such a case, the plant is in the state of 3 days LCO. There are two ways to exit this state:

1) All but one of the failures are repaired, then the 30 days LCO state is entered

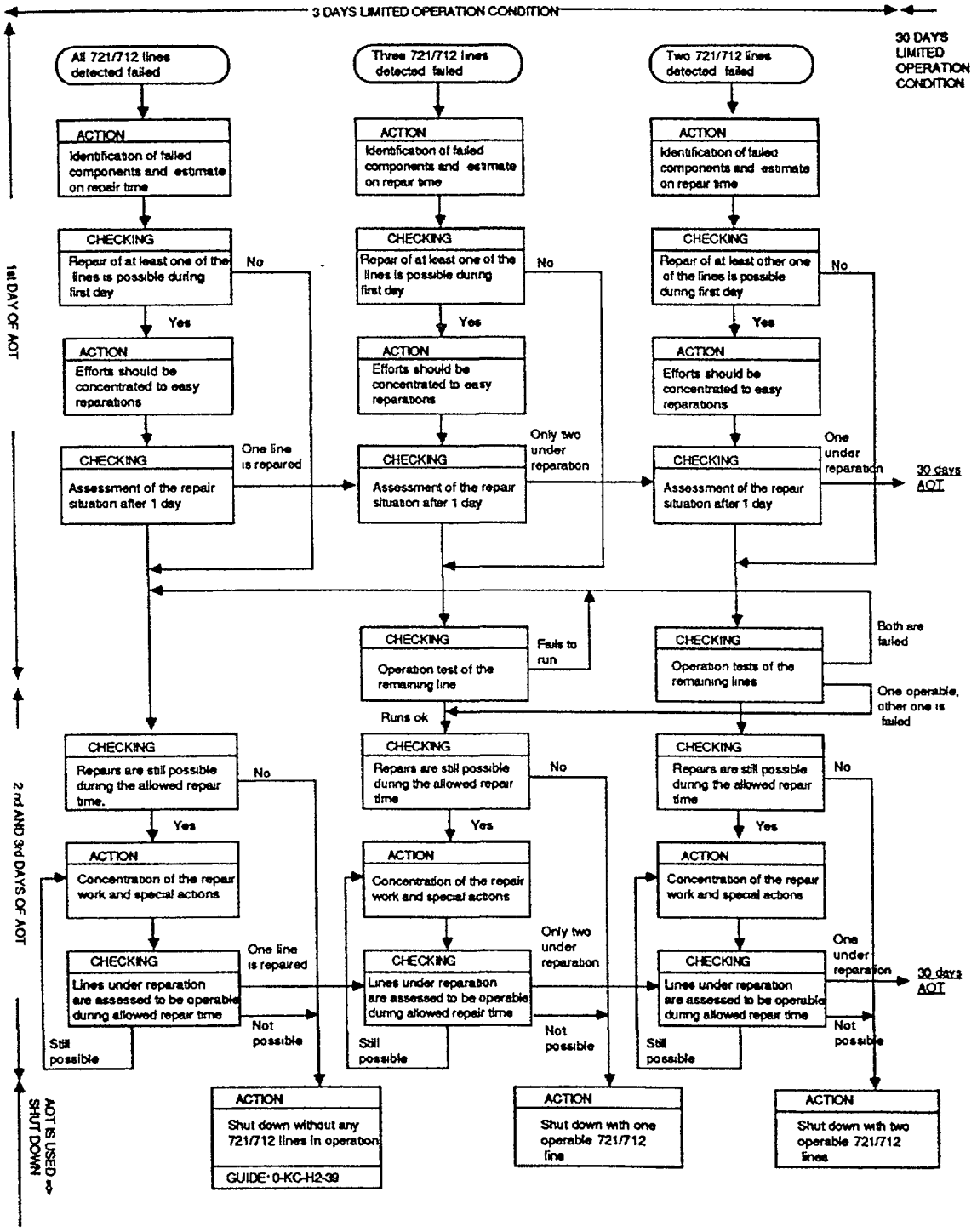


Figure 7.2 Procedure flow diagram which is proposed to aid operators in multiple failure situations.

2) No more repairs are possible during the remaining prefixed maximum 3 days AOT, counted from entering 3 days LCO state, and then the plant shall be shut down to cold shutdown state to complete the repairs.

If the repairs have not been completed during the first day of 3 days AOT, and specially if it is expected that they cannot be successfully completed during the 2 days AOT left, the remaining, intact trains are recommended to be tested at that time point in order to retain still AOT for the repairs of eventually detected additional failures. These additional tests are recommended to be carried out with special care, preceeded by a diagnostic of the possible presence of CCF, in order to avoid unnecessary damages in component parts and to facilitate prompt recovery.

8 SUMMARY OF EXPERIENCES

The relative risk difference for the justification of the continued operation over reasonably long repair times - in the residual heat removal systems with four redundant subsystems - was large, more significant than expected. At this point, when the contributing factors are well understood, the results appear just logical. The relationship between the continued power operation versus shutdown alternative depends on the safety system configuration and capacity, plant transient profile and many other plant specific factors. Hence, the results obtained in our particular case cannot be directly generalised.

The risk analysis methods have proved to be applicable and useful in the comparison and enhanced understanding of operational decision alternatives. The complexity of phenomena to be studied implies, however, that both good analytical skills and understanding of plant operations are necessary for successful treatment of the problem.

The absolute numerical results are sensitive to many input parameters and model assumptions. Fortunately, the conclusions with regard to AOT rules can mostly be based on the relative results, which are sensitive for only a limited part of uncertainties. But even the relative results need to be systematically verified with respect to uncertain data, modelling simplifications and other analysis limitations in order to provide a firm basis for drawing conclusions. Also the possible dependence between different uncertainty factors need to be addressed.

Based on the results, the AOT rules for the residual heat removal systems considered are aimed to be modified so that the repair time limit of three days - currently allowed only in double failure situations - will be extended to situations of three or all four redundant trains failed. The rule change corresponds to choice of the operational alternative with smallest risk in rare, but possible high risk situations.

The methodology developed can be used to support resolution of other problem issues of technical specifications as well, and may find uses in Living PSA applications more generally.

ACKNOWLEDGEMENTS

The authors acknowledge the central role of a work team at TVO, for a successful undertaking of this versatile study, where many kind of information input from the operating, maintenance and safety staff proved vital. Specially, the contribution by M.T. Saarenpää in system modelling and data preparation tasks is acknowledged.

In the earlier development stage, this study served also as a practical case for the Nordic research project NKA/RAS-450 on the risk-based approach to Technical Specifications. The authors will thank the whole project group, and the project K.J. Laakso from the Technical Research Centre of Finland specially, for the many comments and suggestions during the course of this study.

When finalising this report, useful comments were obtained from P.K. Samanta and I. Kim, Brookhaven National Laboratory, in order to improve documenting the methodological features.

REFERENCES

AOT_PRA81 Mankamo, T., Aaltonen, P. Porvari, P. and Virolainen, R., Allowable repair downtime in standby safety systems. ANS/ENS Topical Meeting on PRA. September 20-24, 1981, Port Chester, New York.

AT_PSA87 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), Zurich, Aug 31 - Sep 4, 1987, pp. 765-770.

DECET_85 Mankamo, T., Decision event tree. SRE Symposium 1985, Trondheim.

EPRI_GO GO methodology. EPRI NP-3123. Prepared by Energy Incorporated, Kent, Washington, 1983.

EPRI5238 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.

ESumRepo88 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, April 1988.

ETS_PSA85 Mankamo, T., Perhonen, H., Pulkkinen, U., Kosonen, M. & Vanhala, J., Experiences from the use of PRA methods in the re-evaluation of technical specifications. ANS/ENS Topical Meeting on Probabilistic Safety Methods and Applications. February 24 - March 1, 1985, San Francisco.

ExPSA_TVO86 Kosonen, M., Piirto, A., Vanhala, J., Mankamo, T. & Pulkkinen, U., Experiences of the use of PSA methods at the TVO poer plant. Teollisuuden Voima Oy, June 1986.

IAEA90_JP Hioki, K. & Kani, Y.,Risk based evaluation of technical specifications for a decay heat removal system of an LMFBR plant. IAEA Technical Committee Meeting on The Use of PSA to Evaluate NPP's Technical specifications, Vienna, 18-22 June 1990.

IAEA90_M Mankamo, T. and Kosonen, M, Operational decision alternatives in failure situations of standby safety systems. IAEA Technical Committee Meeting on The Use of PSA to Evaluate NPP's Technical specifications, Vienna, 18-22 June 1990.

IAPS_Pro90. Pilot studies, program proposal. Prepared at the IAEA Technical Committee Meeting on the Use of PSA to Evaluate NPP's Technical Specifications, June 18-22, 1990, Vienna.

Imp_TeRe Mankamo, T, Pörn, K. & Holmberg, J., Uses of risk importance measures. Technical report NKS/SIK-1(90)6, published by Technical Research Centre of Finland, Reserch Notes 1245, Espoo 1991.

LoAFWS87 Mankamo, T., Operational alternatives in failure situations of standby safety systems - application to the AFWS of Loviisa 1. Seminar on the reliability of VVER reactors, 1987.

MiK_Dip85 Kosonen, M., Analysis of Technical Specifications for failure situations in residual heat removal systems of TVO I/II plant. M.Sc. study, Technical University of Lappeenranta, 1985 (In Finnish).

MTS_Dip86 Saarenpää, M.T, Risk comparison of plant shutdown versus continued operation in failure situations of residual heat removal systems for TVO I/II plant. M.Sc. study, Technical University of Helsinki, 1986 (In Finnish).

NKA/RAS-450 Optimization of technical specifications by use of probabilistic methods - a Nordic perspective. Final report of the NKA project RAS-450. Ed. K.Laakso. Prepared by a team consisting of K.Laakso, M. Knochenhauer, T. Mankamo & K.Pörn. Nord Series 1990:33, May 1990.

NKA/SAK-1 PRA uses and techniques - a Nordic perspective. Ed. S. DINSMORE, Nordic Liaison Committee for Atomic Energy (NKA), June 1985.

PM_IAEA85 Heinonen, R. & Piirto, A., Preventive maintenance of safety systems during normal power operation of TVO¦s nuclear power plant. IAEA International Symposium on Advances in NPP Availability, Maintainability and Operation, Munich, 20-23 May 1985.

PhM_SRE86 Mankamo, T., Phased mission reliability - a new approach based on event sequence modeling. Scandinavian SRE Symposium '86, 14-16 October 1986, Otaniemi

PO_PSA89 Mankamo, T., Phased operations and recovery options - advances in event sequence quantification. PSA'89, Pittsburgh, April 2-7, 1989.

PRA_PGuide PSA procedures guide. NUREG/CR-2815, 1985.

PSA91_CS Novakova, H & Kovacs, Z., Optimization of VVER technical specification by use of probabilistic methods. Int.Symposium on the Use of Probabilistic Safety Assessment for Operational Safety, PSA'91. Vienna, 3-7 June 1991.

PTRSD_90 Mankamo, T., Plant transients in shutdown/startup conditions. Prepared by Avaplan Oy, August 1990, at request of the Finnish Centre for Radiation and Nuclear Safety, Report STUK-YTO-TR 24, December 1990.

PTS_HB85 Minarick, J.W., Austin, P.N. & Selby, D.L., Pressurized thermal shock evaluation of the H.B.Robinson Unit 2. SAIC, ORNL, Draft March 19, 1985.

RELVEC85 Task-oriented reliability analysis program RELVEC. Technical Research Centre of Finland, 1985.

Seabrook Seabrook Safety Probabilistic Study. Prepared for Public Service Company of NH and Yankee Atomic Electric Company by Pickard, Lowe and Garrick, Inc., PLG-0300, December 1983.

SHACAM Mankamo, T.,SHACAM, shared cause model of dependences - a review of MLG method and a modified extension of the Beta Factor method. Avaplan Oy, March 1985.

SRE_90PP Mankamo, T., Operational decision alternatives in failure situations of standby safety systems - Development of probabilistic approach and PC program TeReLCO. Scandinavian SRE Symposium 1990, 8-10 October 1990. Proceedings.

Te_dRAOT Work notes: Delta risk - AOT correlation. T. Mankamo, 25 June 1991.

ThesisM86. Mankamo, T., Availability analysis of standby safety systems, basic methodology for the optimization of the test and repair arrangements and limiting conditions for operation. Thesis Manuscript, 1986.

TI_Opt88 Mankamo, T. & Pulkkinen, U., Test interval optimization of standby equipment, Technical Research Centre of Finland, Research notes 892, September 1988

TS_Resol89 Mankamo, T., Engqvist, A. & Kosonen, M., Resolution strategy of TechSpec problems. 12 June 1989.

TSB_Mad87 Brolin, S., Piirto, A., Laakso, K. & Wahlström, B., Technical Specifications for Nordic BWRs. Structure, experiences and ongoing problems. CSNI/Unipede Specialist Meeting on Improving Technical Specifications for Nuclear Power Plants. September 7 - 11, 1987, Madrid.

TSD_Mad87 Piirto, A., Mankamo, T. & Laakso, K., Development of Technical Specifications using probabilistic methods. CSNI/Unipede Specialist Meeting on Improving Technical Specifications for Nuclear Power Plants. September 7 - 11, 1987, Madrid.

TVO_EmP TVO I/II Emergency procedures, instructions, 1990.

TVO_PRA TVO I/II Probabilistic Risk Assessment. 1989.

TVO_Pros TVO I/II power plant. Prospectus, 1990.

UCLA_83 Apostolakis & Chu, T., Time dependent accident sequence analysis. UCLA-ENG 83-15, March 1983.

V&S_BNL89. Vesely W. & Samantha P.K., Risk Criteria Considerations in Evaluating Risks from Technical Specification Modifications. Technical Report, BNL & SAIC, Draft, January 1989.

Wagner87 Wagner, D.P., Minton, L.A. & Gaertner, J.P., Risk-based analysis methods and applications to nuclear power plant technical specifications. CSNI-Unipede Specialist Meeting on Improving Technical Specifications for NPPs. Madrid, 7-11 September 1987.

DEFINITIONS

The following definitions are based on earlier or ongoing work in the subject area. Any specific changes from earlier definitions are to clarify the terminology, which is still evolving in this subject area.

Allowed outage time

Allowed outage time (AOT) gives the maximum time for repair of safety related equipment in a given operational state. The plant must usually be placed to in safer operational state, if the operability of the faulty equipment is not reached within its AOT. For the faults detected in the power operation state, any repair time exceeding the AOT will require a controlled shutdown in order to complete the repair (usually cold shutdown state).

Average risk level

In the standard PSA approach, the average risk level is calculated by modelling the repair and maintenance downtimes (during power state) as explicit basic event in the component model or by including the fractional downtime in the lumped unavailability model of the component. The average risk level represents the long term mean of the time dependent risk level over the baseline and temporary risk increase states associated with repair and maintenance periods. The average risk level is used as the primary reference risk level, often called the nominal risk level, which uses the **nominal** modelling assumptions and input data.

Baseline risk level

This is the risk level of the plant during power operation assuming that no failures are detected in safety systems and no subsystems are isolated for maintenance. If a demand occurs during the baseline state, the latent or undetected faults in the standby period and failures during the mission time still contribute to the overall system failure probability, and to the baseline risk level. Temporary outages of equipment in safety systems will increase the total plant risk level over the baseline risk level.

Instantaneous risk level

This is the risk level of the plant at a given instant of time based on the current operational state of the plant and its safety systems. Temporary outages of safety equipment may increase significantly the risk level over the baseline risk level.

Limiting condition for operation

The limiting conditions for operation (LCOs) are a part of the plant's technical specifications. These rules are designated to maintain the plant operation within the bounds of safety analyses. The LCOs specify requirements on the number of subsystems that should be operable at different operational states and the allowed outage times for inoperable equipment. These also define specific action statements if such requirements cannot be met.

Technical specifications

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

Test strategy or scheme

The test strategy is concerned with the choice of surveillance test methods and placement (relative timing scheme) of the tests within a group of redundant components or in relation to functionally related systems. In the test scheme, also the relative timing with respect to scheduled maintenance or overhaul outages may be defined. In many cases, several different types of tests are used in combination with a specific timing scheme in order to cover different kind of components in a system, and their different failure modes. The test strategy may define

also the procedure for additional tests of redundant equipment in a failure situation until the elimination of the root cause is verified.

Corrective maintenance

Corrective maintenance (CM) is unscheduled maintenance to repair any random failures or degradations.

Preventive maintenance

Preventive maintenance (PM) is scheduled maintenance of the equipment to retain its basic reliability performance.

Continued operation of the plant in an LCO state

When a failure has been detected in safety related equipment during power operation, the repair is undertaken while staying in the full power state at the increased risk level. This alternative is defined as a continued operation (CO) of the plant in an LCO state.

Controlled LCO shutdown of the plant

The other basic operational alternative is the LCO controlled shutdown (SD) of the plant in order to complete the repair in the zero power state.

LIST OF ABBREVIATIONS

The following list contains abbreviations used in the main text:

AOT	Allowed outage time[1]
CCF	Common cause failure
CM	Corrective maintenance[1]
CO	Continued operation[1]
DG	Diesel generator
ECCS	Emergency core cooling system
LCO	Limiting conditions for operation[1]
LOCA	Loss of coolant accident
LoRHR	Loss of residual heat removal
MCS	Minimal cut set
MSIV	Main steam isolation valve
PM	Preventive maintenance[1]
PSA	Probabilistic safety assessment
RHR	Residual heat removal
RPS	Reactor protection system
SD	Controlled shutdown of the plant[1]
SR	Surveillance requirement[2]
ST	Surveillance test[2]
STI	Surveillance test interval[2]
TS	Technical specifications[1]
TVO	Teollisuuden Voima Oy, Finland

[1] A more detailed definition is given in Section 2.

[2] Compare with 'test strategy and scheme' in Section 2.

HOW TO ORDER IAEA PUBLICATIONS

An exclusive sales agent for IAEA publications, to whom all orders and inquiries should be addressed, has been appointed for the following countries:

CANADA UNITED STATES OF AMERICA	UNIPUB, 4611-F Assembly Drive, Lanham, MD 20706-4391, USA

In the following countries IAEA publications may be purchased from the sales agents or booksellers listed or through major local booksellers. Payment can be made in local currency or with UNESCO coupons.

ARGENTINA	Comisión Nacional de Energía Atómica, Avenida del Libertador 8250, RA-1429 Buenos Aires
AUSTRALIA	Hunter Publications, 58 A Gipps Street, Collingwood, Victoria 3066
BELGIUM	Service Courrier UNESCO, 202, Avenue du Roi, B-1060 Brussels
CHILE	Comisión Chilena de Energía Nuclear, Venta de Publicaciones, Amunategui 95, Casilla 188-D, Santiago
CHINA	IAEA Publications in Chinese: China Nuclear Energy Industry Corporation, Translation Section, P.O. Box 2103, Beijing IAEA Publications other than in Chinese: China National Publications Import & Export Corporation, Deutsche Abteilung, P.O. Box 88, Beijing
FRANCE	Office International de Documentation et Librairie, 48, rue Gay-Lussac, F-75240 Paris Cedex 05
HUNGARY	Librotrade Ltd., Book Import, P.O. Box 126, H-1656 Budapest
INDIA	Oxford Book and Stationery Co., 17, Park Street, Calcutta-700 016 Oxford Book and Stationery Co., Scindia House, New Delhi-110 001
ISRAEL	YOZMOT Literature Ltd., P.O. Box 56055, IL-61560 Tel Aviv
ITALY	Libreria Scientifica Dott. Lucio di Biasio "AEIOU", Via Coronelli 6, I-20146 Milan
JAPAN	Maruzen Company, Ltd, P.O. Box 5050, 100-31 Tokyo International
PAKISTAN	Mirza Book Agency, 65, Shahrah Quaid-e-Azam, P.O. Box 729, Lahore 3
POLAND	Ars Polona, Foreign Trade Enterprise, Krakowskie Przedmieście 7, PL-00-068 Warsaw
ROMANIA	Ilexim, P.O. Box 136-137, Bucharest
RUSSIAN FEDERATION	Mezhdunarodnaya Kniga, Sovinkniga-EA, Dimitrova 39, SU-113 095 Moscow
SLOVAK REPUBLIC	Alfa, Publishers, Hurbanovo námestie 3, 815 89 Bratislava
SOUTH AFRICA	Van Schaik Bookstore (Pty) Ltd, P.O. Box 724, Pretoria 0001
SPAIN	Díaz de Santos, Lagasca 95, E-28006 Madrid Díaz de Santos, Balmes 417, E-08022 Barcelona
SWEDEN	AB Fritzes Kungl. Hovbokhandel, Fredsgatan 2, P.O. Box 16356, S-103 27 Stockholm
UNITED KINGDOM	HMSO, Publications Centre, Agency Section, 51 Nine Elms Lane, London SW8 5DR
YUGOSLAVIA	Jugoslovenska Knjiga, Terazije 27, P.O. Box 36, YU-11001 Belgrade

---

Orders from countries where sales agents have not yet been appointed and requests for information should be addressed directly to:

Division of Publications
International Atomic Energy Agency
Wagramerstrasse 5, P.O. Box 100, A-1400 Vienna, Austria