IAEA-TECDOC-599

Use of probabilistic safety assessment to evaluate nuclear power plant technical specifications

Report of a Technical Committee Meeting held in Vienna, 18–22 June 1990

IAEA

April 1991

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.

PLEASE BE AWARE THAT
ALL OF THE MISSING PAGES IN THIS DOCUMENT
WERE ORIGINALLY BLANK

USE OF PROBABILISTIC SAFETY ASSESSMENT
TO EVALUATE NUCLEAR POWER PLANT TECHNICAL SPECIFICATIONS
IAEA, VIENNA, 1991
IAEA-TECDOC-599
ISSN 1011—4289

Printed by the IAEA in Austria
April 1991

FOREWORD

In recent years a number of countries have successfully been using risk and reliability-based methods to modify limiting conditions for operation and surveillance test requirements. Some countries are using or planning to use on-line monitoring systems as a complement or alternative to the present set of operating limits and conditions. In December 1989, the IAEA convened a consultants' meeting to provide insights based on US and Nordic experience on the use of risk- and reliability-based methods to improve and justify new changes, and to scope an international plan of pilot studies to be performed under IAEA auspices. In order to promote the use of risk and reliability techniques to improve safety and operational flexibility, the IAEA has convened a Technical Committee Meeting on "The use of PSA to Evaluate NPPs Technical Specifications" in Vienna from 18 to 22 June 1990.

The meeting was attended by 37 participants from 17 countries. The twenty-three papers which have been presented in the meeting indicated that there is a worldwide recognition that risk and reliability techniques can be a useful tool to optimize technical specification requirements.

This TECDOC, prepared by the participants of the TCM, summarizes the insights from the various papers presented and the plenary discussions. It also presents, based on the knowledge available at the meeting, a regulatory perspective for the use of PSA-based Technical Specifications in Member States.

Finally, the proposal of a pilot study programme on the use of risk and reliability methods for TS optimization to be undertaken by Member States under the coordination of the IAEA is discussed.

EDITORIAL NOTE

In preparing this material for the press, staff of the International Atomic Energy Agency have mounted and paginated the original manuscripts as submitted by the authors and given some attention to the presentation.

The views expressed in the papers, the statements made and the general style adopted are the responsibility of the named authors. The views do not necessarily reflect those of the governments of the Member States or organizations under whose auspices the manuscripts were produced.

The use in this book 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 specific companies or of their products or brand names does not imply any endorsement or recommendation on the part of the IAEA.

Authors are themselves responsible for obtaining the necessary permission to reproduce copyright material from other sources.

This text was compiled before the unification of Germany in October 1990. Therefore the names German Democratic Republic and Federal Republic of Germany have been retained.

CONTENTS

1. INTRODUCTION

The Technical Specifications (TS) define the limits and conditions for safe operation of a nuclear power plant. These limits and conditions are mostly based on deterministic analyses and engineering judgment. Experience has (however) indicated operational and safety concerns with some of these requirements. Some elements of these requirements may be considered unnecessary or may not be conducive to the safety of the plant. Requirements are at times unnecessarily restrictive and many times become burdensome to the extent that they may direct attention from safe plant operation. In recent years a number of countries have successfully been using risk and reliability based methods to modify limiting conditions for operation and surveillance test requirements. Some countries are using or planning to use on-line monitoring systems as a complement or alternative to the present set of operating limits and conditions.

In September 1987, OECD/CSNI/UNIPEDE and CSN organized in Madrid an International Conference on Improving Technical Specifications for Nuclear Power Plants. The Conference was well-attended, showing the interest in seeking modifications and enhanced understanding to TS and also generated interest in applying risk and reliability based methods for TS modifications. In December 1989 the IAEA convened a consultants meeting to provide insights based on US and Nordic experience on the use of risk- and reliability-based methods to improve TS and justify new changes, and to scope an international plan of pilot studies to be performed under IAEA auspices (see Annex I).

In order to promote the use of risk and reliability techniques to improve safety and operational flexibility, the IAEA has convened a Technical Committee Meeting on "the use of PSA to Evaluate NPPs Technical Specifications".

2. PURPOSE OF THE MEETING

The purpose of the meeting was to compile, review and exchange experience on risk- and reliability-based improvements to TS. In addition, participants discussed a plan for pilot studies on risk- and reliability-based evaluation and modification of Technical Specifications to be undertaken under IAEA auspices. Thus, the technical committee meeting encouraged participation from member countries in these pilot programs. The insights from the pilot program will provide the technical basis for the preparation of an IAEA safety series document to provide guidance on the application of PSA to TS evaluations.

This TECDOC, prepared by the participants of the TCM, summarizes the insights from the various papers presented and the plenary discussions. It also presents, based on the knowledge available at the meeting, a regulatory perspective for the use of PSA-based Technical Specifications in Member States.

3. INSIGHTS FROM THE TECHNICAL PRESENTATIONS

Papers were distributed according to the subject area addressed among three technical sessions, namely:

Session 1: Programmes and methodology
Session 2: Computer applications/software development and decision-aiding techniques
Session 3: Case studies and applications

Insights from the papers presented and from the technical discussions are summarized next. All papers submitted with full text are included in Annex II.

3.1. Session 1: Programmes and Methodology

Eleven papers were presented and discussed in this session.

Optimization of Technical Specifications by Use of Probabilistic Methods, A Nordic Perspective
(Presented by K. Laakso, Finland)

Developments in probabilistic safety assessment have provided a new tool to analyze, present and compare risk effects of proposed modifications of rules in TS. For example, temporary high risk situations have been identified in advance, so that they can be prevented or controlled. Also, excessively stringent but not safety-significant requirements can be modified in order to improve operational flexibility of the plant.

The main areas covered in the Nordic project were alternative operational decisions in failure situations during power operation, preventive maintenance in one subsystem at a time in 4-redundant standby safety systems during power operation, and effectiveness of surveillance test procedures and schemes of standby equipment. The project results provide a framework and reference for utilities and authorities to prepare similar risk and reliability evaluations for analysis and justification of permanent TS modifications needed for other components, systems and plants.

In the long run, one should try to attain living PSA by analyzing equipment outages and plant incidents to indicate improvement needs at the plant, in the technical specifications and in the PSA. Additionally, the presentation and use of PSA results in supporting technical and operational decisions must still be improved.

In the discussions after the presentation it was noticed that representatives of Finnish and Swedish utilities and authorities have worked in this research project in order to facilitate the practical applicability and the use of the results for TS modifications.

EPRI Perspectives on the Use of Risk-Based Technical Specifications in Controlling Plant Operations
(Presented by J.P. Sursock and D. True, USA)

The following points were made in the presentation and in the discussion which followed:

A number of technical and institutional obstacles exist which inhibit the wholesale adoption of a real-time risk monitor for NPPs in the USA.

EPRI has begun a project aimed at:

- developing "flexspecs" which are pre-defined, prioritized options available to the plant operator to avoid entering an LCO or extend the duration of AOT, and;
- developing the concept on an Integrated Risk Advisor (IRA) which will serve as a computerized tool box to assist operators in maintaining compliance with TS. The IRA is not a risk calculator like the ESSM (see session 2), but rather contains pre-determined configuration controls developed on a risk basis.

The EPRI project is scheduled to complete the conceptual development of the IRA this summer and complete the development and testing of an IRA in a plant by 1992.

Application of PSA to Operational Safety Decisions in Hungary
(Presented by Mr. E. Hollo, Hungary)

PSA is a good tool for TS evaluation, but detailed time-dependent analysis is needed. The optimum test interval determined from PSA studies is normally shorter than the present practice. Present TS criteria are too conservative, AOT time limitations can be relaxed.

Results are used in PAKS NPP as background information for operational decisions. Modification of TS is under discussion. Up to now studies, in Hungary, were performed on "safety function level". The analyses on modification of AOT and test frequency on "unit level", i.e. to core damage frequency, should be carried out. Common cause failures should be considered for realistic quantification in the analysis.

Present TS prescription for AOT described in the paper is too rigorous considering 3x100% redundancy for safety systems. Increasing the AOT for a single failure instead of unit shut-down should be considered.

The Use of PSA to Evaluate Technical Specifications - a Design Viewpoint
(Presented by J.M. Hopwood, Canada)

The objective of this paper was to complement the primarily operations-oriented discussions at the meeting, with a presentation of the designer's viewpoint on the use of PSA, based on the current CANDU 3 design program.

The CANDU 3 design and PSA program have now evolved to the point where Operating Policies and Procedures (equivalent to Technical Specifications) can be assembled.

Since most changes of plant configuration (i.e. equipment removal from service) occur during outages, it is important to incorporate a comprehensive shutdown assessment into the PSA at the design stage, and consider both shutdown and startup also. This can then be used to pre-define a matrix of available maintenance configurations at the design stage, minimizing later conflicts with operational goals.

The possibility was noted of undue regulatory backfitting requirements, when probabilistic risk requirements are created but deterministic requirements are still retained. This should be addressed by strong communication between licensee and regulator.

The acceptance criterion for the CANDU 3 PSA was noted. Since the standard design is site independent, the criterion is based on core damage. The design requirement is that all individual event sequences should have severe core damage frequency $<10^{-6}$/year, and an internal target that severe core damage sum frequency $<10^{-5}$/year. So far, the PSA results indicate that this target will be met.

It was noted that both event trees and event sequence diagrams are to be used in the CANDU 3 PSA. Event sequence diagrams are event trees with explicit chronological data including elapsed time before system demands which clarify the operator's role in accident mitigation.

The Status of PSC and Technical Specifications Improvements Based on Probabilistic Methodology
(Presented by S. Volkovitskij, USSR)

The regulatory body in the USSR (SCSSINP) recognizes in principle the use of probabilistic methodology as a supplementary tool to the deterministic approach for NPP safety assessment and for evaluation of technical specifications. Probabilistic indicator goals in the USSR regulations are based on large radioactivity releases, severe core damage, and take into account the destruction of the pressure vessel as a design basis initiating event. At present investigations are under way on establishing similar indicators on functional-system level. The problem is to develop a consistent and sufficient system of indicators and procedures for the reliable assessment of such indicators.

In order to streamline and adjust the whole PSA system and to promote nuclear safety, SCSSINP recognized a necessity to develop a series of guidelines for conducting PSA. This work is now in progress.

The Soviet Union regulatory body considers all attempts to implement methods of reliability and risk analysis and improvement of technical specifications of NPPs to be useful and promotes these activities in the research and design organizations and by NPP personnel. But, as in the past, the regulatory body will assume regulatory decisions in the near future mainly on a deterministic basis.

As an example of the use of probabilistic methodology for assessment of TS two studies were realized by R&D organizations last year. One of them was devoted to validation of repair and maintenance schedules of Kola NPP. The second one is a series of works for study probabilistic indicators of reactor primary circuit components failure.

Allowable outage times (AOTs) and Surveillance Test Intervals (STIs) Reevaluation by PRA Procedures
(Presented by S. Martorell, Spain)

Late in 1987 the Spanish Council for Nuclear Safety (CSN) started a Technical Specification Analysis Program called "APET". This program studied existing methodologies and their scientific basis that are related to probabilistic analysis of TS. The first stage was finished in early 1989, the second phase consists of applying the selected methodology. Some results of this program were presented here.

This paper does not aim to provide a guide for specific AOT's and STI's revision program, it rather tries to explain a process to evaluate the risk associated with these requirements. The reevaluation process by PSA procedures proposed consists of three sequential steps:

First of all, a qualitative analysis is developed, it consists of defining and modelling the unavailability for those systems involved in the revision process. The final result must be unavailability data, fault trees and their corresponding minimal cut sets.

In the second step, a quantitative analysis can be developed using time-independent or time-dependent models. The time-independent one allows a first estimation for the system average unavailability or risk, due to AOT and STI requirements. This analysis is completed with data uncertainty studies and measures of risk importance analysis. With the time-dependent analysis we obtain a second estimation for the system average unavailability and also the time-dependent plant vulnerability. The Frantic-III code has been used to accomplish the time-dependent evaluation.

Finally, because risk evaluations related to AOT and STI requirements can vary depending on assumptions, models and data used, it is deemed necessary to carry out sensitivity studies in order to verify conclusions derived from all previous analyses. These studies can also help to limit errors included by models and reliability data. In particular, we focus our attention on data uncertainties and therefore additional calculations were performed to investigate the sensitivity to the input used. This study showed that data bases and recollection for component reliability data have to be carefully obtained from operational experience.

Regulatory Aspects of the use of PSA to Evaluate Technical Specifications
(Presented by J. Rumpf, GDR)

A deterministic approach is used for licensing of NPP. In addition, a level 1 PSA for each unit either in operation or under construction is required and is under way. A reevaluation is planned every ten years (including PSA level 1).

Research programmes concentrate on the use of PSA for TS and living PSA application to be used by the operators.

Insights from research activities include:
- total PSA based TS revision is not necessary
- TS evaluation has to be based on at least a level 1 PSA (dependencies are important)
- plant-specific data as well as "realistic" accident sequence modelling have to be used
- temporary exemptions from TS require more sophisticated methods (e.g. living PSA)
- up to now no probabilistic safety criteria (PSC) have been established
- absolute PSC are not considered possible
- uncertainties of physical models should be discussed.

The regulatory body promotes activities in the field of R&D to enable operating organizations to perform PSA appropriately. Operators have different positions. They should be required to use PSA as a communication tool.

Feasibility Assessment of a Risk-Based Approach to Technical Specifications
(Presented by B. Atefi, USA)

An assessment was made with regards to the potential benefits and feasibility of a risk-based approach to TS. This assessment was based on analytical and some actual plant operational analysis. The preliminary conclusion is that risk-based approaches to TS have the potential to better optimize the current deterministic requirements. Such optimization can improve plant safety and availability by providing the plant operational staff with additional flexibility to deal with TS. Furthermore, detailed analysis of the technical and institutional issues associated with these approaches indicates that at this time there are no major obstacles to initiate a pilot study to further analyze the practical issues associated with implementation of such an approach.

Approaches for Ascertainment of Allowable Outage Times (AOTs)
(Presented by K. Theiss, FRG)

Based on the requirements of German Nuclear Safety Criteria of NPP the KTA-report 1407 guideline was developed to present methods concerning the ascertainment of AOTs in NPP.

Both probabilistic methods so-called Reference-method and Risk-method ascertain AOT on a system specified level. The methodological approaches take into account that the unavailability level of safety equipment will not exceed a defined boundary value at any time of NPP operation.

The deterministic approach introduced in the KTA-report is based on two input parameters both structured in a matrix. The sum of the input parameters is assigned to an interval of AOT. This is done by taking into account the operating experience.

The probabilistic safety assessments performed nowadays in all NPP can be considered as a suitable foundation for continuation and further development of the methodological approaches.

VVER Plant Probabilistic Safety Assessment
(Presented by V.A. Volkov and E.P. Larin, USSR)

This paper addressed the methods of probabilistic safety assessment to be used for the evaluation of VVER-1000 reactors in operation. Probabilistic analysis is supposed to be used to optimize operational documentation, to assess weaknesses and enhance safety and efficiency of the operating plants. In this paper, the PSA performance programme adopted in VNIIAES* is described.

The following steps for PSA of operating NPPs are being carried out:

- preparation of request for proposal to classify events and faults,
- collection of plant operational data including events and faults
- event analysis,
- development of dynamic calculation codes,
- analysis of practical solutions affecting safety and stability using probabilistic methods.

To complete the work a considerable effort and expertise is still required.

Uncertainty Analysis in the Process of Reliability Estimation
(Presented by J. Holy, Czechoslovakia)

A history of uncertainty analysis at the Nuclear Research Institute was presented. The framework for those studies was described including the fault tree method, probability characteristics of primary events with lognormal distributed random variables, error factors quantifying the spread of these variables, and two numerical methods to evaluate uncertainty propagation using fault trees and the computer codes SAMPLE and COSMOS.

---

* VNIIAES: All-Union Research Institute for Nuclear Power Plant Operations (USSR).

Properties of error factor and its time-dependent behaviour for a typical medium-size safety system considering inspection and repair, human errors, and discontinuous unavailability on demand as a function of time, ("as good as new" approach) were studied.

A new method to estimate the error factor of time-dependent unavailability of components under inspection and repair including human factors was mentioned.

Various arguments against PSA studies often concentrate on the credibility of the results connected with rare input data. An intuitive approach leads to the impression that: "The larger and more complicated the fault tree, the more uncertain is the resulting system probability characteristic". The results of the study described in this paper do not confirm this statement, instead they support the opposite insight, i.e. uncertainty is reduced at the system level.

General Comments

Mr. A. Wild (Canada) noted four important points not always properly highlighted in PSAs.

1) Boundaries of the analyzed systems should be properly defined and this definition must correspond to that used in design and operation.
2) Probabilistic Safety Analysis should be embedded within the engineering process which starts at an early design stage and continues throughout the life of the system.
3) Computer tools should enhance the capabilities of analysts and operators, not replace their thinking.
4) Fault trees are important as a communication tool. Various specialists (designers, thermohydraulicists, operators..) may have different sets of priorities and often contradictory ideas on what constitutes proper practices. Fault trees can clarify "what we are talking about".

Conclusions, remarks and outlook

Technical specifications have been based on deterministic analyses prepared for the Final Safety Analysis Report and on engineering judgment. Developments in PSA and reliability analysis provide a new tool to calculate the risk effects of alternative requirements in TS. It should be noticed that approximately 70-80% of all limits and conditions in technical specifications are, however, of such kind that they are not suitable for probabilistic evaluation. PSA is, however, a valuable tool in the analysis of specific technical specification problems in plant operation.

In order to identify whether an extensive probabilistic evaluation of a TS problem is safety- or cost-justified, a pre-study including definition of boundary conditions and prerequisites is recommended.

The task of TS optimization can be defined as:

- optimal use of excessive safety margin available to provide operational flexibility and,
- solving of individual TS problems, normally by minimizing temporary risk increases.

It was noticed in the discussions that the plant level influences of the test configurations can be determined by help of an existing PSA, but the effectiveness of standby equipment tests has to be studied in more detail at system and component level based on the analysis of operating experience. The methods and model development needs in the plant shutdown risk analyses go beyond the scope of usual PSAs, although an existing PSA helps the study. Temporary risk increments, caused by unavailability of standby equipment due to preventive maintenance periods during power operation can be evaluated by a "simpler" adaptation of an existing PSA plant model.

Further efforts are required to (1) improve methods and criteria which would allow a broader use of PSA for technical specification evaluation and, (2) use PSA to support risk monitoring and decision making during plant operation needs.

3.2. Session 2: Computer Applications/Software Development and Decision Aiding Techniques

This session covered two different aspects of computer application and software development on decision aiding techniques. The first described an on-line "living" PSA model technique and consisted of a presentation and demonstration of the ESSM facility installed at Heysham B Power Station in the UK. The second aspect covered work aimed at developing the methods for safety system reliability estimations particularly of TS evaluations. This section consisted of four presentations from the USSR and Poland.

The use of Probabilistic Safety Analysis Methods for Planning the Maintenance and Testing Unavailabilities of Essential Plant at Heysham 2 AGR Power Station

(Presented by B.E. Horne, UK)

The paper described the background of the development of the present ESSM installation at Heysham B Power Station and summarized the benefits that have resulted from its use over the past 18 months. In this the concept of "living PSA model" had been developed from that of being modifiable to accommodate design changes as they occur in a fairly relaxed timescale, to that of being modifiable to model plant unavailabilities and systems reconfigurations as they occur on an interactive timescale. Although the initial development of this facility had been as an interactive PSA tool it included, in addition to the level 1 probabilistic model, a set of deterministic rules, the so-called "skyline rules" such as single failure criteria, hazards models, etc. It was emphasized that the development of customized PSA models and the special software techniques were only a part of several

issues that had to be addressed before the facility could be accepted by the Regulatory Authority for use in place of the conventional TS. Other issues were:

- operator interfaces had to be "operator comfortable" and verifiable (e.g. ESSM is menu-driven)
- software security had to be ensured at different levels (e.g. program structure)
- code verification had to be comprehensively demonstrated
- operational procedures had to be devised by Station for using the ESSM in a controlled, realistic and practical manner
- software and hardware failures had to be accommodatable, i.e. reversionary procedures provided, and assurances of non-faulty operation provided
- updating procedures had to be comprehensive, controlled and verifiable
- different, particular computer installations had to be accommodated

Although the ESSM was developed for an AGR application, it was suggested that the experience gained could be profitably applied to other reactor types.

ESSM Demonstration

The demonstration of the ESSM exactly replicated the facilities provided at Heysham B Power Station. The facilities demonstrated were:

(a) initialization of the living PSA model
  - for plant unavailabilities
  - for plant reconfigurations.
(b) deterministic assessment
(c) probabilistic assessment
(d) plant status
(e) plant replacement advice
(f) predictive planning
(g) post-event analysis, i.e. cut-set analysis, etc.

From the discussion and questions that followed, the following points emerged:

1. The ESSM is an aid to judgment for the operator, not a decision tool.
2. The deterministic "skyline" assessment used the same system fault trees as the PSA.
3. The probabilistic assessment was carried out using one large consolidated fault tree with some 48 top events.
4. Modifications to the design fault trees were required for them to be suitable for use as an operator aid, particularly for maintenance and testing planning.

5. The current size of fault tree model was approximately 7500 gates and 500 super components.
6. The main uses were for the planning of plant unavailabilities for maintenance in a "risk management" role, and less frequent uses were by the operator in monitoring risk and operating status of the plant.

The future perspectives suggested were that the ESSM facility would be developed further in the UK to remove some of the pessimisms in using a design PSA in a "living model"; use the information derived in the computations more comprehensively, (e.g. generate importances) rank dominant components, and provide a risk control facility for predictive planning.

Methods of Evaluation and Service Reliability of Unique Devices and Plants
(Presented by I. Fedik, USSR)

The main insights from the paper presented were a development of a methodological approach and an effective algorithm for processing of different experimental data for reliability estimation of the nuclear reactor and its components at the stage of design. This included data having different levels of detail.

The methods described allow the systematic prediction error to be eliminated in practice and allowed systematic errors to be decreased. The present approach has been used for three types of nuclear reactors and has given good results.

The problem of "translation" of qualitative information into a quantitative one and its formatting is a subject for further research and investigation.

Features of Method and Program Product used for Probabilistic Safety Analysis of Nuclear Plants
(Presented by A.N. Roumiantsev, USSR)

The paper presented a method of PSA based on the formalized representation of a probabilistic model of an NPP process flowsheet in the form of the multi-component systems and elements having branched linkages, including loop (feedback structures like networks), and considered as abstract discrete automations of the "input-output" type. If the probabilistic models investigated did not contain any loop linkages of events, this method reverted to the traditional methodology of "fault trees".

An analysis of the probabilistic characteristics of failure events is complemented with the analysis of the confidence levels of the results obtained by using the entropic methods of error handling. Probabilistic characteristics of the failure events are described in terms of functional dependencies of time. All initial data used for determination of probabilities are accompanied by error intervals.

The methods described were implemented in the development of the BAMC software product suitable for use on IBM-line mainframes and PCs.

Some results concerning safety feature of various designs of NPP with VVER-1000 reactors were presented. Some data have been presented in order to demonstrate an applicability of PSA approach for an analysis of the Chernobyl accident.

The importance of dealing with ranges of error for initial probabilistic data has been stressed. Attention was drawn to taking into account a need to define risk values with direct use of error handling technique, as an example, which is based on entropic approach. The Chernobyl accident may be used for verification of the probabilistic arguments on NPP safety including needs to deal with probabilistic feedback structures.

PSA approach, technique, software, initial data collection and approximation - all of them are under development and improvement. There is no "frozen" status of art in that field.

Two basic features of methods reported are of significant interest. They are entropic error handling technique without Monte Carlo and feedback structure of events especially for modelling of human error and "external" events.

Implementation of risk values calculated with direct accounting of errors in initial data instead of mean values of probabilities is of greater importance in the case of large (5 to 10 times) error intervals of initial failure data. Under such conditions a mean value of failure probability brings less information than a value of upper boundary of the confidence interval.

It was concluded that great care is required in dealing with low probability events and in particular where teams of operators are involved. Such teams can have different objectives. Great care was also required where multiple events are not considered in instructions provided to the operators. It could have been demonstrated that the probability of the Chernobyl accident was estimated as in the range 10^{-8} to 10^{-12} per RY, i.e. beyond the range of those sequences that would be normally considered. In practice, due to dependencies between operator actions, the practical estimate would be (10^{-2} to 10^{-3}) X 100 reactor years, (i.e. about one).

Development of Basic Software for PSA-Based Technical Specification Evaluations
(Presented by M. Borysiewicz, Poland)

General purpose PSA level 1 computer programmes need to be extended to provide an efficient tool for evaluation of PSA-based Technical Specifications. The effort should be focused on:

(i) development of a software environment (integrated package of codes and structured data bases) that facilitate computing various risk measures as functions of AOT's and STI's parameters, with minimum re-analysis of minimum cut sets that may already exist from PSA studies,
(ii) implementation of detailed component unavailability models and MCS probability calculation algorithms that account for three individual segments of component unavailability cycle (i.e. test, repair and between tests) and different testing and maintenance schemes of plant items represented by MCS elements.

The general conclusion from the work to date is that the use of selected PSA micro-computer codes and data bases integrated with mainframe versions of codes with capabilities of SETS, SEP and SOCRATES may ensure achievement of above goals (i) and (ii),

Generally, complexity of modelling and numerical difficulties limit the use of the Markovian process in safety and reliability analyses to relatively small systems. The areas of TS evaluations, where this approach improves over the current FT techniques, should be better identified.

NPP Channel Structure Safety System Reliability Analysis: Methods and Computer Code SHARM-2
(Presented by G. Loskutov, USSR)

The paper summarized the special investigations that had been performed on methods of reliability assessment of safety systems which were structured in channels. The methods were based on fault tree and minimal cut-set evaluation approach. Insights from the presentation were:

- the development of methods for the reliability analysis of a safety system structured in channels based on the different test and maintenance strategies has been performed,
- the development of SHARM-2 code package for mainframe computers has been performed,
- the comparison between two different code packages (SHARM-2 and PSAPACK) has been performed.

The conclusions drawn from the paper were that these methods allow the optimization of maintenance and test strategies of the systems on the NPP under operation, and therefore increase the safety of the NPP without changes in system structures.

3.3. Session 3: Case Studies and Applications

The degree that probabilistic and deterministic approaches are used in the design and operation of NPPs varies considerably. However, one trend was clearly identified. Utilities with long operating experience make use of their own plant experience on the system and component level in a pragmatic, systematic way. PSA tools are used as

supplementary tools at the plant and at the system level. In some instances PSAs are used to justify good practices and to avoid big plant modifications. In other instances PSA was successfully used for operating and maintenance improvements. For new plants PSA has been successfully used as a design tool taking into account operating and maintenance practices.

A consensus seems to be that a strong technical support for all plant activities related to operation and maintenance is necessary. Maintenance and testing on essential safety equipment should be defined such as to least impact the safety margins at a given plant configuration. Planning maintenance AOT and testing STI is a major issue.

The proper plant design with regard to redundancy on a safety based cost benefit analysis seems to be feasible using PSA techniques when maintenance and operation practices are included.

Collection of plant specific failure rates and unavailabilities on systems shall be a continuous effort during nuclear power operation. The comparison of predicted values in the design phase with actual values achieved gives deep insight into failure mechanism. The most comprehensive date source is the operating plant.

The use of Probabilistic Safety Evaluation to Obtain Plant Operational Improvement
(Presented by E. Mink, Belgium)

The presentation has given good examples on how plant operating flexibility was improved by changing the AOT in the TS to more realistic figures.

Reallocation of safety system capabilities in time periods when, on a risk basis, less safety systems are necessary, is a good practice. This gives the operator margins to plan maintenance and testing. Relaxations are realized in areas where too stringent restrictions existed prior to performing a PSA. Minimizing testing increases availability.

The Development of Technical Specification Surveillance Requirements for Sizewell "B" Power Station
(Presented by W.B. Sargeant, UK)

The paper describes the adaptation of Standard Technical Specifications to the licensing requirements in the UK for the first PWR to be build by Nuclear Electric (formerly a part of Central Electricity Generating Board). The application of probabilistic methods in the design and safety analysis is described, and the decisions to be taken on the scope, structure and interdependence of the technical specifications for Sizewell "B" Power Station are assessed.

Licensing commitments have been made to the Nuclear Installations Inspectorate (NII), the regulatory authority, on the use of PSA at levels 1, 2 and 3, and on the provision of an operator aid to assist compliance with the Technical Specifications.

Provisions have been made in the Station Instrumentation system to structure the on-line data base to be available for input to a system to monitor compliance with Technical Specifications. The detail of the computerized aid to the operating staff have yet to be decided, but the use of PSA in the development of Technical Specifications has been agreed. The discussions on the paper concerned the allocation of faults within the initiating fault schedule and allocation of frequencies. The definition of uncontrolled release of radioactivity was reported for safety assessment purposes as applying to faults/fault sequences resulting in releases greater than 1 ERL.

Control of Power Dependant Safety Margins
(Presented by R.E. Häusermann, Switzerland)

The flow path of the information of plant data is very important and the correct information must at all times be available at each level of decision. The status of the safety systems in terms of availability is the key parameter. Loss of safety in terms of availability must be evaluated and actions taken to prevent unacceptable situations. The T.S. is a filter in this process.

A complex system must be broken down into working elements such as procedures and data sets to suit users' needs. Flow diagrams support this activity. Feedback from operational experience provides important motivation for constant improvements.

The computer is a tool not a substitute for human knowledge. Close coordination between plant operators and maintenance personnel is a must.

Plant status should be properly assessed for all possible system configurations and plant risk controlled, based on the available safety systems. The tool to allow this is still open, however, it must be developed from the well established practices. PSA methods will support the work.

Risk-Based Evaluation of Technical Specifications for a Decay Heat Removal System of an LMFBR Plant
(Presented by K. Hioki, Japan)

The AOTs should be determined based on the concept of risk which comes not only from the outage but also from the shutdown state.

The number of AOT hours and test intervals differ depending on the design. It cannot be calculated on-line in a real-time mode. Thus, it is necessary to calculate them in

advance. The method to estimate the total risk is not yet established. If the multiple failures, common cause failures and human factors are to be taken into consideration, the problem is more complicated.

The risk curve that is caused by the reactor shutdown must be calculated more precisely in order to obtain realistic answers.

Use of PSA to Evaluate Operating Strategy Compliance with Operating Policies and Principles Requirements
(Presented by P.N. Lawrence, Canada)

In Canada, the technical specifications are called Operating Policies and Principles (OP&P). The OP&Ps are largely deterministic being based on the plant's safety analysis and engineering judgment.

The OP&Ps concentrate on safety principles rather than detailed operating rules and procedures. In this way, the OP&Ps have been maintained at a manageable size. All operational procedures and programs, including the safety monitoring programs, must comply with the principles contained in the OP&Ps.

We use system-based unavailability models developed from a PSA to demonstrate compliance with the safety principles in the OP&Ps. We do not have rigid rules for the application of the results of the PSA because we do not believe that we can predict all possible plant configurations.

The OP&Ps, and the supporting operational programs, have evolved over the years. Only when we are confident with new methods, or when plant data suggests deficiencies with current programs, will we make significant changes.

We will continue to investigate further application of PSAs to operational decision making. In the near future, this will most likely take the form of ensuring that the OP&Ps are focused on the major contributors to public risk. It is unlikely that a PSA will be used to monitor and control risk on a continuous basis.

Currently, system-based unavailability models are used to control test frequencies, control configuration and monitor performance of safety-related systems.

Operational data is collected at the component level and used to analyze performance from the component level through to system and function levels. Component and system performance are regularly compared to predictions in the unavailability models; where significant differences are found corrective actions are taken.

Open Issues

How can we further incorporate the insights of PSA studies into our operational programs?

How significant are the long-term benefits of applying PSA techniques likely to be?

Insights from Discussions

In the application of the OP&Ps, the PSA is one of several tools available as an aid to decision making. In the near future, it is unlikely that we will use the PSA on-line to "make" operational decisions.

We believe that the majority of operational decisions can be taken with the aid of system-based unavailability models. We appreciate that this is not always the best approach, e.g. complex changes to support systems, however, we still have access to insights gained from the PSA in such circumstances.

Operational Decision Alternatives in Failure Situations of Standby Safety Systems
(Presented by T. Mankamo, Finland)

The paper describes a method to investigate the AOT issues based on a systematic approach. The risks of continued operation and shutdown alternative are compared in regard to which one is the safer alternative.

The methods have been applied at TVO plant (BWR) to failure situations of the Residual Heat Removal systems. Based on the results, appropriate modifications to the technical specifications and operating instructions are under way. The repair time limit of three days, currently allowed only in double failure situations, will be extended to failure situations of three or all four redundant trains in the Residual Heat Removal systems considered.

The development of the method has been done closely coupled with the TVO case study.

The technical specification modification is under consideration in Finnish regulatory body (STUK).

The method is generally applicable to the analysis of operational alternatives in case of standby system failure. However, the analysis results are highly dependent on plant specific characteristics.

Evaluation of VVER 440 Technical Specifications using PSA
(Presented by Z. Kovács Czechoslovakia)

In the paper two case examples are chosen to demonstrate revision of VVER 440 technical specifications regarding surveillance frequencies and out-of-service times.

Two V-213 type units have the same Reactor Protection Systems (RPS), but different test invervals for measuring channels, namely:

a) each channel has to be demonstrated operable once each month;

b) each channel has to be demonstrated operable once every two months.

The results show us that the unavailability of the RPS up to three months test interval of channels is constant. The increase in unavailability occurs after three months. Therefore, the two month test interval is more convenient. The suggestion was given to change the test interval to two months.

In case of the second case example, AOT risk measures at the system level were calculated for the components of High Pressure Core Cooling System (V230 type reactor). Some MOVs were found to have high contribution to the system unavailability. The current TS do not allow their maintenance during power operation. The risk measure for MOV was calculated and the conclusion is to allow their maintenance with AOT=72 h (the average repair time is 32 h).

In the near future the TS risk contribution for the systems will be evaluated at the higher levels: accident sequence frequency and core melt frequency.

For the case presented for the RPS, the Fussel-Vesely importance values were computed using the TREE MASTER computer code.

4. REGULATORY PERSPECTIVE FOR THE USE OF PSA-BASED TECHNICAL SPECIFICATIONS

Representatives of each one of the countries attending the TCM attempted to characterize their regulatory position with respect to risk-based Technical Specifications. In some cases, a representative of the regulatory authority was present. In most cases, however, participants were not from the regulatory authority. Therefore, these descriptions should not be taken as official positions, but they do give a rough idea of the variation in the attitudes of the regulatory bodies in various countries regarding the use of PSA in the area of Technical Specifications.

BELGIUM

For the most recent operating plants in Belgium deterministic Technical Specifications are used. The use of PSA as part of this effort is still under consideration. For emergency systems designed against external events, the determination of AOTs is supported by probabilistic calculations. For older plants, an extensive reevaluation of Technical Specifications is in progress. The Belgium licensing authority (VINCOTTE) is conducting a systematic program collecting unavailability data for main safety systems. Based on the results of this program, the maintenance strategies are discussed with the utilities.

CANADA

In Canada, the technical specifications are called Operating Policies and Principles (OP&P). The OP&Ps are largely deterministic being based on the plant's safety analysis and engineering judgment.

The OP&Ps are written by the licensee and approved by the regulator, the Atomic Energy Control Board of Canada (AECB). The OP&Ps are explicitly mentioned in a station's license and all revisions must be approved by the AECB.

The OP&Ps focus on safety principles.
It is the responsibility of the licensee to develop programs which demonstrate compliance with the safety principles. The regulator regularly reviews the scope and application of the programs, and can ask for revisions or clarification.

In the near future, PSAs may be used to ensure that the deterministically based OP&Ps are focused on the major contributors to public risk. It is unlikely that a PSA will be used to monitor and control risk on a continuous basis. However, system based unavailability models derived from PSA studies are currently being used to monitor and control safety-related system performance.

CZECHOSLOVAKIA

The regulatory body has contracted a PSA study of the Dukovany Unit 1 nuclear power plant. The objective of this work is to calculate the core melt frequency and to make suggestions, if necessary, for maintaining the core melt frequency below 10^{-5}/year. Other activities of the regulatory body in this area include reliability analyses to support changes to the Technical Specifications for safety systems of the V230 and V213 type reactors and reliability analyses for research reactors.

FINLAND

The Finnish Centre for Radiation and Nuclear Safety (STUK) supports the development and use of risk and reliability assessment for nuclear power plant safety evaluation and development. The regulatory authority has a three person (full-time) group involved in PSA and reliability assessment, including review of the PSAs performed by the utilities. STUK requires a mini-PSA and reviews it prior to the issuance of a building permit for any new nuclear power plant. A level 1 PSA must be prepared by the utility/vendor and accepted by STUK prior to the operating permit (fuel loading) of new plants. Probabilistic safety goals at the safety function level are applied for plants to be designed. The regulatory authority considers probabilistic safety analyses, as applicable, as part of the justification material, in the review and acceptance process of modifications of technical specifications. STUK participates in the Nordic SIK-1 research project (1990-93) on safety evaluation (living PSA and safety indicators), which is

coordinated by the Technical Research Centre of Finland. STUK is presently developing a computerized tool (STUKPSA) to be used as a conversation tool between authority and utilities in safety-related matters.

GERMAN DEMOCRATIC REPUBLIC

The GDR regulatory authority has initiated a research program to investigate the feasibility of basing Technical Specifications on PSA. No final results are currently available.

Licensing of nuclear power plants is based on a deterministic approach. In addition, a level 1 PSA is required. No general requirement exists for the reevaluation of Technical Specifications; they are considered well established and verified. Modifications to TS are done using a deterministic approach. In addition, a PSA analysis is required, if reasonable.

No quantitative probabilistic safety criteria are established by the GDR regulatory authority. Qualitative criteria based on reliability analyses of systems are used (e.g., staggered testing).

GERMANY, FEDERAL REPUBLIC OF

In the FRG, Licensing Procedures of NPP Technical Specifications were laid down generally on the basis of deterministic approaches. In this context probabilistic methods have been used supplementary to ascertain allowable outage times of modern NPPs. At the present time there is no further development of these methods.

In the near future an investigation project which is supported by the German Regulatory Authority BMU will be finished. In the so-called Safety- and Information System, SAIS, existing reliability programs are implemented. The SAIS is going to work on the level of operator-decision support both, to optimize changes in design, strategy of testing and maintenance procedures, and to inform directly about reliability of current plant conditions. Development of the SAIS is performed in co-operation with the NPP Brokdorf (BWR) as a reference-plant.

HUNGARY

Regulation practice in general is based on Hungarian and Soviet rules. Present PSA objectives of the regulatory body are the evaluation of design targets to demonstrate compliance with licensing requirements and the selection of the most crucial event sequences to be included in the emergency operating procedures. The use of PSA for modification of requirements in the present mainly related the AOTs or STIs, is another objective of the regulatory body.

JAPAN

In Japanese safety regulations, operational limits and limiting conditions for operations are specified, however, they are only basic requirements and based on the deterministic methods. Each utility applies detailed procedures voluntarily.

The probabilistic approach is not officially adopted in Japan to determine Technical Specifications requirements. Probabilistic methods are, however, used supplementarily to evaluate the validity of Technical Specifications. The trend in Japan is to utilize probabilistic methods more in the future. Some studies are being made on the applicability of probabilistic methods to the establishment of Technical Specifications.

MEXICO

A risk and reliability based evaluation program, applied to Technical Specifications is planned to be carried out by the Mexican Regulatory Commission. This is intended to improve the decision-making process for unforeseen deviations on limiting conditions for operation, as well as utility proposals for modification of surveillance test intervals and allowed outage times. In order to implement this program, the Laguna Verde PSA is at present under review by the Regulatory Commission.

NETHERLANDS

The Dutch government has asked the utilities to start a program to improve the existing Technical Specifications. In this program, the developments in other countries, especially the Technical Specifications Improvement Program in the United States has to be taken into account. The improved TS for the Boossele PWR and Dodewaard BWR must be completed by 1991.

POLAND

Technical Specifications for the first nuclear power plant ZARNOWIEC, now under construction (as included in PSAR) have been developed by the plant designer. They are based mostly on deterministic criteria and engineering judgment. The final version of operating limits and conditions will be prepared by the utility and presented for the approval of the regulatory authorities (National Inspectorate for Radiation and Nuclear Safety) as part of the safety documentation required for the operating license.

PSA is being implemented in Poland for supporting safety decisions in the design and construction of ZARNOWIEC. PSA is also recognized by the regulatory authorities as an important tool in the licensing process.

PSA experience gained so far and the recognized potential of this methodology in enhancing nuclear power plant safety encourages the use of the risk-based approach for

supporting safety decisions related to NPP operation. Effort on the development of the most appropriate methods has been initiated in several research organizations and by the regulatory authorities. Regulatory authorities will encourage the design organizations and the utility to use this approach in development of an appropriate structure for plant TS.

Online monitoring systems may be considered by the regulatory authorities as a final goal in balancing operational safety and the availability of the plant. However, this approach is not likely to be implemented in Poland before well-established experience with using PSA is accumulated and a living PSA model is adopted by the utility and by the regulatory authorities.

SPAIN

In Spain, the regulatory agency, Consejo de Seguridad Nuclear, CSN, has been requiring since 1983 a PSA for each of the Spanish NPPs in a time-phased way. These requirements are being done according to a general Integrated Programme on PSA. The objectives of the Integrated Programme are not only the realization of the studies, but also their use for future applications.

One of the future applications of PSA that CSN is promoting is the evaluation and improvements of NPP Technical Specifications. For this reason, the CSN has an ongoing Programme on this subject, aimed at developing technical procedures for this systematic application of the PSA models. This Programme is under contract with a Spanish university and preliminary results are expected in 1991.

SWITZERLAND

The owners of nuclear power stations in Switzerland are required to submit Technical Specifications as part of the operating permit to the Swiss Regulatory Body, HSK (Haupabteilung für die Sicherheit um Kernanlagen). The use of PSA was originally a strong wish of the HSK. However, as progress has been made in developing PSA methods, the operators have seen the benefits as a supplement to existing practice.It still remains, in Switzerland, the operator's responsibility to assure safety. The method of proof is left to the operator, but the HSK must be convinced.

The following is a brief summary of the application of PSA to Swiss plants (in chronological order of application).

Leibstadt
(Startup 1984) Level 1 and level 2 PSAs have been developed for Leibstadt. In addition, a special PSA study for the bunkered redundant system, called the Special Heat Removal System (SEHR), was performed. A living PSA is being investigated for general use, and PSA is also being investigated for a power uprating.

Beznau
(Startup 1969) Beznau had to backfit a bunkered redundant system. To prove the adequacy of the system, a level 1 PSA was performed for system optimization. A level 2 PSA is under consideration.

Mühleberg
(Startup 1971) Same as Beznau

Goesgen
(Startup 1980) To investigate the most appropriate way to use PSA, HSK requested, in the first phase, a program like that of Leibstadt.

UNION OF SOVIET SOCIALIST REPUBLICS

An intensive implementation of the PSA approach for an analysis of safety of nuclear power plants in the USSR, mainly for an analysis of nuclear power plant design safety features, began in 1987 after the Chernobyl accident. As a result of efforts in recent years, the PSA methodology and technology as well as the original software packages and corresponding data bases with experimental and operational information have been developed. The PSA technique became a routine tool for designers and analysts.

Much of the PSA work and recommendations developed by the international scientific community, were analyzed and used for development of the PSA approach and techniques in the USSR. At the present time some preliminary, but sufficiently detailed, PSA analyses of design safety of VVER-1000 reactors were completed. This activity is under way for nuclear power plants with other types of reactors.

A set of "living" PSA systems based on use of PCs is under development with expected deployment on operating nuclear power plants in the near future (1992-1993).

The current practice of nuclear power plant safety analysis, as it was before, is mainly based on the use of the deterministic approach. At the same time, the PSA approach is considered as an important additional source of safety information that supplements results produced by deterministic methods.

The new version of the main regulatory document, "General Rules of Ensuring Nuclear Power Plant Safety " ("OPB-88") that will come into force on 1 July 1990, contains some probabilistic safety goals for nuclear power plants under design which should be achieved with use of the PSA approach, namely:

- the probability of radioactive release, which demands evacuation of the population beyond the predetermined distance, must not exceed $1x10^{-7}$ per reactor per year;

- the probability of severe core damage or core melt during beyond design basis accidents, must not exceed $1x10^{-5}$ per reactor year.

Thus, implementation of the PSA approach for the analysis and justification of the safety of new nuclear power plants in the USSR became a law.

UNITED KINGDOM

In the UK, the nuclear power plant operators are required to define the limits of operation for the station. These appear in a variety of station specific documents and as the Identified Operating Instructions which are equivalent to Technical Specifications for plants operated by Nuclear Electric. The operating limits are approved by the Regulatory Authority in the UK, the Nuclear Installations Inspectorate.

For the older plants, such as the Magnox reactors, the early AGRs and the Atomic Energy Authority (AEA) Prototype Fast Reactor and the Steam Generating Heavy Water Reactor, the limits of operation are largely based on deterministic criteria supplemented in some areas by probabilistic analysis.

Currently, PSAs are being carried out for all these plants as part of the Long-Term Safety Review of the Magnox and AGR reactors and for the licensing by NII of the Atomic Energy Authority reactors (which were formerly exempt from licensing by NII). One of the requirements of these PSAs is that they should address the unavailability of protection system equipment during periods of maintenance or test to demonstrate that the deterministic operating limits are acceptable. As a result of the analyses presented by licensees to date, changes have been made to the operating limits and new limits added to prevent items from being removed for maintenance which would have led to an unacceptable increase in the level of risk. There is currently no requirement by NII to provide an on-line facility to allow monitoring of the compliance with the limits of operation.

For the new AGRs at Heysham 2 and Torness, the operating limits are based explicitly on PSA with deterministic criteria added as a back stop. Although the design and the required limits of operation of these two plants are virtually identical, they are operated by different licensees - Heysham 2 by Nuclear Electric (formerly CEGB) and Torness by Scottish Nuclear (formerly SSEB). This has led to two quite different approaches being adopted for monitoring to assure that the limits of operation are being complied with.

For Heysham 2, the Essential Systems Safety Monitor (ESSM) provides an on-line tool for monitoring compliance with the operating limits and planning maintenance strategies.

For Torness, the allowable combinations for the outages of protection systems have been determined by multiple runs of the PSA. The results have been tabulated (hard copy only) and this is used by the operators for planning and decision-making.

Both of these arrangements have been assessed by NII and accepted as meeting the license requirement. This reflects the approach to licensing in the UK where NII places no specific requirement on the licensees who are allowed to devise their own ways of meeting the requirement of the standard license applied to all nuclear sites.

For the PWR proposed for Sizewell B, the licensee, Nuclear Electric, intends to provide the limits of operation in the form of Technical Specifications. These will be based on PSA.

It is also required by NII that a tool is provided to assist the operator in monitoring compliance with the technical specifications and for planning purposes. However, Nuclear Electric's proposals for this have not yet been received by NII.

UNITED STATES OF AMERICA

The U.S. Nuclear Regulatory Commission has, since 1987, been doing preliminary feasibility studies to investigate whether risk could be used to determine allowed outage times (AOTs) and surveillance test intervals (STIs) in Technical Specifications. These studies have concluded that it is feasible to set up a pilot application of a real-time risk based system to investigate its potential use as a replacement for some deterministic Technical Specifications requirements. At this time, no detailed discussions have taken place with a U.S. utility to set up such a pilot program.

At the present time, the U.S. industry and the NRC are engaged in the final stages of developing new deterministic Standard Technical Specifications. This development work has taken all the resources available for Technical Specifications work. It is not anticipated that much work will be done by the NRC until the new Standard Technical Specifications are completed at the end of 1990.

The U.S. NRC is following closely the work done in other countries, particularly the British ESSM and the work in the Scandanavian countries. Several NRC Commissioners and other senior managers have visited Heysham. The NRC staff has briefed the Commission on ESSM and other risk-based work.

In the meantime, the NRC staff has reviewed and approved various proposals for changing AOTs and SITs based on risk. In particular, some use of risk is being made in the new Standard Technical Specifications, especially for AOTs and STIs of safety-related instrumentation.

In summary, the NRC is actively studying the potential benefits of risk-based Technical Specifications and implementing some changes on a limited basis.

5. PILOT STUDIES

Limited scope pilot studies using risk and reliability techniques are useful to demonstrate the usefulness of these techniques to optimize Technical Specifications, and provide insights into practical issues associated with such applications.

Two types of pilot studies were suggested for consideration at the meeting by member states. The first type of pilot study is based on collecting actual plant data and calculation of changes in plant operational risk using a plant-specific PSA. The second type of pilot study is based on selecting the individual TS requirements that are creating operational or safety problems, and use risk and reliability techniques to assess the effect of changes to these individual requirements on the plant risk.

Based on discussions among participants it was suggested that the appropriate starting point for pilot studies is the second option, namely application of risk and reliability techniques for improvement of individual TS. This initial attempt could be followed by the more comprehensive data gathering and analysis suggested by the first option. Several countries indicated initial interest in participating in the pilot study. A brief description of the suggested pilot study is presented next.

5.1. Individual Technical Specifications Improvements Using Risk and Reliability Techniques

Limited scope pilot studies to demonstrate the practical application of reliablity- and risk-based analyses are proposed. Candidate studies must have the potential for completion and plans for implementation within 18 months and, therefore, must be limited to a single system, function, or other logical subset of operating limits and conditions. High quality logical PSA models or custom models for necessary systems and functions should be available for use in the pilot study.

Selection of candidate TS for optimization should consider the following criteria: 1) each requirement to be evaluated for change shall be a problem TS; that is, it places an operational, cost or safety burden on the plant, and 2) there should exist reasonable alternative requirements that can potentially reduce the burden without adversely impacting safety.

Steps of the pilot study will include:

- identification and documentation of problem TS for analysis;
- enumeration of alternative requirements;
- evaluation of alternatives using reliability- and risk-based methods;
- comparison of alternatives including the use of non-risk criteria;

- plans for implementation of selected alternatives along with any associated monitoring or reliability program commitments, if applicable;
- documentation of analysis and pilot study process

There are numerous risk- and reliability-based methods that can be employed in the pilot studies. More than one approach may apply within each case study.

Methods include:
- Risk-based evaluations of Allowable Outage Times (AOTs), Surveillance Test Intervals (STIs) or setpoints using PSA models.
- Technical Specifications optimization using Reliability Centered Maintenance or a similar systematic process.
- Design of reliability program elements to justify Technical Specifications relaxations.
- Substitution of annual system or function unavailability targets and calculations for AOTs.
- Real-time instantaneous risk targets and calculations to replace specific Technical Specifications requirements.

The risk criteria for acceptability of TS changes must be clearly identified. Criteria can include: an absolute risk limit for the TS, a relative or differential risk limit for new requirements compared to the old, qualitative considerations along with risk in a clearly defined decision process, or risk trade-offs which yield no net risk increase.

The form of the resulting operating limits and conditions can be single action AOT and test requirements, multiple option AOT and test requirements based on plant configuration, or case-by-case requirements based on risk or reliability targets.

The results and insights from the pilot study programme will serve as a basis for the IAEA to develop a procedures guide on the practical use of reliability and risk methods to optimize technical specifications.

6. CONCLUSIONS

Technical Specifications are an important part of the overall requirements for the operation of nuclear power plants. They define an envelope of operability that keeps the reactor in the safe operating regime. Deterministic TS for different types of reactors in various countries have provided a very good basis for defining this safe envelope of operability so far. However, in the early 1970's the concept of Probabilistic Safety Assessment (PSA) was introduced as an additional tool to supplement engineer's knowledge and judgment about the risk profile of the plants. Over the past fifteen years, these risk and reliability techniques have been used increasingly in the nuclear community for design, safety, and regulatory-related decision making.

It is apparent from the twenty-three papers and from the large representation of Member States (37 participants from seventeen countries in the meeting) that worldwide there is a recognition that risk and reliability techniques can be a useful tool to optimize the Technical Specification requirements. Furthermore, it is recognized that this optimization can enhance both the safety and the availability of the plant. Whether this optimization process will be concentrated on a select number of individual requirements or a fundamental look at the basis for all the Technical Specification requirements is not clear at this time. Most countries participating in this conference appear to have embarked on at least looking at evaluation of select individual Technical Specification requirements that either, from safety or operational point of view are considered a burden to plant staff.

At least one country, namely England, has implemented a fundamentally risk-based approach to Technical Specification for one of their nuclear power plants and has provided us a great deal of knowledge and insight into both the technical and institutional issues related with such a system.

During the meeting there was a very lively discussion about the need for some modelling improvements in the use of PSA techniques that are unique to the Technical Specifications application. This includes better modelling of failure rates for standby components whereby the effect of "demand stress" in testing the component and "standby stress" due to lack of component operation is properly taken into account. This is particularly important in optimization of Surveillance Test Intervals (STIs). Another unique feature of application of PSA techniques to Technical Specifications at the plant level is, that typical cutoff frequencies used in plant PSA cannot be applied to a PSA model used for Technical Specifications. This is due to the fact that a multi component failure, low frequency accident sequence can become a dominant sequence due to unavailability of one or more components in the sequence. This, elimination of low frequency sequences is not an acceptable practice for Technical Specifications requirements. This also brings up issues of how to retreat human reliability and recovery factors for these low frequency sequences that change characteristics following unavailability of one or more components.

A good deal of discussion was also spent on institutional issues associated with implementation of a risk-based approach to Technical Specifications. These institutional issues are primarily related to acceptability of these techniques by the plants operating staff. Again, the British experience in this regard is quite valuable.

The last international meeting focusing on Technical Specifications was held in Madrid, Spain in 1977. In that meeting only a portion of papers were on the subject of application of risk and reliability techniques to Technical Specifications. In this meeting essentially all papers focused on the application of risk and reliability techniques to Technical Specifications. The large number of papers and participants from various countries and the depth of the technical discussions show progress that the international nuclear community has made in applying risk and reliability techniques to optimize the technical specification requirements.

The initiation of a pilot study program suggested during this meeting, and sponsorship of more technical exchanges and meetings of this sort by the IAEA, are appropriate initiatives to best use risk and reliability tools to enhance plant operational safety while increasing plant availability at the same time.

Annex I

USE OF RELIABILITY METHODS AND PROBABILISTIC SAFETY ASSESSMENT TO IMPROVE OPERATIONAL LIMITS AND CONDITIONS

Report of a Consultants Meeting
Vienna, 4–8 December 1989

1.0 Introduction

1.1 Background

Operating limits and conditions have been established at most, if not all, power reactors in the world as a way to assure that the reactor is operated safely and in a manner which is consistent with the assumptions made in the plant safety analyses.

In the United States, for example, these operating limits and conditions are called Technical Specifications and are required by law to be part of the operating license issued by the regulatory authority for each reactor. In most European countries Technical Specifications have similar contents. Because of the widespread (though not universal) use of the term Technical Specifications to describe these operating limits and conditions, that term will be used in this report.

The ultimate goal of the Technical Specifications is to prevent radiological accidents at the reactor and thereby to protect the health and safety of the public and plant personnel.

Because of the vital importance of this goal, the individual requirements of the Technical Specifications have been defined with margins to assure that even under adverse conditions, equipment which must operate to prevent or mitigate the consequences of an accident will be capable of performing its function when called upon.

These requirements, have been developed, applied and improved in most countries over a period of years, and have, in general, been based on analysis and engineering judgment as to the amount of margin or conservatism that is necessary.

As more and more reactor-years of operation accumulate, the experience with Technical Specifications has led to the identification of several problems with Technical Specifications.

Some of the more significant examples are discussed below. Technical Specifications may require reactor shutdowns in situations which are not safety significant or even in cases where the shutdown may not be the safest course of action, given the state of the plant.

Since the individual surveillance test intervals (STIs) and allowed outage times (AOTs) of the Technical Specifications are, in general, derived separately and were not established in a manner directly dependent on plant risk, it may be possible that the Technical Specifications allow operation in a configuration that results in a relatively high risk compared to operation with all equipment operable.

Alternatively, Technical Specifications can prevent removal of components from service without consideration of risk-significance of the situation, thereby reducing plant operational flexibility. This can have adverse impact on plant operating cost and availability.

The testing and surveillance requirements contained in the Technical Specifications are also based, for the most part, on engineering judgment. This results in some equipment being tested more frequently than necessary. This is important since testing is a source of reactor trips and other plant transients as well as wear of safety equipment.

For these reasons several efforts have been initiated by the nuclear industry in several countries, generally with the encouragement of their regulators, to study the use of Probabilistic Safety Assessment (PSA) and reliability analysis as a tool to overcome these difficulties.

Using these reliability and risk-based methods, a number of Technical Specifications requirements in these countries have been modified.

In addition, other efforts are underway to remove from the Technical Specifications those requirements which are not germane to operation of the reactor (such as fire protection and utility organization requirements) and to make the Technical Specifications easier to understand and use.

1.2 Current Programs in the United States

The United States Nuclear Regulatory Commission (USNRC) began to deal directly with these concerns by forming a Task Group in August 1983, to review existing Technical Specifications requirements at that time. The Task Group summarized its findings in NUREG-1024 [1]. Motivated by these findings, the industry and the USNRC began major research programs on risk based improvements to Technical Specifications. Subsequently, on December 31, 1984, the USNRC established a Technical Specification Improvement Program (TSIP) with the dual goals of reassessing the entire area of Technical Specifications and providing recommendations for necessary changes and improvements that would enhance their usefulness and effectiveness. The U.S. nuclear industry, through the former Atomic Industrial Forum (AIF), initiated a similar effort at about the same time. In the Fall of 1985, the TSIP and AIF working groups published two separate reports for improving Technical Specifications [2,3].

In response to the TSIP and AIF recommendations, the USNRC issued an Interim Policy Statement on Technical Specifications Improvements that discussed the basic philosophy behind Technical Specifications requirements and established a set of criteria defining the requirements that should be included in Technical Specifications for nuclear power plants [4]. In addition the policy statement recommended further development of risk and reliability techniques for defining the requirements of and supporting changes to Technical Specifications.

Current efforts in the U.S. involve close cooperation between the TSIP, various individual utilities and utility organizations. These consist of four main elements:

1) Restructured Standard Technical Specifications: Through a coordinated industry program these have been submitted by each of the major U.S. reactor vendor-type utility owners' groups, and are presently being finalized in discussions with the USNRC. About forty per cent of the former limiting conditions for operation (LCOs) have been moved to other licensee-controlled documents, when they have not met any of three retention criteria. Those remaining have been revised to a more user-friendly format.

2) Individual Improvements: These are specific improvements in Technical Specifications applicable to a generic class of plants, based on a lead plant evaluation. Coupled with these are USNRC evaluations of owners' group generic topical reports requesting STI and AOT relaxation based upon risk and reliability analyses.

3) Modifications to Surveillance Requirements: The USNRC undertook a study of Technical Specifications surveillance requirements to ascertain if improvements were necessary. Every surveillance requirement in the Standard Technical specifications for the four U.S. reactor vendors was reviewed against four criteria:

a) Does the surveillance test result in plant transients?
b) Does the surveillance test result in unnecessary wear to plant equipment?
c) Does the surveillance test result in radiation exposure to plant personnel which is not justified by the safety significance of the test?
d) Does the surveillance test place a burden on plant personnel which is not justified by the safety significance of the test? (that is, is it a waste of time?)

With the participation of representative utilities of each reactor type this study found many surveillance tests which met one or more of these criteria and are candidates for revision. The identification of those tests which caused inadvertent reactor trips was considered especially important.

The results of this study are undergoing final review by the USNRC and will be published soon as an official USNRC report. United States nuclear utilities will then be encouraged to make changes to their Technical Specifications to eliminate or reduce the frequency of detrimental tests.

4) Application of Risk and Reliability-Based Methods for Optimization of AOTs and Surveillance Testing: An NRC/Industry working group was established in 1988 to consider this important area. Plant risk profile data have been submitted by three participating utilities. The major issues associated with the implementation of a real time risk based approach to Technical Specifications are being developed by Science Applications International Corporation, which has performed the major study in this area for the USNRC [5]. Other efforts in this area include the Procedures for Evaluating Technical Specifications (PETS) Program performed by Brookhaven National Laboratory (BNL), and many programs undertaken by the Electric Power Research Institute (EPRI) for the U.S. nuclear industry. The present stage of the USNRC work in this area is scheduled for completion in February, 1990 , with consideration for development of a computerized system to apply risk and reliability calculations and rules to advise the operator of allowed operating limits and conditions based on the current plant configuration. A pilot application of such a system is anticipated.

1.3 Current Programs in the Nordic Countries

In the Nordic countries the Technical Specifications are prepared by the operating organizations and approved by the regulatory authority (the Swedish Nuclear Power Inspectorate in Sweden and the Finnish Centre for Radiation and Nuclear Safety in Finland). At this time extensive operating and design experience has accumulated, and it has become necessary to deal with a number of problems that have appeared and which would benefit from specific modifications in these Technical Specifications rules. The goal of the modifications is to further improve nuclear safety and also to enhance the effectiveness and flexibility of plant operation and maintenance.

Developments in PSA have facilitated an analysis of the risk effects of alternative requirements in the rules. This makes possible a relative comparison and balancing of the rules from the risk point of view, and a justification of modified rules. For example, temporary high risk situations in plant operation can be identified and evaluated in advance so that they can be controlled. Also, excessively stringent but not safety-significant requirements may be modified in order to improve the operational flexibility and plant economy. At the beginning of the project [6] the LCOs and STIs were selected for evaluation by use of probabilistic and reliability methods.

The project work has been carried out by a Nordic Working Group, consisting of experts on Technical Specifications, PSA and reliability methods and plant operation.

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

The group has identified and selected Technical Specifications requirements and rules, concerning the active safety-related functions and systems, to be studied during the project. The pilot case studies have mainly concentrated on standby safety systems and functions. The work in these pilot studies has already contributed to proposals or approval of modified Technical Specifications rules [6].

2.0 Insights from the Programs in the United States and Nordic Countries

2.1 Insights from the USNRC Office of Nuclear Reactor Regulation efforts on Improvements to Technical Specifications Using Risk-Based Approaches

To improve the overall effectiveness of the Technical Specifications, the USNRC has initiated an effort to identify and evaluate alternative risk-based approaches that could bring greater risk perspective to these requirements [5]. This project is one of the initiatives sponsored by the NRC for improving the Technical Specification requirements using risk and reliability techniques.

The objectives of this study are: 1) identification of different risk-based approaches for improving current Technical Specifications, 2) assessment of characteristics of each approach including their advantages and disadvantages, and 3) recommendation of one or more approaches that might result in improving the current Technical Specification requirements.

Before discussing the alternative approaches identified, it is important to note that PSA techniques are only suitable for application to LCOs and STIs and some reactor trip setpoints. Even within these categories, PSA techniques are suitable for addressing only a portion of the current Technical Specifications. This is because many of the Technical Specifications requirements such as shutdown margins or pressure, temperature or flux limits are not the type of requirements that PSA is suited for. Case study results from two nuclear power plants indicate that approximately one-third of the LCOs and the corresponding AOTs and STIs can be analyzed using PSA techniques.

This study identified and evaluated four risk-based approaches. These are: 1) a real time risk-based approach, 2) a reliability goal-oriented approach, 3) a data-oriented approach, and 4) an approach based on configuration control. Detailed analysis of the advantages and disadvantages of each of these approaches indicate that from the analytical point of view, the best approach for controlling plant operational risk using risk and reliability techniques is the real time risk-based approach.

In the real time risk-based approach, the AOTs and STIs for different components or systems are based upon the importance of the component to the plant core melt frequency or risk. To assess the characteristics of a real time risk-based approach to Technical Specifications, a set of criteria for calculation of AOTs and STIs was developed. These criteria were based on the effect of unavailability of one or more components on the core melt frequency of the plant. The criteria included consideration of the USNRC's previously proposed safety goals on the core melt frequency limits. To test these criteria, the PSA model for two of the plants analyzed as a part of the NUREG-1150 effort were used [7,8]. For a series of cases involving unavailability of one or more components in these plants, AOTs were calculated using the real time risk-based approach and were compared to the current AOTs for these components.

For the first reference plant, AOTs calculated using the real time risk-based approach are in some cases higher than in the current Technical Specifications and are in other cases lower than the current Technical Specifications. For example, the real time risk-based AOT for outage of one diesel generator is much shorter than the current AOT for this equipment, whereas the real time risk-based AOT for low pressure injection (LPI) pump is substantially higher than the current AOT for this component. This points out the risk or core melt significance of the diesel generator versus LPI pump for this plant.

For the second reference plant, AOTs calculated using the real time risk-based approach and current AOTs are quite comparable, despite the fact that the core melt frequency of the second plant is higher than that of the first reference plant. The primary reason for this result is that the core melt frequency in the second reference plant is more evenly distributed among many dominant accident sequences. This implies that compared to the first reference plant, the second plant is not as vulnerable to failure of some components relative to others.

The real time risk-based approach is capable of generating AOTs for simultaneous, multiple component failues. This is a major advantage of this approach compared to the current approach to Technical Specifications.

Existing Technical Specifications do not have AOT requirements for failure of most combinations of components, which constitute the majority of component outage scenarios with highest contribution to the increase in core melt frequency.

In addition to the criteria for determining real time risk-based AOTs, a set of criteria for calculation of STIs using PSA techniques were developed. These criteria are based on the linkage between STI and AOTs in the real time risk-based approach to Technical Specifications.

The major conclusions of this study are as follows. The real time risk-based approach to Technical Specifications offers an attractive method for bringing greater risk perspective to the Technical Specifications. This conclusion is based on the fact that this approach utilizes the most comprehensive plant risk model currently available, and is capable of addressing balance of plant systems, beyond design basis accidents, severe accident issues, and the USNRC's proposed safety goal. These are all areas that are critical to the safe operation of nuclear power plants. In this approach, the AOTs and STIs are based on instantaneous core melt frequencies or risk importance of various components and systems. In addition, this approach offers the capability for calculating AOTs for multiple component failures, an advantage that is currently lacking in the Technical Specification requirements.

It is envisioned that risk-based calculations will be performed at the actual time that an AOT or test is considered. However, it is possible that real time decisions can be based on rules developed from risk analyses done previously.

Follow on work to this study is currently underway to define and address major issues associated with the implementation of a pilot study using risk-based approach to Technical Specifications that would enhance the safety and availability of plants. The major issues under study include: risk-based criteria, characteristics of the risk-based computer code necessary for real-time or near real-time calculations, a guideline on the level of detail and approaches used in the plant risk model for this purpose, cost estimates associated with the pilot study, Technical Specification requirements for components not included in the plant risk model, reliability-centered approaches for setting STIs, and institutional issues such as the need for licensees', monitoring of plants' components and systems, comparison of the plant's actual performance with assumptions used in plant risk model, frequency of plant risk model update, and the need for USNRC monitoring of the plant performance.

Once these issues are analyzed a decision will be made about the feasibility and usefulness of initiating a pilot study that would compare the characteristics of a risk-based alternative to the current deterministic Technical Specifications.

2.2 Insights from USNRC Procedures for Evaluating Technical Specifications (PETS) Program

The objectives of the PETS program are a) to study risk and reliability based approaches for modifying existing Technical Specifications, and b) to study alternative approaches for risk-based improvements to Technical Specifications. In seeking risk-based modifications to existing AOTs and Surveillance Requirements (SRs), the program developed approaches to apply risk analysis methods to Technical Specifications, investigated the issues associated with risk-based analyses, demonstrated the appliction of PSA methods to AOT and STI requirements at a nuclear power plant using a PSA, developed computer codes necessary to facilitate the application, provided approaches for numerical criteria in deciding acceptability of the modification and prepared risk method guidance for conducting the anlysis. Currently, the approaches and strategies of a risk-based configuration control system are being analyzed along with a framework for integrating surveillance requirements with various plant activities.

The major topics related to insights on risk-based modification to Technical Specifications are itemized below followed by a summary discussion.

1. Expected risk contributions associated with present Technical Specifications.
2. Maximum risk contributions allowed by present Technical Specifications.
3. Proper evaluation of the risk contributions associated with Technical Specifications.
4. Effect of PSA uncertainties in evaluating risk contributions from Technical Specifications.
5. Numerical criteria to assess acceptability of risks associated with Technical Specifications.

Based on a plant-specific study of the risks associated with AOT and STI requirements at a nuclear power plant, it was observed that the risk contributions assiciated with these requirements vary as much as four to five orders of magnitude. For this plant, the risk contributions associated with a significant portion of these requirements are small, whereas in some individual cases the contribution are significant. PSA methods can be used to prioritize these requirements. These requirements with small risk contributions can be loosened with little or no adverse risk impacts. Individual cases with significant contributions are candidates for reliability program activities [9].

In a variety of cases the maximum risk contributions allowed by Technical Specifications are significantly larger than the expected risk contributions calculated by PSA. That the maximum risk contributions allowed by Technical Specifications can be significantly higher than the expected contributions implies that the Technical Specifications in themselves do not necessarily control risks to the generally low levels indicated by PSAs. The variation in risk contributions come from four principal sources:

a) multiple components being allowed down at the same time,
b) components allowed to be repeatedly down,
c) test scheduling of different components being uncontrolled, and
d) maximum allowed downtimes.

It is important that appropriate evaluation of risk contributions along with necessary sensitivity or uncertainty analyses considering relevant issues be performed in evaluating risk impact of loosening (or of tightening) of Technical Specifications. With regard to evaluating the risks associated with allowed downtimes, both the risk from a given downtime and the expected risk from the average number of downtimes need to be calculated. It is the evaluation of the given downtime risk, and not the average risk contributions from downtimes, that is generally critical for assessments of allowed downtimes [10,11].

For risk contributions associated with surveillance tests, it is important to consider scheduling of tests as well as the interval between tests. Technical Specifications often do not address test scheduling and some scheduling of tests can have adverse impacts on risk. In evaluating risk impact of surveillance tests, human error common cause contributions should be considered. Appropriately defined staggered strategies may be necessary to avoid or minimize these contributions. It is furthermore important that risk significant failure mechanisms are detected by the test, which PSAs simply assume to be the case [12,13].

The uncertainties which are associated with PSAs carry over to evaluations of the risks associated with Technical Specifications. They include not only data uncertainties but also modeling and assumption uncertainties. In general, even with the uncertainties, the calculated risk contributions from Technical Specifications can be meaningfully used to assess the acceptability of Technical Specifications modifications from a risk standpoint. Furthermore by focusing on the risk contributions specifically associated with the Technical Specifications, only the uncertainties associated with these contributions need to be evaluated, which greatly reduces the uncertainty considerations.

The risk level at which the Technical Specifications risk contributions are evaluated is one of the most important factors in the uncertainty considerations. The risk level can be a system unavailability, a safety function unavailability, an accident sequence frequency, the core melt frequency, or a public health risk measure such as the expected early fatalities from accident. If the Technical Specifications risk contributions are evaluated at a risk level lower than a safety function unavailability, then significant system interactions can be overlooked. This applies particularly to evaluations of Technical Specifications for support systems but also applies in general to evaluations of Technical Specifications for frontline systems.

If Technical Specicfications are being evaluated for systems which mitigate the consequences of accidents, such as containment systems, then the risk measure needs to incorporate consequence considerations. To avoid the large uncertainties associated with complete consequence evaluations, the risk measure can consist of the accident sequence frequencies categorized according to release characteristics [14].

Criteria for acceptability of proposed Technical Specification modifications using risk based evaluations can include risk trade-off with not net risk increase or small increase in risk. To evaluate the acceptability of Technical Specification modifications with an associated risk increase, numerical criteria are to be considered. Efforts to derive numerical criteria that assure that the risk contribution from Technical Specifications are not dominant compared to other risk contributions and are consistent with a suitable safety goal or target value should be pursued [15].

The study of risk-based configuration control was directed at controlling plant configuration from a risk perspective that can not only provide more direct risk control, but also can result in more operational flexibility. Based on study of the configuration risks at two U.S. plants, the insights obtained are summarized below [16].

1) Some equipment configurations can cause large core-melt frequency increases. There are a number of such configurations that are not currently controlled by Technical Specifications. The expected frequency of occurrence of the impacting configurations is small, and the actual core melt probability contributions from the contributions are generally small.

2) Many such core melt frequency significant configurations can result from double component combinations, and in some instances, a single component outage can result in significant core melt frequency increases. This indicates that a plant can quickly move to a high core melt frequency level and that the process is not always

gradual, i.e. plants do not necessarily get into a significant core melt frequency configuration due to accumulation of out-of-service components.

3) There are also combinations of components which can cause significant core melt probability contributions if the outage duration is not controlled.

4) During operation, when plants operate near normal core melt frequency level flexibility can be provided for outage durations of non-risk impacting components and configurations. Appropriate surveillance tests can be defined to assure that a plant is truly operating at a low risk level.

The implications for configuration control approaches are:

1) A configuration control system could be developed to assure that core melt frequency significant configurations are avoided during power operation. Since these configurations can occur quickly and when they do occur can incur significant contributions in a short duration, a planning process can be defined for performing tests and maintenances so that, to the extent possible, such configurations do not occur. If they should occur, options for transferring to less risk-impacting configurations could be made available.

2) A configuration control system can also assure that combinations of components are identified whose simultaneous downtimes need to be controlled. The allowed downtimes can be defined to control core melt probability contributions and at the same time provide flexibility in operation.

2.3 Insights from EPRI Technical Specifications Research and Demonstration Activities

The Electric Power Research Institute (EPRI) has been a focal point for research and demonstration, sponsored by the U.S nuclear utilities, to optimize Technical Specification requirements. EPRI has emphasized practical applications of reliability and risk-based methods which demonstrate the usefulness of the methods and which transfer the technology to other utilities.

One specific project, Reliability and Risk-based Evaluation of AOTs and STIs, resulted in 1) development of an analysis method and computer code to use PSA methods for Technical Specifications evaluation 2) a system to identify and classify Technical Specification problems 3) demonstration analyses at two plants and 4) insights into the limitations and benefits of this analysis approach. These results are documented in references [17-21].

The development and demonstration of Reliability Centered Maintenance offers another method for Technical Specifications optimization, specifically for improving the content and frequency of surveillance tests. Examples of such evaluations are discussed in reference [22].

Other recent activities in the US provide an opportunity to commit to certain forms of reliability monitoring in exchange for relaxation of Technical Specifications. Work supported and planned at EPRI provides an

example of reliability program commitments that can justify Technical Specifications relaxations for the Emergency Diesel Generators. A related concept under consideration is the commitment to annual availability goals for safety systems in exchange for less strict AOT limits.

Finally, a pilot application of a real-time plant status monitor (PSM) at one plant has shown the practicality of monitoring the reliability of the plant and the status of its compliance with the Technical Specifications in order to make operational decisions regarding testing and maintenance. This pilot system shows the promise of removing prescriptive AOT and STI requirements and allowing flexible operating decisions based on the reliability and risk-implications of the current plant configuration.

Additional EPRI research projects show the potential to 1) consolidate and reduce test and calibration activities by carefully evaluating surveillance test content, 2) reducing instrument calibration frequencies by applying expert-system monitoring of redundant instrument channels and 3) reviewing test and failure records to justify test frequency relaxations based on the established reliability of components. Each of the above results can be incorporated into an integrated, reliability-based evaluation of Technical Specifications.

As a result of these and other U.S. industry projects, numerous insights emerge. These insights indicate that significant safety and cost improvements can be gained by the application of reliability- and risk-based analysis. However, they also indicate the need to further investigate several concerns related to implementing these concepts for controlling operating limits and conditions, and they indicate the need for trial applications of these concepts within the real operating and regulatory environments of nuclear power plants.

Specifically, EPRI research has shown that reliability- and risk-based methods can be applied to optimize AOTS, STIs, and reactor trip setpoints. At one plant about 40% of all needed Technical Specifications changes could be justified by such methods.

By addressing specific problem tech.specs and setting objective criteria for allowable changes in risk and reliability, many adjustments can be made within the current structure of plant Technical Specifications.

The analyses often require assumptions and data based on past or predicted operating experience. The acceptance of the analysis is strengthened if the utility will commit to monitoring and verification of these assumptions and data along with the changes in Technical Specifications.

As the operating requirements become more complicated and commitments grow in number, the value of a computerized system to aid the operator in applying the requirements suggests itself. Experience with PSM indicates that such a system is useful and practical.

There are many theoretical advantages to replacing prescriptive Technical Specifications with a real-time plant model which allows operational decisions to be made based on the current plant configuration. Numerous technical and administrative problems, however, must perhaps be overcome before such a system can be implemented.

Decision criteria must be as clear and unambiguous for operators as for current prescriptive Technical Specifications. Operators must have confidence that the models and data are accurate and complete, and calculations or inquiries of the system must not be difficult or time-consuming. Furthermore, the system must offer benefits of increased flexibility and improved plant operations. Implementation of the above concepts can be more or less difficult depending on the nuclear regulatory process of the country. In the U.S., utilities must provide a strong technical justification for all Technical Specifications change requests and must secure regulatory approval of all changes before they are implemented. Substitution of prescriptive Technical Specifications requirements with a real-time decision process would require a change in the current regulations philosophy and a change in current regulations themselves.

Pilot applications of the above concepts are feasible and necessary before widespread application is practical.

2.4 Insights on Optimization of Technical Specifications from the Nordic Countries' Programs

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

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

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

1. generally, to make optimal use of the available flexibility for Technical Specifications as a set.

2. specifically, to solve individual Technical Specifications problems in an optimal manner, normally by minimizing the plant risk.

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

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

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

Level 1 PSAs have been completed for thirteen nuclear power plants in Sweden and Finland and are currently being performed for the remaining three plants. Therefore, another main objective was to test and develop the use of PSA plant safety models for analysis and verification of Technical Specifications rules.

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

- proposed permanent modifications of Technical Specifications rules
- temporary exemptions from Technical Specifications rules.

The use of PSA methods also enhanced the understanding of the related complex operational situations and activities by systematic treatment and presentation of the many factors affecting the plant safety and availability.

A quick and approximate guide for timely decision making in specific operational and maintenance situations can be provided by precalculated risk importance measures. The use of these measures for evaluation of the safety significance of faults or maintenance tagging has also been demonstrated during the project.

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

- make risk-based comparisons of alternative plant operating principles during failure situations in safety systems and search such operating modes that give minimum risk

- evaluate risk increments temporarily caused by unavailable equipment, due to preventive maintenance in safety systems during power operation

- analyze the coverage and efficiency of single tests and quantify alternative test schemes of redundant equipment.

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

- reconsideration of plant shutdown requirements in situations when multiple failures occur in specific safety systems
- justification of modified rules for preventive maintenance in 4 x 50% standby safety systems during power operation
- improvement of the effectiveness of surveillance test procedures and schemes of standby equipment.

3.0 Proposed Actions

3.1 Introduction

The Technical Specifications define the limits and conditions for safe operation of a nuclear power plant. These limits and conditions are mostly based on deterministic analyses and engineering judgment. Experience has indicated operational and safety concerns with some of these requirements. Some elements of these requirements may be considered unnecessary or may not be conducive to the safety of the plant. Requirements are at times unnecessarily restrictive and many times become burdensome to the extent that they may divert attention from safe plant operation. In recent years a number of countries are successfully using risk and reliability-based methods to modify limiting conditions for operation and surveillance test requirements. Some countries are using or planning to use on-line monitoring systems as a complement or alternative to the present set of operating limits and conditions (or Technical Specifications).

In September 1987, OECD/CSNI/UNIPEDE and CSN organized in Madrid an international conference on improving Technical Specifications for nuclear power plants. The Conference was well attended signifying the interest in seeking modifications and enhanced understanding to Technical Specifications and also generated interest in applying risk- and reliability-based methods for Technical Specifications modifications. In December 1989 IAEA convened a consultants meeting with two basic objectives: a) to provide insights based on US and Nordic experience on the use of risk- and reliability-based methods to improve Technical Specifications and justify new changes, and b) to define the purpose and scope of a technical committee meeting and pilot studies to be performed under IAEA auspices.

This technical committee meeting will provide a forum for reviewing recent advances and future trends in this area. The pilot study plan on risk- and reliability-based evaluation and modification of Technical Specifications to be undertaken under IAEA auspices will also be finalized during this meeting. The insights from the pilot program will provide the technical basis for the preparation of an IAEA safety series document. Recognizing the difficulty with the existing requirements, this meeting will help generate interest in appropriate use of risk and reliability techniques for Technical Specifications improvement to achieve improved safety and operational flexibility.

3.2 Technical Committee Meeting

The purpose of the meeting is to compile, review and exchange experience on risk- and reliability-based improvements to Technical Specifications. In addition, participants will discuss the pilot studies proposed below in this document and will provide guidelines on the scope and ways to document these pilot studies. Thus the technical committee meeting will seek and encourage participation from member countries in these pilot programs.

3.2.1 Provisional Program

To meet the objectives of the meeting the programme will include technical sessions and working groups. Participants are encouraged to present papers in order to stimulate discussions and improve understanding of the methods and applications. Practical case studies and implementation of their results by the utilities and regulatory authorities are encouraged to be presented in the sessions.

Session I

Programs for risk and reliability based-evaluations and modifications of Technical Specifications.

- Industry Programs
- Vendor Programs

Session II

Applications and methods for modification of Limits and Conditions for safe operation:

- modification and determination of allowed outage times
- risk-based improvements to action statements
- operability requirements (including consideration of different plant states)
- interface with surveillance requirements
- preventive maintenance during power operation and refueling outages

Session III

Application and methods for evaluation of surveillance testing requirements

- Periodic surveillance tests and their intervals
- Effectiveness of tests
- Test scheme arrangements for redundant equipment
- Changes in set points
- Reliability-centered maintenance for optimization of STIs
- Integration of surveillance requirements with other activities

Session IV

Managing Technical Specifications using risk-based status monitoring

- Risk-based configuration control systems
- Use of risk-monitoring and control
- On-line risk advisors

Session V

Regulatory Perspective on the Use of Risk and Reliability Techniques in Technical Specification

- Current Practices in Member States
- Risk-Based Criteria
- Potential For Future Applications

Session VI Working Groups

Following all the presentations in the technical sessions, four parallel working group sessions will be organized as follows:

Working Group 1: Limits and Conditions of Safe Operation
Working Group 2: Surveillance Testing Requirements
Working Group 3: Risk Based Safety Status Monitoring
Working Group 4: IAEA Pilot studies

The working groups will be focused on discussing and reviewing the papers presented in the respective sessions and will prepare a summary document reflecting the experiences and the lessons learned. Working Group 4 will specifically review the IAEA draft document on the pilot studies and will finalize the pilot study plan.

Session VII

Summary and Conclusion from the Discussions

- Report on international status and experience on the use of reliability and PSA methods for Technical Specifications evaluation
- IAEA pilot study plan
- Future IAEA activities

3.3 Pilot Studies

Limited scope pilot studies which demonstrate the practical application of reliability- and risk-based analyses are proposed in this section. Candidate studies must have the potential for completion within 18 months. Studies already completed or currently underway are also welcomed. Actual cases of implementation of Technical Specifications changes due to risk- and reliability-based analyses would provide additional benefits to this pilot study.

Two types of pilot studies are suggested for consideration by member states. The first type of pilot study is based on collecting actual plant data and calculation of changes in plant operational risk using a plant-specific PSA. This type of study is discussed in detail in Section 3.3.1. The second type of the pilot study is based on selecting the individual Technical Specification requirements that are creating operational or safety problems, and use risk and reliability techniques to assess the effect of changes to these individual requirements on the plant risk. These types of pilot studies are discussed in Section 3.3.2.

3.3.1 Assessment of the Effect of the Current Technical Specifications on the Plant Operational Risk

Current Technical Specifications requirements might in some cases not be effective in controlling plant risk, and in other cases they might be too restrictive, preventing the necessary flexibility that the plant operations personnel might need. To assess these concerns, a pilot program is proposed whereby the participating members would initiate an effort to gather actual data on plant operation and develop the plant risk profile as a function of time using a plant-specific PSA.

The primary objective of such an exercise would be:
1) to determine if there are cases of multiple component outages that plant can enter into without violating their current Technical Specifications that result in large increases in plant risk, and 2) to assess if there are any configurations that the plant would want to enter into that do not result in significant increase in plant risk but are prohibited by the current Technical Specifications.

The starting point of the data gathering portion of this effort would be for each participating nuclear power plant in a member country to determine the initial plant status in terms of components that are out of service. Once the initial plant status is recorded, the plant personnel are requested to keep a daily record of changes to plant status. There are two types of data that are necessary for this purpose. First, there is need for a daily record of what components are taken out of service, and what components are put back into service. All changes to plant status should be recorded regardless of whether the component is taken out on a voluntary basis for preventive maintenance, a normal test, or as a result of an actual component failure. The second type of data is related to situations where the plant would have wanted to take a component out of service for preventive maintenance, special test, or any other reasons, but they were prevented because having taken the component out of service would have resulted in entering an LCO violation.

The case study must consider the difference between the actual equipment inoperability and the administrative definition of inoperability which could be much more conservative. This difference will significantly affect study results.

Using these data, the plant personnel can next calculate the changes in the plant operational risk profile due to plant configuration changes using their plant-specific PSA. These calculations can be performed on a daily, weekly or monthly basis depending on the plant's preference and availability of the required resources. For this pilot program it is proposed to use core melt frequency to represent plant operational risk to avoid the larger effort associated with containment and consequence analysis, and questions regarding uncertainty with Level 2 or 3 analyses. The starting point for these calculations would be to calculate the core melt frequency of the plant for the initial plant configuration that data gathering effort was initiated. From this point, the core melt frequency of the plant would be calculated for each change in plant configuration due to taking a component out of service or restoring a component back to operation. In addition to this, for each scenario that the plant would have wanted to take a component out of service for preventive maintenance or other purposes, but were prevented because of violation of LCO limits, a calculation should be done on the increase of the plant's core melt frequency if that component had been taken out of service.

The potential benefits of such a pilot program are:

1) Insight into the changes in the plant core melt frequency profile as a function of time during normal operation of the plant. Specifically, assessment of the effectiveness of the current deterministic Technical Specifications in controlling plant operational risk.

2) Effect of current deterministic Technical Specifications in preventing the plant to have the necessary flexibility in performing tests or preventive maintenance on various components without a substantial increase in plant's operational risk.

3) Identification of actual scenarios consisting of multiple component outages that do not result in Technical Specifications violations, but result in large increases in core melt frequency and are not intuitively obvious to the plant operators. This point would provide the initial input on whether a real-time risk-based advisory system would be useful in assisting the plant operators in controlling plant operational risk.

Overall, such a pilot program could provide a large body of information about the current Technical Specifications in various countries regarding a) the ability of the current Technical Specifications in controlling plant operational risk, b) reduction of the flexibility necessary for operation of nuclear power plants, and c) the need or usefulness of a plant risk advisory system to assist the plant operations staff in dealing with complicated multicomponent outage and maintenance scenarios.

3.3.2 Individual Technical Specifications Improvements Using Risk and Reliability Techniques

Limited scope pilot studies which demonstrate the practical application of reliablity- and risk-based analyses are proposed.

Candidate studies must have the potential for completion and plans for implementation within 18 months and, therefore, must be limited to a single system, function, or other logical subset of operating limits and conditions. High quality logical PSA models or custom models for necessary systems and functions should be available for use in the pilot study.

Selection of candidate Technical Specifications for optimization should consider the following criteria: 1) each requirement to be evaluated for change shall be a problem Technical Specification; that is, it places an operational, cost or safety burden on the plant, and 2) there should exist reasonable alternative requirements that can potentially reduce the burden without adversely impacting safety.

Steps of the pilot study will include:

- Identification and documentation of problem Technical Specifications for analysis
- Enumeration of alternative requirements
- Evaluation of alternatives using reliability- and risk-based methods
- Comparison of alternatives including the use of non-risk criteria
- Plans for implementation of selected alternatives along with any associated monitoring or reliability program commitments, if applicable
- Documentation of analysis and pilot study process

There are numerous risk- and reliability-based methods that can be employed in the pilot studies. More than one approach may apply within each case study. Methods include:

- Risk-based evaluations of AOTs, STIs or setpoints using PSA models. Analysis codes such as SOCRATES and FRANTIC can be used
- Technical Specifications optimization using Reliability Centered Maintenance or a similar systematic process
- Design of reliability program elements to justify Technical Specifications relaxations
- Substitution of annual system or function unavailability targets and calculations for AOTs
- Real-time instantaneous risk targets and calculations to replace specific Technical Specifications requirements.

The risk criteria for acceptability of Technical Specifications changes must be clearly identified. Criteria can include: an absolute risk limit for the Technical Specifications, a relative or differential risk limit for new requirements compared to the old, qualitative considerations along with risk in a clearly defined decision process, or risk trade-offs which yield no net risk increase.

The form of the resulting operating limits and conditions can be single action AOT and test requirements, multiple option AOT and test requirements based on plant configuration, or case-by-case requirements based on risk or reliability targets.

3.3 Other Initiatives

Application of reliability- and risk-based methods for Technical Specifications optimizations will result in more flexibility in operating limits and conditions. Such flexible requirements are best handled when incorporated into a computerized aid for the operator and engineering staff.

This aid will keep track of all the operating limits and conditions, will track relevent equipment status, will perform necessary on-line risk calculations or decision logic, will track monitoring requirements or other associated commitments, and will present the resulting requirements and advice to the operating staff in a clear format.

After establishing the success of the pilot applications discussed above, the structure and form of a computerized operational tool should be specified. Consideration should then be given to extension of the pilot studies to develop the computerized operational tool along with its implementation at an operating nuclear plant.

REFERENCES

[1] Technical Specifications -- Enhancing the Safety Impacts "NUREG-1024, November 1983.

[2] Memorandum for Harold Denton, Director, Office of Nuclear Reactor Regulation, from Don H. Beckham, Director, Technical Specification Improvement Project, Subject: Final Report of the Technical Specification Improvement Project, September 30, 1985.

[3] Technical Specifications Improvements, by AIF Subcommittee on Technical Specification Improvements of the Committee on Reactor Licensing and Safety, October 1985.

[4] Commission Interim Policy Statement on Technical Specification Improvements for Nuclear Power Reactors, February 1987.

[5] Alternative Approaches to Risk-Based Technical Specifications, Final Report, B. Atefi, D. Gallagher, E. Lofgren, R. Liner, Jr., Science Applications International Corporation, June 3, 1988.

[6] Optimization of Technical Specifications by Use of Probabilistic Methods. A Nordic Perspective 1985-1989. Draft Report NKA/RAS 450, Nov. 1989. Nordic Liaison Committee for Atomic Energy (Ed. by K. Laakso, Technical Research Centre of Finland).

[7] Analysis of Core Damage Frequency from Internal Events: Surry Unit 1, NUREG/CR-4550, SAND 86-2084, November 1968.

[8] Analysis of Core Damage Frequency from Internal Events: Sequoyah Unit 1, NUREG/CR-4550, Vol.5, SAND 86-2084, February 1987.

[9] Evaluation of Risks Associated with AOT and STI Requirements at the ANO- Nuclear Power Plant, P.K. Samanta, S. Wong, and J.Carbonaro, NUREG/CR-5200, BNL-NUREG-52024, August 1988.

[10] Evaluation of Allowed Outage Times (AOTs from a Risk and Reliability Standpoint, W.E. Vesely, NUREG/CR-5425, Brookhaven National Laboratory, August 1989.

[11] Risk Methodology Guide for AOT and STI Modifications, P.K. Samanta, W.E. Vesely, E. Lofgren, and J. Boccio, BNL Technical Report, A-3230-12-02-86, December 1986.

[12] Evaluation of Diesel Unavailability and Risk Effective Surveillance Test Interval, W.E. Vesely et al., NUREG/CR-4810, Brookhaven National Laboratory, May 1987.

[13] Consideration of Test Strategy in Defining Surveillance Requirements, P.K. Samanta, T. Ginsburg, and W.E. Vesely, BNL Technical Report, A-3859-10-18-89, October 1989.

[14] Evaluation of Uncertainties Associated with Technical Specification Risk evaluations, P.K. Samanta, J. Penoyar, and W.E. Vesely, BNL Technical Report, A-3859-11-3-89, November 1988.

[15] Procedure to Define Numerical Criteria to Assess Risk Associated with Technical Specifications, W.E. Vesely, BNL Technical Report, A-3230, June 1986.

[16] Analyses of Approaches and Strategies for Risk-Based Configuration Control Systems, P.K. Samanta, W.E. Vesely, and I.S. Kim, BNL Technical Report, A-3220-10-13-89, October 1989.

[17] D.P. Wagner, W.E. Vesely, and L.A. Minton, Risk-Based Evaluation of Technical Specifications, NP-4317, Electric Power Research Institute, March 1987.

[18] D.J. Bizzak, M.E. Stella, and J.R. Stukus, Identification and Classification of Technical Specification Problems, NP-5475, Electric Power Research Institute, December 1987.

[19] D.J. Bizzak, A.S. McClymont, and J.E. Trainer, Risk-Based Evaluation of Technical Specification Problems at the LaSalle County Nuclear Station, NP-5238. E-P-R-I, June 1987.

[20] W.P. Sullivan, C. Ha, and D.C. Pentrien, Technical Specification Improvements to Containment Heat Removal and ECCS Systems, NP-5904, July 1988.

[21] D.P. Wagner and L.A. Minton, PC-SOCRATES Users' Guide (Draft Report), EPRI RP-2142, Batteille Columbus Laboratories, March 1987.

[22] J.P. Gaertner et al., Demonstrations of Reliability Centered Maintenance, NP-6152, Vol.1, January 1989, Vols. 2-3, September 1989.

EXPERTS WHO PREPARED THIS DOCUMENT

Consultant's Meeting (4-8 Dec. 1989)

B. Atefi	Science Applications International Corporation Virginia, USA
J.P. Gaertner	EPRI Washington, USA
K. Laakso	VTT/SAH Technical Research Centre of Finland
R. Lobel	NRC, Technical Specification Branch, Washington, USA
P. Samanta	Brookhaven National Laboratory Upton, N.Y., USA
M. Wohl	NRC, Technical Specification Branch, Washington, D.C., USA
B. Tomic	IAEA Division of Nuclear Safety

Technical Officer: L. Lederman
Division of Nuclear Safety
IAEA

Annex II

PAPERS PRESENTED AT THE MEETING

OPTIMIZATION OF TECHNICAL SPECIFICATIONS BY USE OF PROBABILISTIC METHODS — A NORDIC PERSPECTIVE

K. LAAKSO
Technical Research Centre of Finland,
Espoo, Finland

A. ENGQVIST
Swedish State Power Board,
Vällingby, Sweden

M. KNOCHENHAUER
ABB Atom AB,
Västerås, Sweden

M. KOSONEN
Teollisuuden Voima Oy,
Olkiluoto, Finland

B. LIWÅNG
Swedish Nuclear Power Inspectorate,
Stockholm, Sweden

T. MANKAMO
Avaplan Oy,
Espoo, Finland

K. PÖRN
Studsvik Nuclear,
Nyköping, Sweden

Abstract

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

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

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

1. INTRODUCTION

1.1 Technical Specifications

The Technical Specifications (TS) define the limits and conditions for safe plant operation. In the Nordic countries the Technical Specifications are prepared by the operating organizations and approved by the regulatory authority. These operational safety rules have been defined with margins on the safe side, mainly on the basis of deterministic analyses prepared for the Final Safety Analysis Report (FSAR) of the nuclear power plant and on the basis of engineering judgement. At this time an extensive operating and design experience has accumulated and a number of problems have appeared which require specific modifications to the TS rules. The modifications aim to improve the nuclear safety further and also to enhance the effectiveness and flexibility of plant operation, maintenance and testing.

A general overview of the structure and contents of the TS in the Nordic Boiling Water Reactor (BWR) plants follows in Table 1.

Table 1 General contents in Nordic BWR Technical Specifications for operation.

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

At the beginning of the project [1] limiting conditions for operation and periodic testing were selected for evaluation by use of probabilistic methods.

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

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

This project concentrated on the issue of permanent TS modifications.

The active safety-related systems and safety functions were found suitable as case study objects. The practical part of the studies thus mainly concerned standby safety systems and functions.

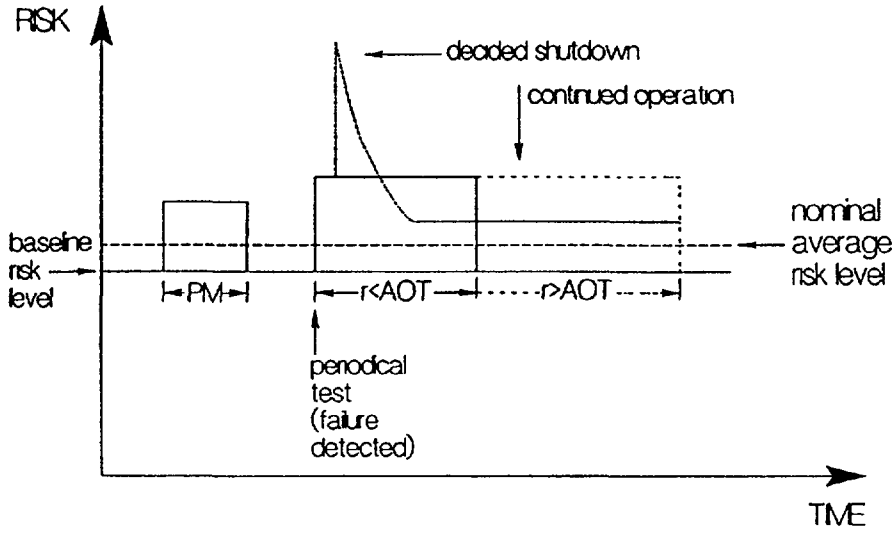
1.2 Probabilistic safety assessment

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

PSAs have now been completed for thirteen nuclear power plants in Sweden and Finland and are currently being performed for the remaining three plants. Therefore, one main objective was to test and develop the use of PSA plant safety models for analysis and verification of TS rules. This has also contributed to the current development of living PSA issue.

1.3 The task of optimization

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



Abbreviations:

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

Figure 1 Summary of risk definitions when considering the influence of failure and maintenance situations in safety systems during power operation

Therefore the task of TS optimization has a twofold meaning:

1. Generally to make optimal use of the excessive safety margin available for a specific set of TS rules to provide operational flexibility.

2. Specifically, to solve individual TS problems in an optimal manner, normally by minimizing the temporary risk increases.

2. RESULTS

2.1 Practical results for utilities and authorities

The case studies have produced useful results for specific Nordic nuclear power plants (TVO and Forsmark), for example:

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

The use of PSA methods through their systematic approach also enhances the understanding of complex operational situations where many factors affect the plant safety and availability. An example of that is given in another paper of this meeting [2]. Thereby the readiness for prompt safety-related decisions on operational problems can be considerably improved.

2.2 Method development

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

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

An approximate guide for prompt decision making in specific failure and maintenance situations during plant operation can be provided by precalculating so-called risk importance measures.

The use of risk increase factor for such TS considerations, i.e. evaluation of the safety significance of unavailability of equipment due to fault or maintenance, was developed and tested further during the project.

The Fig. 2 gives an overview of the items evaluated during the project.

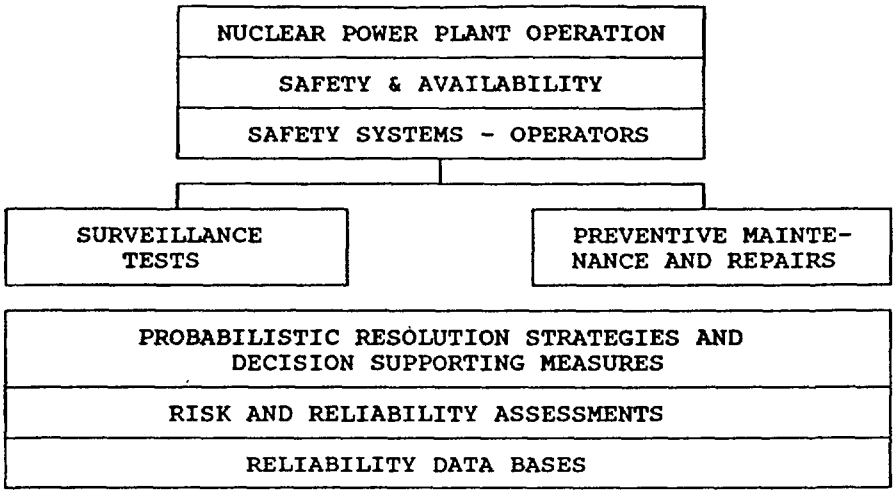


Figure 2 An overview of the items evaluated during the project.

3. CONCLUDING REMARKS

Some complementary conclusions from the NKA/RAS-450 project are given in this chapter of the paper. Topics for proposed continued work are given. Potential opportunities for further use of the project results are also presented.

3.1 The use of probabilistic decision criteria

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

1. Quantitative demonstration of numerical acceptability, with or without the use of a formal acceptance criterion.

2. Case-by-case decision based on weighing quantitative results against qualitative assumptions and boundary conditions.

3.2 Optimization of limiting conditions for operation

It was concluded that usually the total average risk can be affected relatively little by the optimal choice of the allowed outage times (AOT) for repairs in safety systems with four trains. However, in the cases of multiple failures in a safety system, order of magnitude differences may exist between the expected risks over the failure situation in question, depending on which operational mode is selected. The central LCO issue, the decision between repairs during continued power operation or plant shutdown for repairs, has also a significant economic consequence because of the high income loss caused by a forced plant shutdown.

The TVO shutdown risk analysis concerning the residual heat removal function shows an example where the probability of the safety function to be unavailable, when demanded, is much more sensitive to the reliability of the equipment and operations than to the AOTs of equipment [2]. This difference depends on the undetected unavailability time due to latent faults in standby equipment. The TS-related equipment is maintained with care at Swedish and Finnish plants, but the frequency of failures and disturbances is not directly treated in TS. However, the failure occurrence determines the likelihood of entering into rare multiple failure situations. Hence, we want to strongly emphasize the primary role of reliability assurance measures for the achievement of as low failure and disturbance frequencies at the plants, as reasonably achievable.

In order to provide a proper risk perspective, it is often necessary to calculate more than one risk measure. The choice between operational alternatives in TS should be made with due regard to:

- instantaneous risk frequency during a failure situation
- integrated risk over the failure situation in question

- increment in lifetime risk due to the expected number of similar failure situations.

This approach is structured by a decision tree in Fig. 3, and it has similarities with the approach presented in Ref. 3.

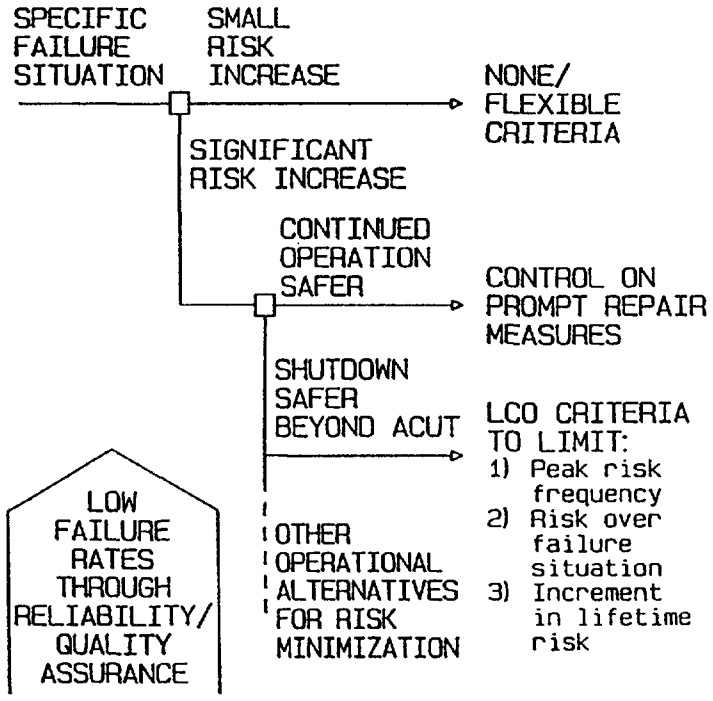


Figure 3 Decision three presentation for the proposed criteria on allowed outage time (AOT) during power operation in the case of critical failures detected in safety systems.

3.3 Preventive maintenance of standby safety systems during power operation

Performing preventive maintenance (PM), in one subsystem at a time of four subsystems during power operation in the newest Nordic BWR plants, has many qualitative benefits compared to PM during refuelling outage. The qualitative benefits were not possible to express in quantitative terms, but it can be expected that improved equipment reliability, at least partially, counterbalances the few percent's unavailability contributions from the PM periods during power operation. One disadvantage of performing the PM during refuelling outage is that it is loaded with a large number of tasks within a tight time schedule. Within

the project the temporary risk increments, caused by unavailability of equipment due to PM during power operation, were evaluated by adaptation of a PSA plant level model.

It was possible to justify the introduction of a limited period of preventive maintenance during power operation, based on:

- the relative comparison of temporary risk increments during the PM periods with the nominal average risk level of plant operation
- the designed excess margin of the four subsystem configuration to single failure criteria with one subsystem unavailable due to PM.

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

The safety systems in Forsmark 1/2 and TVO I/II plants, designed for emergency cooling of the reactor core, are presented as an example in Fig. 4.

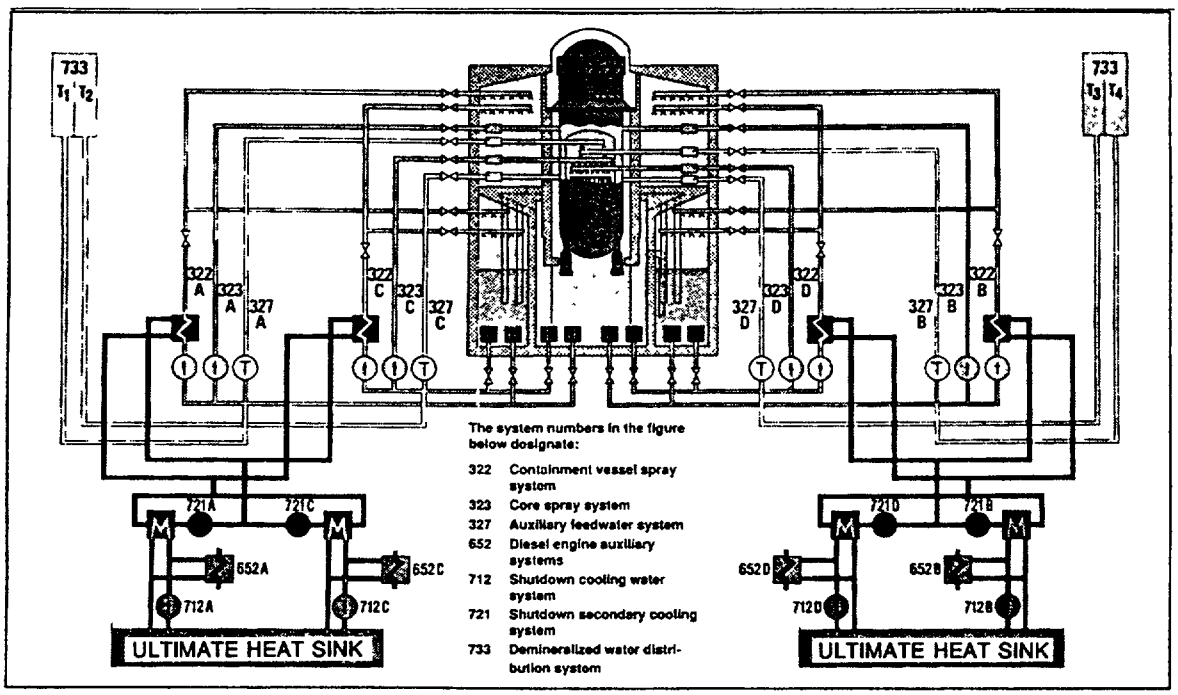


Figure 4 A schematical presentation of emergency cooling systems in a BWR plant.

3.4 Test arrangements

When comparing the accident and testing conditions for motor-operated closing valves (MOV) in safety systems, considerably deviating operating conditions were found in some cases, concerning e.g. differential pressures over slide and increasing temperatures. This finding is also significant for the PSA issue, because failure data mainly originates from surveillance tests and the reliability of some MOVs may thus be questioned in more severe accident scenarios. Appropriate studies and corrective actions for reliability and testing improvements of valves are under way at the power companies.

The different case studies of motor-operated closing valves, emergency diesel generators and auxiliary feed water systems have included practical qualitative and quantitative analyses of test effectiveness.

The use of functional block techniques also showed encouraging results when evaluating the coverage of system tests for an auxiliary feedwater system.

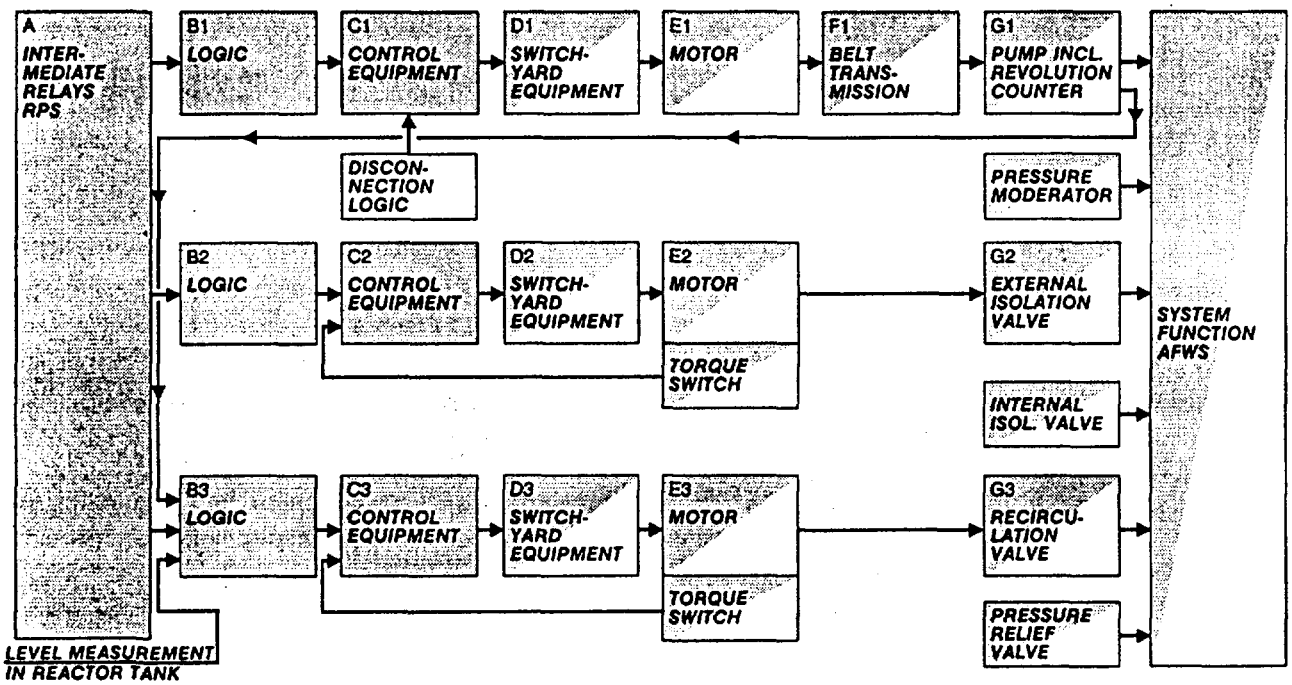


Figure 5 Test coverage chart for the test of RPS signals in the auxiliary feedwater system.

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

The test interval is often the primary free variable which, however, has contradictionary influences as presented in Fig. 6. Balancing between these influences is a main optimization task.

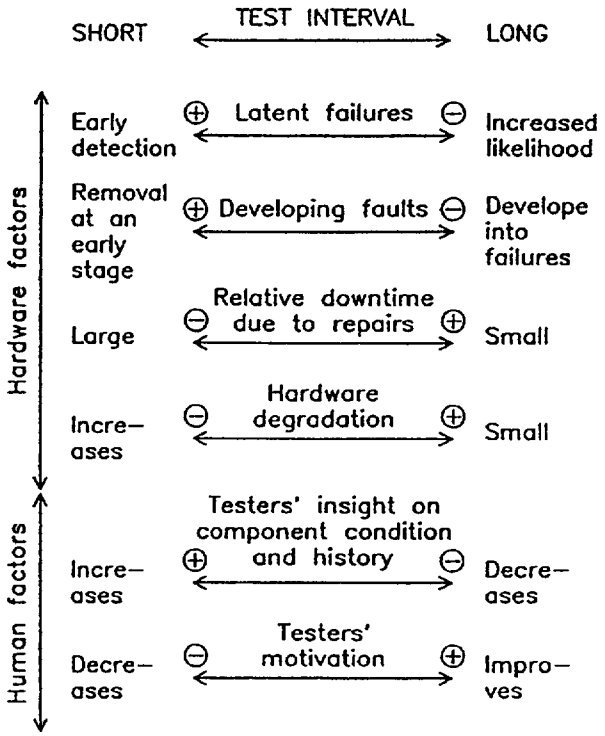


Figure 6 Test interval influences.

3.5 Future plans

In the long run, one should try to attain the Living Probabilistic Safety Assessment (LPSA) by continuously using new experience from operation, maintenance and design to update the PSA models and data. Incidents should be analyzed to indicate improvement needs both at the plant and in the PSA. Systematic use of PSA should be made for decision support in matters concerning safety.

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

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

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

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

A Living PSA is planned to be a flexible system for assessing relative changes in the reactor core damage frequency caused by permanent changes in designs or by temporary changes in operating situations.

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

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

One objective of the NKS/SIK-1 project is to define a feasible risk and reliability based system for control of operational safety to supplement the present technical specifications. Selected parts of such an information system will be tested in practical case studies which form the basis for definition of the information system concept. The case studies will include an evaluation of the benefits and limitations of the use of such a system in different application areas.

3.6 Transfer of results

The most part of the project work has been carried out by a Nordic working group, consisting of experts on operational safety, PSA and reliability methods. Representatives from utilities, regulatory authorities, research institutes, vendors and consultants have worked in this group. The group has communicated with the nuclear power utilities and authorities and others interested in the subject and arranged several project seminars in Sweden and Finland.

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

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

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

REFERENCES

1. Optimization of Technical Specifications by Use of Probabilistic Methods - A Nordic Perspective. Edited by Kari Laakso. Prepared by a team consisting of Kari Laakso, Michael Knochenhauer, Tuomas Mankamo and Kurt Pörn. 157 pages. Nord Series. May 1990:33.

2. Mankamo, T. & Kosonen, M. Operational Decision Alternatives in Failure Situations of Standby Safety Systems. To be presented at the IAEA Technical Committee Meeting on the Use of Probabilistic Safety Analysis to Evaluate Nuclear Power Plant's Technical Specifications. Vienna, June 18 - 22, 1990.

3. Wesely, W., Samantha, P. K. Risk Criteria Considerations in Evaluating Risks from Technical Specification Modifications. Technical Report BNL & SAIC, Draft Jan. 1989.

EPRI PERSPECTIVES ON THE USE OF RISK-BASED TECHNICAL SPECIFICATIONS IN CONTROLLING PLANT OPERATIONS

J.-P. SURSOCK
Electric Power Research Institute,
Palo Alto, California

D. TRUE
ERIN Engineering and Research, Inc.,
Walnut Creek, California

United States of America

Abstract

In recent years there has been considerable interest in the use and application of probabilistic risk techniques to the development of technical specifications. The Electric Power Research Institute (EPRI) has participated in the investigation and application of these methods in the U.S. and continues to support new and innovative approaches. This paper describes the program EPRI has established for the evaluation and development of risk-based technical specifications in controlling plant operations.

The paper identifies institutional and technical obstacles associated with the concept of a real-time risk monitor, and then proceeds to describe the current EPRI program.

Flexible technical specifications actions or "flex specs" promise to increase operating flexibility by providing the plant operating staff with pre-planned alternative actions to be taken in response to a specific limiting condition for operation, depending upon the plant configuration.

The introduction of additional complexity into the technical specifications will require additional tools to be developed to assist the plant operating staff in determining the options available. EPRI is investigating a PC-based tool for use in this application. This tool, called an Integrated Risk Advisor (or IRA), will provide the control room operators with information on flex spec options, support system unavailabilities, tracking of component and system reliabilities, as well as access to standard technical specification information.

---

1. Introduction

The concept of Risk based Technical specifications (RBTS), sometimes considered synonymous with a real time risk monitor (RM), presents a tremendous opportunity for improving both plant safety and plant operating flexibility. The Electric Power Research Institute (EPRI), has been actively involved in the development and application of risk-based approaches to technical specifications for the past seven years. EPRI views the development

of RBTS in much broader terms than a risk monitor. Rather, EPRI envisions a computerized tracking and operator support tool which will provide assistance to the plant operating personnel when they need it, without increasing their burden.

The concept termed Integrated Risk Advisor (IRA) is sometimes confused with that of the Risk Monitor ("risk-meter"). The purpose of this paper is to clarify the concept of IRA as currently (June 1, 1990) envisioned by EPRI and describe the EPRI program.

The RM can be conceived as a real-time or off-line computation of the "safety risk" (according to some criteria) of the plant in its current configuration. This information would presumably be used by the operators to help evaluate the advisability of removing certain components from service under the existing configuration or continuing to operate in the existing state. Thus, the RM would take into account all the components' unavailabilities at a given time and perform a Probabilistic Risk Assessment (PRA) to compute the corresponding risk level. Projected actions on components or systems (e.g. isolation of a system for 24 hours for repair) can then be evaluated on the basis of the incremental risk they would introduce.

There are, however, several institutional and technical problems affecting the concept of a RM. These problems are discussed in the first part of this paper. They have led EPRI to seek another concept that would minimize these problems and facilitate the broader application of Risk-Based Technical Specifications (RBTS). The concept of the IRA is still evolving and can only be firmed up after the planned effort of extensive interviews with interested utilities is completed in July 1990. A preliminary set of characteristics is given in the second part of the paper.

Historical Background

Since 1984, the U.S. nuclear industry and the US Nuclear Regulatory Commission (NRC) have been exploring the potential benefits of RBTS, mostly as a result of two developments: the ever increasing complexity of Technical Specifications (TS) (which are causing the problem) and the maturing of PRA methods (which afford a cost-effective solution).

The NRC program has evolved along two axes. The technical issues that need to be addressed in order to implement RBTS are evaluated as part of the "Procedures for Evaluating Technical Specifications" (PETS) program; while a more recent effort, in coordination with an ad hoc industry working group, has attempted to define the basis and requirements for a real time, on-line RM. The main function of the RM is to provide an instantaneous evaluation of the plant risk, in its actual configuration. This information can then be used by the plant operator in making decisions on optimizing the timing for equipment maintenance and testing.

The industry, through the four NSSS Owners' Groups, has also initiated a major restructuring of the TS. The purpose of developing these "Standard Tech Specs." (STS) package is to streamline the existing TS documentation, to

provide consistency among the four US suppliers, and to provide the operator with clearer directions. This effort is now almost completed. Lead plant topicals will soon be submitted to the NRC for review.

During this period (1984- 1988), EPRI sponsored the development of a systematic approach to identify and evaluate "problem" TS that could be reassessed from the standpoint of their risk significance. Most of these "problem' TS are characterized by over-restrictive Allowed Outage Times (AOT) and Surveillance Testing Intervals (STI). These restrictions not only could lead to unnecessary plant unavailability and equipment wear but could also, in some circumstances, reduce the actual safety of the plant. A central piece of EPRI's technology is the SOCRATES computer code, which evaluates the risk impact of changes to AOTs and STIs.

The EPRI approach and the SOCRATES code were applied at Commonwealth Edison's (CECo) Lasalle Station and Georgia Power's Plant Hatch, both BWRs. At Lasalle, after a comprehensive review of the Tech Specs, three key "problem" TS were selected for further evaluation by the EPRI methodology. As a result of the analysis, special testing requirements for the emergency diesel generators were relaxed, a temperature trip setpoint in the main steam tunnel was eliminated and a realistic AOT for the scram discharge volume vent and drain valves was established. At plant Hatch, the methodology was applied to evaluate multiple AOT/STI trade-offs. The emergency core cooling and containment heat removal systems were analyzed and the results indicated that it is possible to extend 24 STIs/AOTs if 3 STIs/AOTs were made more restrictive. The combination significantly reduces plant operating costs while maintaining an equivalent level of safety.

Several utilities have actively been involved in risk-based modification of their TS. For instance, CECo's Byron plant was successful in demonstrating that extending most equipment AOTs from 3 days to 7 days is not detrimental to safety. Northeast Utilities' Millstone-2 plant also successfully demonstrated that extending the auxiliary feedwater pump AOT from 2 to 7 days results in a negligible risk increase and Virginia Power's North Anna plant proved a similar conclusion for one loop of their service water system.

However useful and significant, these "line-item" TS improvements are somewhat limited in their scope of applications. A more general approach is needed which should take advantage of recent developments both in improved understanding of risk and success path analyses and in advances in the field of expert systems. Currently EPRI, in cooperation with Pacific Gas and Electric Co. (PG&E) and Westinghouse Electric Corp. (WEC), is seeking to develop the specifications of an IRA. The concept is explained later in this paper. However, it is important first to recognize the key institutional and technical challenges that risk-based methods could face.

2. Challenges faced by risk-monitors

The broad use of risk-based TS in controlling plant operations marks a potentially significant step in enhancing the flexibility and safety in plant operations. However, a number of obstacles are present which, if not

properly addressed, could prevent successful implementation. These obstacles can be generally classified into two major categories: 1) institutional; and 2) technical. Institutional issues involve the difficulties in incorporating RBTS into the operating and regulatory environments. These are probably the most significant obstacles. Technical issues involve the specific technical challenges associated with using a PRA model to support operating decisions.

2.1 Institutional Obstacles to the Implementation of a Risk Monitor

Over the past ten years, nuclear power plant risk analysis techniques have made possible significant improvements in our ability to model, understand, and improve overall plant safety. One of the products of these efforts has been the identification of plant risk contributors. Of particular importance has been the understanding that the current technical specifications are sometimes inconsistent with these risk contributors. With the advent of these insights, there has been much interest in improving TS through the use of risk-based techniques. However, before embarking on the development and implementation of a RBTS monitor, it is useful to understand and acknowledge the major institutional obstacles which are presented by such an endeavor.

2.1.1 Conflict Between Licensing Basis and Risk Basis

Nuclear power plant design bases are fundamentally based on the assumption of initiator plus worst single failure (i.e., defense in depth). For any given initiator, regardless of likelihood, and any given single failure, regardless of likelihood, the plant should be designed to prevent core damage. In risk-based evaluation, the likelihood of various initiators and subsequent failures is explicitly addressed and accounted for. Thus, an event which is a limiting design basis event may be a minimal risk contributor. In fact, past PRAs have demonstrated this. The current TS were also based on this same philosophy, although additional considerations such as transients have been factored in. Nevertheless, the adoption of a fully RBTS monitor would most probably conflict with the licensing basis for the plant.

An excellent example of such a situation was presented to the NRC Industry Working Group. This example involved a comparison of current TS requirements on various BWR safety systems in light of their risk significance in a plant-specific PRA. The results of this evaluation showed that the low pressure core spray system (LPCS) had very little risk significance and could be removed from service nearly indefinitely without significantly impacting the plant's overall core damage frequency. Thus, a system required in the licensing basis of the plant to mitigate a design basis event (i.e., large LOCA), would be largely uncontrolled by a RBTS monitor.

Due to the realistic and integrated nature of PRA techniques, it is not surprising that such conflicts between the design basis and the risk profile would occur. There are many potential contributors to such situations:

- The realistic success criteria used in PRAs sometimes eliminate controlling conservatisms found in design basis evaluations.

- The crediting of systems or components in non-design basis conditions.

- As mentioned above, the accounting for the likelihood of events can virtually eliminate some design basis challenges (i.e., LOCA plus loss of off-site power) as risk contributors.

This conflict between the plant design basis and the calculated risk basis may present a significant impediment to the implementation of fully RBTS. Not only would the regulators have to fundamentally alter their evaluation of operational and design improvements, but there may also be legal obstacles to this approach. (The British ESSM system has not been faced with this same obstacle, because a risk basis analysis was used in licensing the plant).

2.1.2 Compatibility With Plant Culture

Currently, plant operators evaluate the acceptability of plant configurations based on a set of well-defined limits. Along with each of these limits is a description of the basis for the limit so that, if the operator questions the basis, the necessary information is provided for interpretation. With a RM, the bases, assumptions and explanation are buried in the software of the monitor. The operator is not provided with any information, other than the conclusions. This is likely to make plant operators uncomfortable until some confidence is developed in the tool. There is no way of knowing how long the integration process may take, but it is certain to be significant due to the magnitude of the change required on the part of the operators.

2.2 Technical Obstacles to the Implementation of a Risk Monitor

While risk analysis techniques have significantly improved over the past decade, the results of plant risk assessments are still subject to a great deal of uncertainty and, in some cases, technical disagreement among experts. Both the absolute value of the overall core damage frequency and the associated uncertainties need to be interpreted with great caution.

One proposed version of the risk monitor would use the absolute value of the plant core damage frequency directly in the evaluation of plant configurations and would directly influence plant operating decisions based on this uncertain value. Even if relative risk increments are used as measures, model uncertainties would have to be sufficiently reduced to prevent them from overshadowing such incremental risk. While it is acknowledged that wide implementation of a RM is many years away, and risk analysis techniques are bound to improve during that time, several key aspects of risk analysis will be very difficult to make precise:

- Human reliability analysis

- Common cause failure treatment

- External event impacts

- Failure rate data

- Event sequence success criteria and thermal hydraulic performance

The ESSM system used in the U.K. appears to have largely avoided or minimized many of these problems by focusing the RM concept on a single plant function (i.e., heat removal). It should be recognized that the expansion of such a monitor to a full plant risk model increases the complexity by orders of magnitude. These factors make it difficult to envision the development of a full plant, real-time RM in the foreseeable future

The technical obstacles facing the development of a RM concept can be categorized into two general classes for the purposes of discussion: 1) configuration management issues; and 2) configuration evaluation issues. The first category primarily involves those technical issues influencing the development of software or tools necessary to implement and maintain a RM concept. The second category involves the technical issues which are faced in attempting to use PRA tools in evaluating plant configuration for the purposes of making operating decisions. The following sections provide a more detailed discussion of each of the specific issues.

2.2.1 Configuration Management

In this context, configuration management involves the technical aspects of the monitoring, control and regulation of the plant RM. The following major technical issues are involved:

- Tool design: there are many possible approaches to the development of the monitor including the incorporation of all BOP and safety system components, treatment at a system or sub-system level such that the operator must evaluate which sub-systems are affected, and others. This approach must be defined and evaluated by operating personnel prior to the monitor development.

- Fidelity: The RM must represent the actual plant configuration with a certain level of accuracy. Since infinite fidelity is not practical, tolerable deviations and simplifications would have to be agreed upon and standardized. Thereafter, periodic upgrades, reflecting design or procedures modifications have to be carried out. Criteria would have to be generated to separate those modifications to be incorporated from those not to be incorporated (i.e., filtering process).

- Regulatory review: as this RM will be used to make decisions which will influence public health and safety, one of the important issues which must be factored into the design of the monitor is a means for regulatory review of the risk model as well as a periodic review of the plant configuration inputs to the monitor.

2.2.2 Configuration Evaluation

The assessment of the risk profile requires the evaluation of the plant configuration at a given point in time to determine the instantaneous level of plant risk. The issues associated with the development of a configuration evaluation tool are significant. Some can be simply resolved by some small amount of additional research, others will require substantial long-term interaction between the regulators and industry. The most significant of these issues are:

- Human Reliability Analysis: In addition to general weaknesses in quantifying human reliability, shortcomings in this topic not only include errors of commission which, to date, have barely been investigated, but also the totally unchartered territory of "latent errors" which might play an important role as event initiators.

- Common Cause Failure (CCF) events: The existing generic database is minimal and the methodology for adapting it to plant specific analysis is subject to considerable engineering judgment.

- External Events: Studies have shown that some of these intiators (fires and seismic) could contribute more than half the total core damage frequency. It thus appears important to include them in a RM. Yet, these studies are often controversial because lack of good fire and seismic models and lack of adequate initiating events database force very conservative assumptions on the analyst.

- Component Failure rate database: Even the Component Reliability Parameter System (CRPS), the most complete database available, contains many "holes" in both component types and failure modes. Although it is deemed adequate for many applications, including Individual Plant Examinations (IPEs), it may be insufficiently accurate for a RM (see discussion on uncertainties above).

- Initiation of events: RM should consider the potential for initiating a plant challenge either due to maintenance initiating a plant transient or by requiring shutdown of the plant.

  This relatively new concept may become a major element of any Risk Based Tech. Specs approach since it establishes the trade-off between the risk of, say, extending a component allowed outage time and the risk inherently associated with the transition process from full power to hot standby or cold shutdown. This is particularly true if the component in question is needed for the operation of the Residual Heat Removal (RHR) system.

- PRA models: PRA modes have advanced significantly over the past ten years in their ability to reflect realistic plant performance. However, a number of aspects of PRA modeling may not be compatible with a real-time RM, without further development. These include:

  - Success criteria
  - Scope of PRA model

- Definitions: the use of a RM will require a much broader application and interpretation of system operability requirements. The term operability (or conversely the term "inoperable") will need to be further defined before a RM can be effective.

- Quality assurance: the control of the quality of the RM will be an essential element of its success as a TS alternative. In particular, the quality assurance of the model, assumptions, software and data are significant.

- Criteria: the criteria used in developing and evaluating the RM are fundamental to its success. The two key criteria issues involve: 1) the risk measure used in the RM (e.g. core damage frequency, release rate, fatalities, etc.) and 2) the risk criteria used in interpreting the results (i.e. the magnitude).

- Long-term management of a RM: the proper management of a RM after it has been implemented needs to be further evaluated. Two aspects are of particular importance:

  - Validation of assumptions
  - Maintenance of the models

All of these obstacles may be overcome eventually. However, significant changes may be required in the operation, analysis and regulation of plant operations for this approach to be successful.

3. The EPRI/PG&E/WEC Program

By contrast, the EPRI/PG&E/WEC program does not start with the premise that a real-time RM is a cost effective solution at this time.

A major goal of the program is to develop an IRA to assist plant operators and management in their in their regulatory compliance as reliance on RBTS increases. The envisioned characteristics of the IRA are discussed below. The program is divided into three phases. The first phase is intended to scope the problem and to ensure that the characteristics of the IRA are consistent with utilities needs and their operating philosophies. This phase will also explore applications of the "flexible" TS concept which could be a major element of the IRA.

The second phase will concentrate on defining the specifications of the IRA and the third phase will oversee its actual implementation and demonstration.

3.1 Utilities Interviews

As a crucial first step, the project team has embarked on a series of interviews with five representatives US utilities. The interviews will be conducted at the plant site with a team of senior utility staff knowledgeable in the areas of operation, maintenance, licensing, TS, regulatory compliance, PRAs, and training. The interviews will cover current problems with TS, and a cost-benefit review of various RBTS approaches used within the industry , including IRA and RM concepts. A major outcome of these interviews, scheduled to be completed in July 1990, will be a well-defined set of utility needs that could be incorporated in the IRA.

3.2 Flexible Technical Specifications

A second objective of the project is to develop the concept of flexible TS, or "flex-specs". Flex. specs would provide pre-planned, well-defined alternatives regarding required actions when the plant is operating in a degraded state. It will build upon the new standardized Tech. Specs (e.g. MERITS) currently developed by industry and reviewed by NRC. As an example, equipment AOT may be extended provided that:

- The surveillance frequency of backup systems is increased during the extended AOT (e.g., if HPI pump A must remain out of service beyond the normal 72 hours, then check or test HPI pumps B and C every X hours.); or

- Steps are taken in the procedures to increase operator awareness during these extended periods, and additional operator actions have been identified that would mitigate consequences of certain classes of accidents; or

- Alternate systems have been identified which can fulfill the same function as the out-of-service system (e.g., using some risk criteria a cross connect diesel-generator from sister unit would allow extending AOT from 72 hours to 91 days if one diesel is inoperable and from 2 hours to 91 hours if two diesels are inoperable.); or

- Other risk-compensating measures are identified for specific TS limitations.

Clearly, the flex specs concept further connects system reliability, component availability and testing intervals requirements. The complexity thus introduced may become an additional burden to the plant operator unless adequate tracking tools are also made available. The IRA is such a tool. One of its purpose is to provide assistance to the operators in identifying options. The IRA will, most likely, <u>not</u> compute a "risk" at every instant. It will not necessarily have the capability to determine whether putting a given piece of

equipment out-of-service will increase the plant risk or whether it is better to postpone a given maintenance activity. The IRA will, however, provide valuable information along the lines described in the following section.

4. Characteristics of an Integrated Risk Advisor (IRA)

It is important to stress the modular aspect of the IRA concept. These characteristics need not be considered as a bundled package. Rather, each utility may choose those characteristics that would best support its operating philosophy and discard the others. The IRA should also have the flexibility to allow each utility to add its own IRA functions within the given software environment. Potential characteristics of an IRA are discussed below.

4.1. Identifying Pre-defined Options for Flexible Tech Specs.

Methods are currently being developed, for certain classes of TS that would allow a more flexible definition of the Limiting Conditions of Operation (LCO) requirements (see section 3.2). For example, the operator may be allowed to extend the AOT of a charging pump if additional surveillance is performed on a redundant charging pump. In some cases, several options may be available. The IRA would identify the available (pre-defined) options and provide the basis for each option.

4.2. Tracking Availability of Mitigating Equipment

Inoperable support systems may impact the operability of other support systems and/or front line systems. The IRA would be able to identify alternative equipment which can be used in-lieu of the unavailable systems. Using dependency matrices, the IRA would be able to identify the exhaustive consequences of a malfunction or of a maintenance action leading to temporary removal of equipment from service on LCOs.

4.3. Tracking Systems Reliability Targets

In order to establish the risk basis of certain categories of TS, certain assumptions must be made regarding the reliability of support systems. The IRA will include complete information regarding these assumptions. The IRA will track these systems and evaluate their actual reliability relative to the assumed one. In case of a projected shortfall, the IRA will provide an early warning to the operator so that the faulty systems are more closely watched for the remainder of the cycle.

4.4. Assisting Operators in Monitoring Compliance With LCO's

This function may be particularly useful when several AOT/STIs have been interconnected through a risk analysis (trade-offs). For example, at Plant Hatch, 24 AOTs and STIs were identified for relaxation on account of three others that were tightened. Should one of these tighter STI or AOTs be candidate for relaxation in the future, the IRA will identify the connection with the 24 others and the trade-offs would have to be reanalyzed.

4.5. Identifying Needs for PRA Configuration Control

RBTS require certain assumptions concerning system configuration and reliability databases. These assumptions are usually incorporated in a PRA which is used as the computational basis for modifying the TS. As plant configuration changes because of hardware modifications or procedure changes, or as reliability data from key components evolve, there may be a need to revisit the PRA. The IRA will process the plant changes and the reliability databases periodically and warn the operator when the magnitude of the change is sufficiently large to trigger a reanalysis of the TS basis.

4.6. Integrating with Reliability Centered Maintenance (RCM) Program

As RCM programs gain acceptance in the nuclear industry, it is possible to consider building an RCM database that would lead to "experience-based TS". The basic point here is that RCM will provide an improved knowledge of failure modes and mechanisms. If repeated surveillance tests indicate that certain theoretical failure modes do not exist in practice, then the affected TS can be simplified accordingly. The IRA would be used to track the failure modes of importance to TS.

5. Conclusions

As RBTS are gaining wider acceptance, the U.S. nuclear industry is looking beyond the "line-item" applications. Several concepts have been proposed and are being evaluated. This paper discusses some of these concepts.

The real-time RM has tremendous appeal but, upon closer examination, appears complex to develop technically and even more difficult to implement institutionally.

The flexible TS concept provides an incremental way to expand beyond the current state-of-the-art. The main appeal of this concept is the ability to take greater advantage of all available equipment at the plant to exit from an LCO, provided careful analysis is done beforehand.

Finally, the preliminary concept of an IRA has been described. The IRA is a modular computerized "tool box". It will integrate many tools that could assist the operator in maintaining compliance with TS. The IRA goes well beyond merely tracking compliance. It also performs an active function of tracking reliability, availability, AOTs and STIs, PRA configuration control, and failure modes.

STATUS OF PSC AND TECHNICAL SPECIFICATIONS IMPROVEMENTS BASED ON PROBABILISTIC METHODOLOGY

S. VOLKOVITSKIJ
Science and Engineering Center for Safety
in Industry and Nuclear Power,
USSR State Committee for Supervision of Safety
in Industry and Nuclear Power,
Moscow, Union of Soviet Socialist Republics

Abstract

In 1990 three supporting probabilistic indicators were included in the new version of the USSR main regulatory document "General Rules of Ensuring Nuclear Power Plant Safety". The series of guidelines for conducting PSA is under development. The nuclear regulatory body encourages the practical use of PSA methodology both for NPP design and operation. Two examples of the use of probabilistic methodology for technical specifications assessment are described. It is stressed that the regulatory body consideres probabilistic methods as an important but supporting tool for making regulatory decisions.

INTRODUCTION

Founded a few months ago USSR State Committee for the Supervision of Safety in Industry and Nuclear Power (SCSSINP) is a regulatory body fulfilling the state supervision of nuclear and radiation safety of Nuclear Power Plants (NPP). Formerly these functions were layed upon the now abolished USSR State Committee for the Supervision of Nuclear Power Safety. Science and Engineering Center for Safety in Industry and Nuclear Power (SECSINP; hereinafter, Centre) promotes the science and engineering support of the USSR regulatory body (Fig.1).

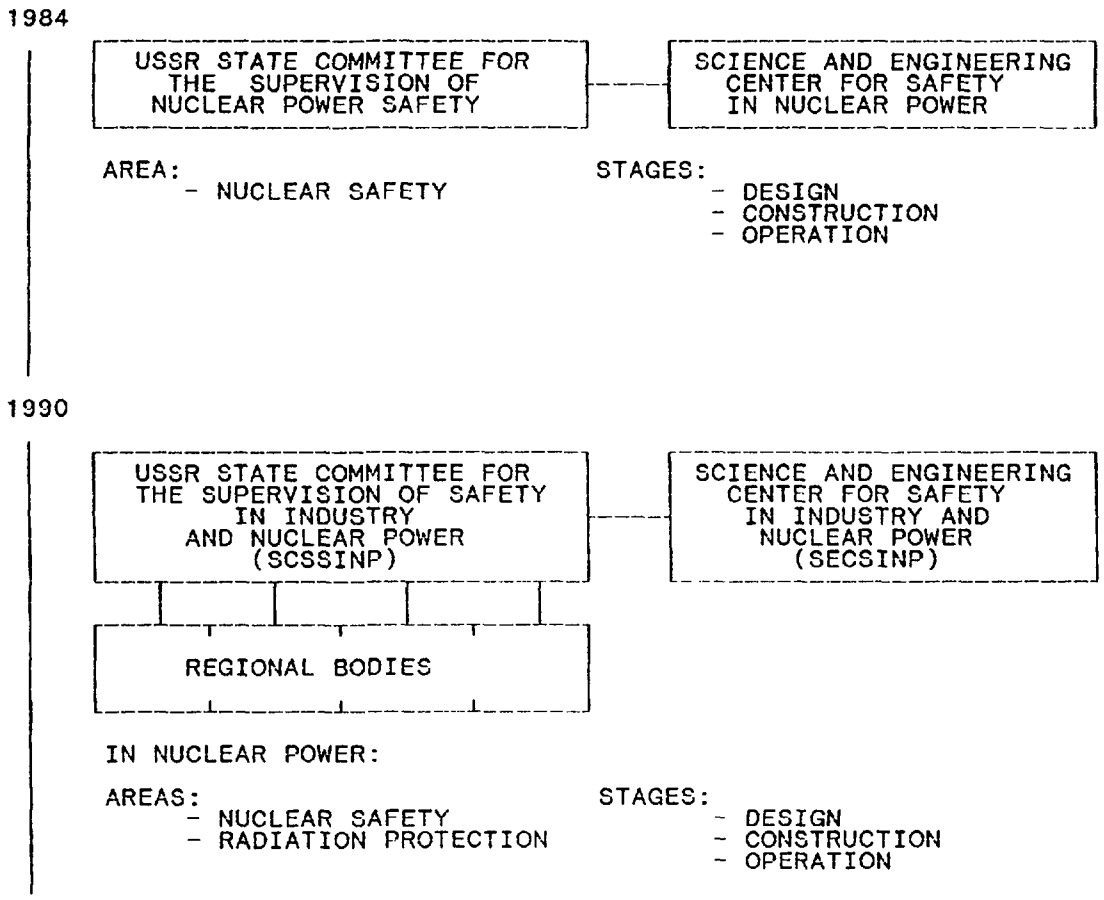


Fig. 1

SCSSINP'S ACTIVITY IN PSA

The next point validates the recognition in the Soviet Union on the regulatory level the role of the probabilistic methodology as a tool for Nuclear Power Plants safety assessment. The revised version of the main nuclear regulatory document in the USSR "General Rules of Ensuring Nuclear Power Plants Safety" (so called OPB-88) comes into action from the 1st July 1990. This document reflects many features of the Basic Safety Principles for Nuclear Power Plants developed by the International Nuclear Safety Advisory Group (INSAG-3). OPB-88 is based on the deterministic approach to the Nuclear Power Plant safety, but for the first time in the Soviet regulatory practice it containes probabilistic indicators. These probabilistic indicators conditionally may be called "criteria", though they are considered as goals. But they will be taken into consideration in regulatory activities and assessment of the design and operating safety levels.

The criteria are as follows:

1. THE PROBABILITY OF RADIOACTIVITY RELEASE, WHICH DEMANDS EVACUATION OF THE POPULATION BEYOND THE PREDETERMINED DISTANCE, MUSTN'T EXCEED 1.10-7 PER REACTOR PER YEAR (RY)

2. THE PROBABILITY OF SEVERE CORE DAMAGE OR CORE MELT DURING BEYOND DESIGN BASIS ACCIDENTS MUSTN'T EXCEED 1.10-5 PER RY

3. THE DESTRUCTION OF REACTOR PRESSURE VESSELS MAY BE DELETED FROM THE LIST OF DESIGN BASIS INITIAL EVENTS IF IT'S SHOWN THAT THE PROBABILITY DOESN'T EXCEED 1.10-7 PER RY

We believe that establishment of probabilistic indicators will influence the process of development and analysis of technical specifications for new generations of Nuclear Power Plants. As a matter of fact it initiates the development of a multy-level system of probabilistic safety cryteria. Presently, research is in progress to establish a number of system-functional level criteria which directly formulate the requirements for safety functions and reliability indicators of most important safety systems. This is due to peculiarities of NPP design, construction, and operation system in the USSR, and by the socio-political atmosphere after the Chernobyl accident.

Late some R&D organisations in the USSR have been actively developing methodology of the NPP probabilistic safety assessment, creating tools and conducting practical works in PSA for new designs and operating plants. In order to streamline and adjust the whole PSA process and to promote nuclear safety the SCSSINP recognized a necessity to develop appropriate methodological basis and norms for conducting PSA. Now the Center is preparing a series of guidelines. In this work it largely benefits from participation of specialists in the IAEA PSA Guidelines Programme.

Besides norms and regulations the SCSSINP promotes the practical use of PSA methodology by personnel of operating NPPs. For this purpose after the IAEA training courses for safety analysts in all aspects of PSA held by Agency in the

USSR in Nowember 1989 the Center organized similar courses for nuclear power plants personnel. At present the practical work on use of PSA methods is organised for assessment of various operating plant safety aspects of Zaporozhje NPP (VVER-1000) and Kola NPP (VVER-440) in operation as typical representatives of mentioned designs. The first preliminary results are expected in 1991 and the total schedule covers a few years. One of the main purposes of this work is assessment and improvement of the plant technical specifications including allowed outage times, maintenance strategy, optimization of surveillance testing intervals for equipment and systems important for safety.

To be more specific on the practical use of the PSA methodology to analyse technical specifications, two examples follow.

During 1989 - 1990 the task force of "Atomenergoproekt" (design organisation) headed by Dr. Y.Shvyriaev carried out the safety systems reliability analysis for two units of Kola NPP to validate the repair-and-maintenance schedules. On the basis of operating reliability data of system components the strategy and allowed outage times for one of three safety system trains during reactor operation were investigated as well as their influence on safety functions performance.

These safety functions are to:

1. maintain the reactor sub-criticality
2. maintain primary reactor coolant inventory
3. remove core decay heat and stored heat via the secondary circuit at high and low pressure in the primary circuit
4. remove heat from containment
5. scrub radioactivity from containment atmosphere

Both front line and support safety systems (Service Water System, Emergency Electric Power Supply Systems) were analysed but without account of personnel errors during maintenance. The effect of initial data uncertainties was also analysed. It is

concluded that the increase of one of the safety train repaire time from 24 to 72 hours factually does not effect the reliability of safety functions fulfilment, given an extraordinary test of the other two trains are carried out and their availability is confirmed.

The second example of the probabilistic methods use is a series of investigations conducted in the Kurchatov Institute of Atomic Energy and the Center to study probabilistic indicators of the VVER and RBMK reactor primary circuit components failure taking into consideration various factors including radiation effects, nondestructive control and periodic testing. The methodology is presented in Ref.[1]. It is based on solving the problem of structural element defects kinetics with an account of statistical uncertanties in initial defects dimentions and mechanical properties of materials. The solution allows to determine the probabilities of different type failures on different operating regimes. To evaluate crack-resistance of different structures several failure models are used: brittle, brittle-ductile and ductile as a function of mechanical properties (Ref.[2]). This method was used for probability assessment of the advanced VVER-88 reactor pressure vessel destruction. Considering real data on defects distribution in reactor pressure vessel welds of VVER-1000 in operation and after radiation defects annealing when the fragile critical temperature reached 180 degrees Celsius the following assessments were made. For a wide range of design basis and accidental operating conditions including enhanced cooling-down and noncontroled temperature fall to 200 degrees Celsius, small and large LOCA, the probability of large-scale VVER-88 reactor pressure vessel rupture varies within (0,02...5)10-6 per RY, the upper limit probability of large LOCA being 1.10-4 per RY. Maximum size of vessel leakage is evaluated as equivalent to 60 mm diameter, and the probability of leakage less than 60 mm lies within the range of (0,2...30)10-5 per RY. The calculations have shown that hydropressing, as a means to initiate cracks of substantial dimensions, is an effective tool to test the vessel defect structure and consequently to lower the probability of its brittle failure in operation. An increase of frequency and

decrease of hydrotesting temperature allow to obtain any reduction of failure probability. The current quantitative estimations may be considered as preliminary ones since the methodology is still being developed.

In general the very task to esteem probability indicators for reactor circuit components failure on the one hand is closely related with the need to evaluate objectively times-to-failure of reactor pressure vessels and the effectiveness of measures to extend lifetimes of the plants. Reactor vessel annealing is one of them. On the other hand this task is connected with the need to evaluate accident initiating events frequency. The latter is reflected in the OPB-88 criterion of accounting failure of reactor pressure vessels and other vessels as initiating design basis accidents events.

It should be noted that presented examples are intended only to illustrate existing areas of research aimed at improving technical specifications of nuclear power plants. But the USSR regulatory body hasn't received yet official requests on making changes in tecnical specifications based on probabilistic methodology.

In conclusion it should be stressed that SCSSINP considers all attempts to implement of reliability and risk methodology for analysis and improvement of technical specifications of NPP to be useful and promotes these activities in research and design organisations and by NPP personnel. But, as in the past, in the near future the regulatory body will make regulatory decisions mainly on the deterministic basis.

REFERENCES

1. Tutnov A.A., Tkachev V.V. Estimation of Probability of Pressure Vessel Fracture Start in Power Plants. Atomic Energy, Vol 64, No.3, March 1988.

2. Karpunin N.I., Tkachev V.V., Tutnov A.A. Probabilistic-quantitative Assessment of Pressure Vessels Failure. In: The Reliability of NPP Pipes and Highe Pressure Vessels. Transactions of the Obninsk Institute of Atomic Energy. Obninsk, 1989. (In Russian).

(Карпунин Н.И., Ткачев В.В., Тутнов А.А. Количественно-вероятностная оценка опасности разрушения корпусов. В сборнике: Надежность трубопроводов и сосудов высокого давления АЭС. Сборник научных трудов. Обнинский институт атомной энергетики, Обнинск, 1989).

ALLOWABLE OUTAGE TIMES (AOTs) AND SURVEILLANCE TEST INTERVALS (STIs) REEVALUATION BY PRA PROCEDURES

V. SERRADELL GARCIA, S. MARTORELL ALSINA,
G. VERDU MARTIN
Departamento de Ingeniería Química y Nuclear,
Universidad Politécnica de Valencia,
Valencia

M.T. VAZQUEZ, J.I. CALVO
Consejo de Seguridad Nuclear,
Madrid

Spain

Abstract

In the early 1980s, several tools for AOT and STI evaluations by PRA procedures were developed. Most of them have been implemented into program codes. Some of these tools were developed before 1980 to assess Plant Safety from a risk point of view (PRA level 1).

The main objective of the paper is to show how the above presented tools can be used in an AOT and STI evaluation program. An analysis scheme is exposed, stressing the most important topics related to qualitative and quantitative analysis. In the last one time-dependent or independent risk evaluation has been considered separately.

Fault and event trees are obtained through the qualitative analysis, and minimal cut set generated to be used in the quantitative analysis. By means of time-independent quantitative analysis a time-independent risk estimation is obtained. Furthermore, the most important STI and AOT requirements are identified using important measures. Also, some sensitivity and uncertainty analysis are performed. The time-dependent analysis uses the results from previous qualitative and quantitative studies. The analysis is specially useful to accomplish with AOT and STI reevaluation because of the time-dependence of these requirements. Additional sensitivity analysis lead to review test and maintenance influence on risk, in order to confirm results from AOT and STI evaluation and are related to: hypothesis and models, data, human error and common cause failures.

At the end of this paper a case of application with the corresponding results of whole analysis is presented. The case of application analyses the benefits of the alternate strategy testings: staggered or sequential for various surveillance test intervals. Furthermore, additional calculations were performed to investigate the sensitivity of the results to the input used. In particular, we study the impact on system unavailability when the time-related (standby) failure fraction varies from 0 to 1 (all functional failures are demand-related or all of them are time-related).

---

1. Background.

From early, at the beginning of using nuclear energy, it has been paid special attention to look for safe operation of nuclear power plants. Several proposals have been exposed to quantify the plant safety. These proposals aimed to define tools that allow to identify and limit the main contributions to the plant unsafeness.

Up to now, engineering judgements have been adopted to limit the occurrency of events that going against public and professional people health or, done them, to minimize their impact. However, several historical milestones have lead to improve the safety evaluation. The term "nuclear risk" was introduced and thus new methods using probabilistic assessments were developed. Some of them are known as Probabilistic Risk Analysis (PRA).

Technical Specification are also related to plant safety and therefore they should be evaluated from a risk point of view. To accomplish with that more recently, from the early 80's, several tools for AOT's and STI's evaluation (included into Techs. Specs.) by PRA procedures have been developed or adapted. Some of these tools had been developed before 80's to assess the Plant Safety from a risk point of view (known as PRA level 1, exposed above). At the same time, some of them have been implemented into program codes that can be used to accomplish with specific topics into the risk analysis related with AOT and STI requirements (fault and even trees construction, measures of importance analysis, time-dependent or independent system unavailability evaluation, sensitivity studies, etc...).

Late in 1987 the Spanish Council for Nuclear Safety started a Technical Specification Analysis Program called "APET" that has been carried out by the Nuclear Engineering Department at the Polytechnic University of Valencia (SPAIN). The APET program was aimed to study developed methodologies and their scientifical basis that were related to probabilistic analysis of Techs. Specs.. Finished this first stage, since early in 1989, the second phase of the APET program has been aimed to apply above methodologies on three nuclear safeguard systems, looking for extracting general results to be used beyond in others nulear system analysis.

The main objective of this paper is to present the above mentioned tools and how they could be used in an AOT's and STI's evaluation program. A scheme for the analysis is exposed (Figure 1), stressing on it the most important topics related to AOT's and STI's reevaluation. Several steps into the scheme are related to qualitative and quantitative analysis.

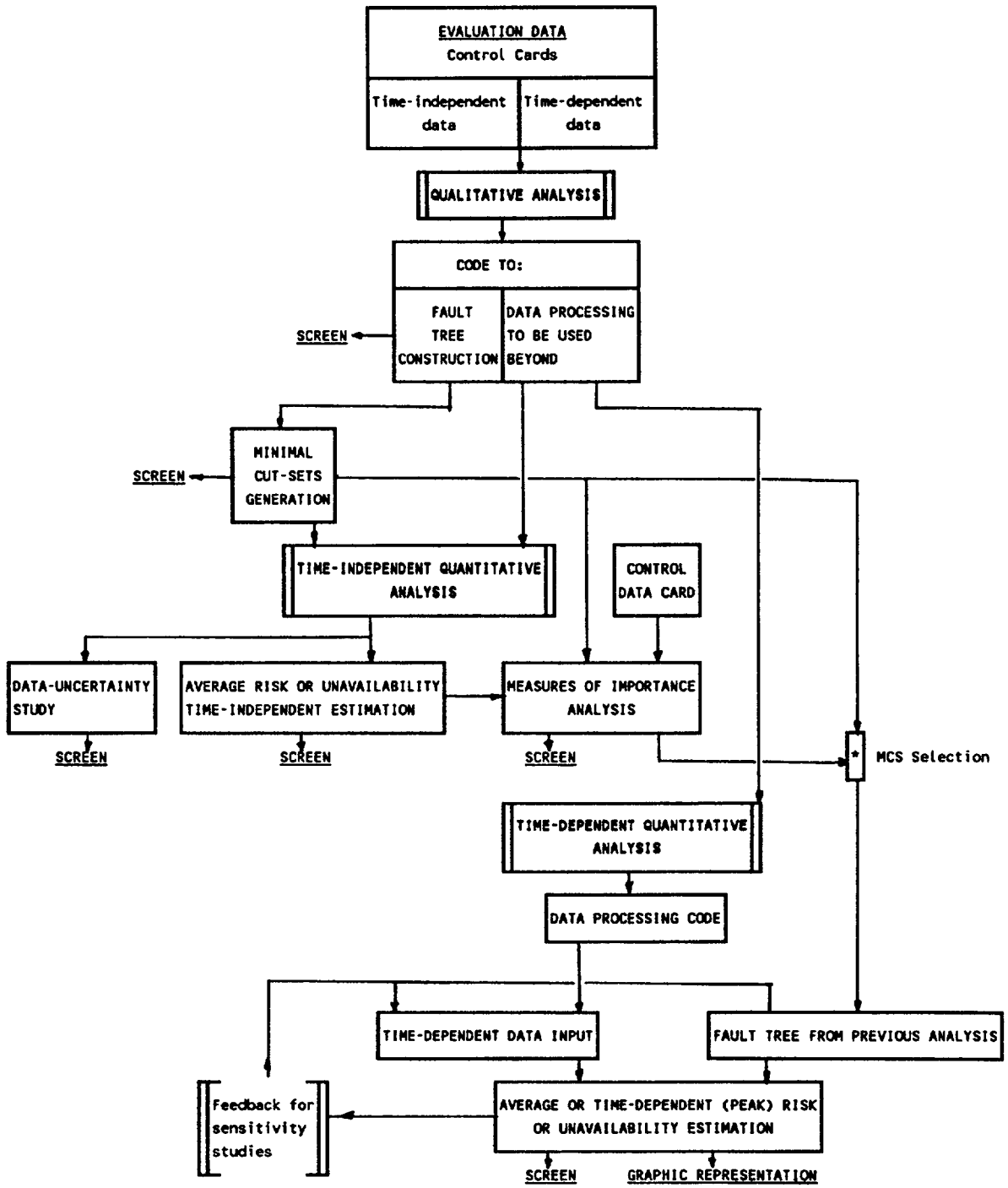


Figure 1. Scheme for AOT's and STI's analysis by PRA procedures

Sensitivity analyses have been identified to be necessaries to accomplish with whole AOT and STI reevaluation program in order to verify postulated hypothesis.

At the end of this paper a case of study with corresponding comments and final conclusions are presented.

2. Preliminary remarks to assess AOT's and STI's requirements.

This paper do not aim to give a guide for an specific AOT's and STI's revision program. But it tries to explain a process to evaluate the risk associated with these requirements, pointing up those topics that more influence the evaluation and that should be taken into account in a revision program. The purpose is to bring together available tools that can be used.

The methodology based on event and fault trees has been adopted as a tool to accomplish with everyone of the focused steps into the process.

Using the above mentioned methodology, two different kinds of studies can be taken into account. The first one, more general, is the start point for the next one. It consists in a probabilistic risk analysis for the plant or safeguard systems. It is known as PRA level 1. The second uses partial results from the first one and it adapts them for the analysis of requirements related with AOT's and STI's.

Often, this second analysis is considered such as a case of application of the PRA methodology. It is not necessary to make the whole first study before going to the AOT's and STI's reevaluation process. However, the experience and information gained in its development is very useful to take next study easier. In many cases, PRA level 1 is available, but it is necessary to adapt it for Technical Specifications analysis. Thus, PRA level 1 fault trees are used for time-independent evaluation; however now, they must be used for time-dependent analysis. So, fault trees should be rebuilt to account for time-dependence on test and maintenance requirements. Also, it is suitable to lump together all independent failure modes of each component with a related test and maintenance requirement, when it is necessary, in a time-dependent analysis such as at present paper.

Qualitative analysis is needed in order to define component failure modes and physical relations among components into the plant (or fault trees) to accomplish with their function when they are required to do it.

Although time-independent models are quite importants in some particular purposes such as it will be exposed below, the time-dependent are the most suitable ones to model AOT's and STI's requirements because they allow to know the plant vulnerability in important instants (test, preventive or corrective maintenances, etc.) introduced by those requirements. With that in mind, several strategies can be adopted to improve it.

3. Scheme planned for the analysis.

In an AOT's and STI's reevaluation process by PRA procedures such as it is studied at present paper, the whole process take into account three sequentially treated parts: qualitative, quantitative analyses and sensitivity studies into the last one. The whole scheme proposed for the analysis is showed in Figure 1.

At first, a qualitative analysis is developed. It consists in defining and modelling the unavailability for those systems involved into the revision process. To do it, fault trees are contructed that express the relationship among component failure or unavailability modes. Depending on the scope for the analysis it could be also necessary to develop partial event trees (or use generic ones) to account for accident sequences where the systems analized are involved. The final result from this analysis must be components unavailability data, the fault trees and their corresponding minimal cut sets (MCS).

Next, the quantitative analysis can be carried out using time-independent or dependent models. Usually both analysis are made (this is the present case).

The time-independent quantitative analysis takes results from the previous qualitative analysis (MCS and related data). Its most important conclusions are derived from data uncertainty studies into the used models and the measures of risk importance analysis. Also, this analysis allows a first estimation for the system average unavailability

or risk included by present AOT's and STI's requirements. This first estimation for the system average unavailability is useful to be used as base case for importance analyses that are carried out in a more realistic way. Measures of risk importance analysis could be considered like a qualitative and quantitative mixed analysis. We adopted the Fussell-Vesely measure for minimal cut sets, and Fusell-Vesely and Achievement worth risk ones for basic events, being the most important ones to be used for AOT's and STI's reevaluation. According to these measures, generated MCS and basic events are ordered from a risk point of view. Fussell-Vesely for MCS is used in order to consider in future analyses only the most important MCS. Fussell-Vesely for basic events is used in order to identify those components which STI's requirement must be mainly reviewed. Finally, the Achievement worth measure is used to identify those components which AOT's requirement must be mainly reviewed. Some sensitivity studies can also be carried out at this point, taking advantage of the lower complexity by using time-independent models, because the lower amount of variables to be handled.

Then, the quantitative time-dependent analysis is carried out. It uses part of the results from the qualitative analysis and takes advantage of the experience gained with time-independent analysis. Thus, previous measures of MCS or basic events importance are considered into the evaluation model. Also, it allowed to focus the most important issues into the revision process. Data processing is also necessary before developing this analysis to do compatibility between both type data used (time dependent and independent). By means of this analysis a second estimation for the system average unavailability and also the time-dependent plant vulnerability (through the time-dependent unavailability) over the base line time are obtained.

Finally, time-dependent models are used for important sensitivity studies related to theoretical models and several parameters modelling component characteristics and Technical Specifications requirements. Because risk evaluations related to AOT's and STI's requirements can be very dependent on hypothesis, models and data used into the analysis, it is seemed necessary to carry out sensitivity studies in order to verify conclusions derived from all previous

analysis. Although these studies can be taken using time-dependent or independent models, it is more convenient the time-dependent one. The sensitivity studies that have been judged to be more interesting are:

. Related to hypothesis and models:
  - Fault tree reconfigurations.
  - MCS truncation.
  - Level for risk evaluation.
  - Risk measure (absolute or relative).
  - Lumped independent failure modes for each component.

. Related to data:
  - Failure rate or demand failure contributions.
  - Test characteristics (override factor, time, test cause failure, reactor trips or transients...).
  - Repair characteristics (mean time, AOT).
  - Preventive maintenance.
  - Surveillance requirements (STI, test strategy, test after failure,...).

. Related to human error.

. Related to common cause failures.

4. Tools implemented into program codes to be used.

Without taking into account set codes that are going to be used, speed and capacity of memory for needed calculations depend on the computer system where they are implemented. Thus, from PC-DOS systems (less resources) to supercomputers can be used as hardware support. At present case, a supercomputer with the standard operating system UNIX has been used. However, such as it is indicated below, a PC-DOS system can be more efficient for developing first steps into the scheme analysis in relation to fault trees construction and data management.

Here, set codes have been adapted for automatic and chained execution. That means that all programs have been modified, mainly their input and output transfers to files. The changes depend weakly on hardware of computer system because a standard operating system, UNIX, is used as software support.

Depending on the kind of analysis needed tools, implemented into codes, are as follow.

Qualitative analysis.

The qualitative analysis is made sequentially in three steps or modules (Figure 2):

- Reliability Data Base Management.
- Fault Tree.
- Minimal Cut Sets.

In the first step, the Reliability Data Base module, we extract reliability data from data bases to be used later (failure rate, unavailability per demand, mision time, test interval, override factor...).

In the second step, the Fault Tree module, we can: construct new fault trees, update or delete existing fault trees, and browse or change their structure. This task is performed by Fault-Tree editors.

Finally, in the MCS module, fault tree reduction and minimum cut sets determination is performed. We have, in this step, the following codes: PREP-MINSET, ALLCUTS, MOCUS or FTAP.

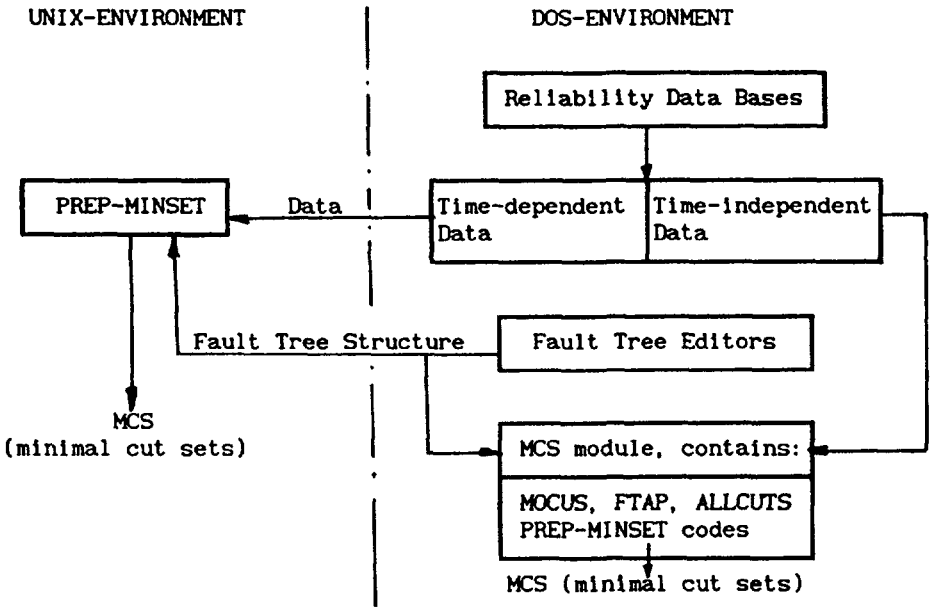


Figure 2. Qualitative analysis

Measures of risk-importance could be focused now between quantitative and qualitative analysis. The IMPORTANCE code, modified, has been adopted to do it. The code includes additional risk measures (achievement worth and reduction risk); also, time-independent study and automatic input-ouput to the other codes. This code has inputs from qualitative analysis (minimal cut-sets and components characteristics) and control data (to select measures of risk importance to be adopted). Additional quantitative analysis might be needed to estimate the system average unavailability or base risk. In this case, time-independent quantitative analysis have to be carried out before. Figure 3 shows such a kind of study. The output from this code are MCS and component order according to risk importance related to reliability characteristics and TS's requirements.

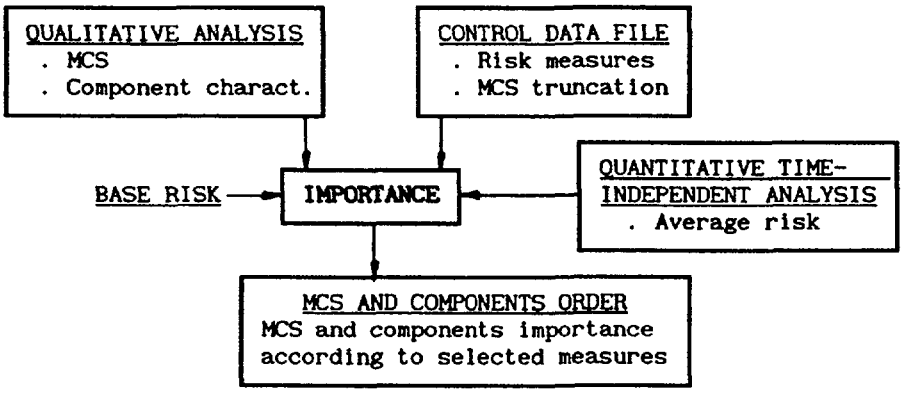


Figure 3. Measures of risk importance

Quantitative time-independent analysis.

Three kinds of time-independent analysis must be made. First and second one use a code for time-independent system unavailability evaluation. The KITT-1 code has been adopted to accomplish with two tasks: average unavailability estimation and time-independent sensitivity studies. Instead of KITT-1, other similar ones like exposed before can be used for these purposes. We have also the MOCUS and FTAP codes, but only in PC DOS operating system. Figure 4 shows inputs and outputs needed.

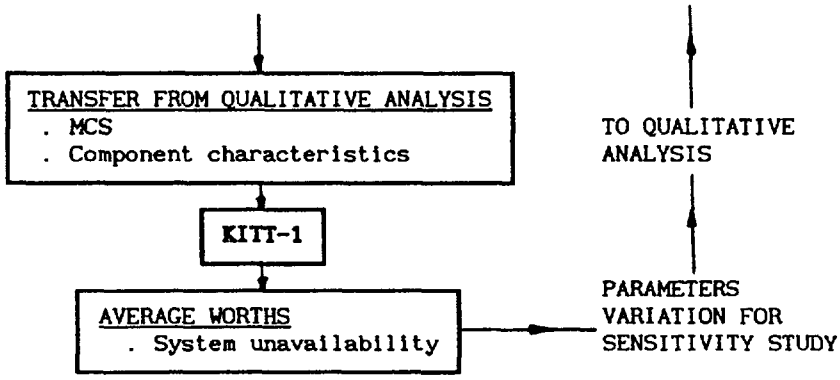


Figure 4. Time-independent quantitative analysis

The third analysis consists in a data uncertainty study by means of the SAMPLE code. MCS and component characteristics together error factors are needed as input. The result includes the average system unavailability and its uncertainty, Figure 5.

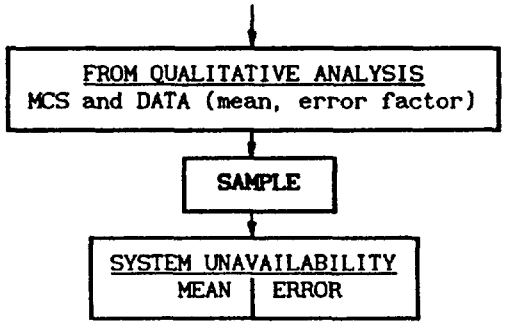


Figure 5. Data uncertainty study

Such as it has previously been exposed, both codes have been modified for automatic execution (automatic input/output transfer).

Quantitative time-dependent analysis.

The FRANTIC-III code has been used to accomplish with time-dependent evaluation, although other codes like SOCRATES can lead this task successfully. This code has also been modified for automatic execution. Before the time-dependent analysis by FRANTIC-III being made, a code for data processing is necessary. Previous analysis use

time-independent data but they are not useful for time-dependent analysis. So, time-dependent data from adequate data bases should be taken out. However, using these new data the results from both time-dependent and independent studies might not be compatibles. To solve this problem the previously handled time-independent data must be used in this analysis. Thus, CALCFRAN code has been developed to adapt previous data to time-dependent data in an automatic execution.

Using these data and the fault-tree (selected MCS and components) AOT and STI reevaluation process using FRANTIC-III can be realized as show in Figure 6. Time-dependent sensitivity studies can also be made by means of these codes.

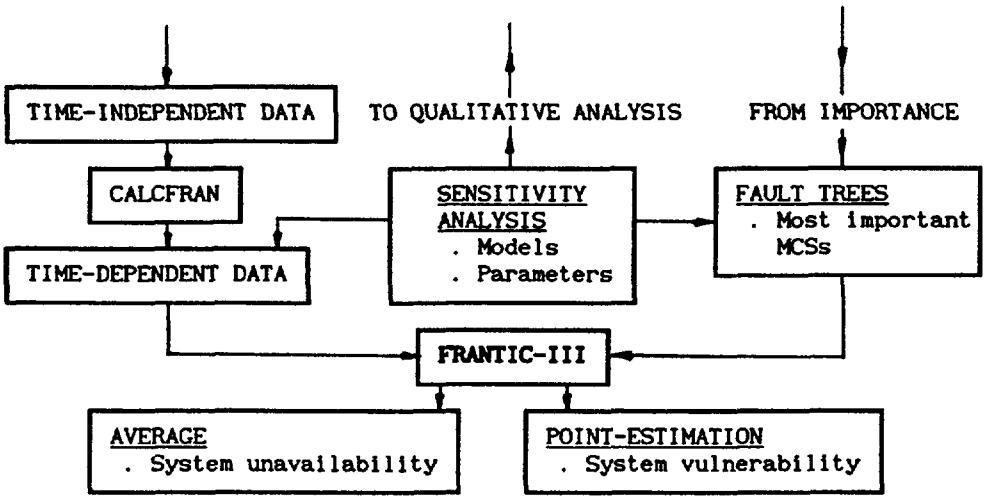


Figure 6. Time-dependent quantitative analysis

5. Case of study.

In evaluating the risks associated with TS's (based on Probabilistic Risk Assesments), the uncertainties must be taken into consideration. The risk evaluations, system, function or core melt evaluations, because of their very nature, are associated with uncertainty. In particular, we focus our attention in data uncertainties, therefore, additional calculations were performed to investigate the sensitivity of the results to the input used.

As we know, the types of component unavailability are:

Time-related failures.

The component failures during the interval between tests represent a component unavailability to perform its function. The unavailability at time t, equal to the probability that a failure will occur before time t, is

$$q(t) \approx \lambda t$$

λ: failure rate

t: time since last succesful test

q(t): point-estimate unavailability

The average unavailability due to time-related failures, over the time between tests, is represented by:

$$q_t = \int_0^T q(t).dt = \frac{\lambda T}{2}$$

Demand related failures.

Each time the component is demanded, it has a probability of failure due to a demand-related mechanism. This probability is independent of the elapsed time since last succesful test, therefore it is independent of the time betwen tests, T. Then,

$$q_d = \text{constant}$$

Test-related.

At each test, a component can be found failed due to either time-related, demand-related, or test-related failures (degradation of a component that requires repair). Therefore, at tests, the component will be unavailable during the possible repair time if a failure is detected

at the test or the time period within the test, in which the normal function of a component is inhibited (override factor). Therefore, we can conclude that standby component unavailability is affected, mainly, in two ways: time-related or demand-related failures.

The analysis presented in this paper is a probabilistic study, where we vary the time-related standby failure fraction, f_s, from 0 to 1.

$$f_s = \frac{q_t}{q_{total}} = \frac{\lambda^* T/2}{\lambda T/2 + q_d}$$

f_s = 0, all functional failures are demand-related.

f_s = 1, all functional failures are time-related.

λ^*, is the new failure rate.

q_{total}, is the average unavailability for the component, obtained from data bases.

We display some results of our study, for a CSS-PWR system, in Figures 7 and 8: "Average Unavailability versus f_s" and "Maximum Point-Estimate Unavailability versus f_s". In the Table 1 we present the relation R(T) and $R_{max}(T)$ for various cases, where:

$$R(T) = \frac{Q_s(f_s=1) - Q_s(f_s=0)}{Q_s(f_s=0)}$$

and

$$R_{max}(T) = \frac{Q_{smax}(f_s=1) - Q_{smax}(f_s=0)}{Q_{smax}(f_s=0)}$$

where Q_{smax} is the maximum point-estimate unavailability and Q_s is the average unavailability of the system.

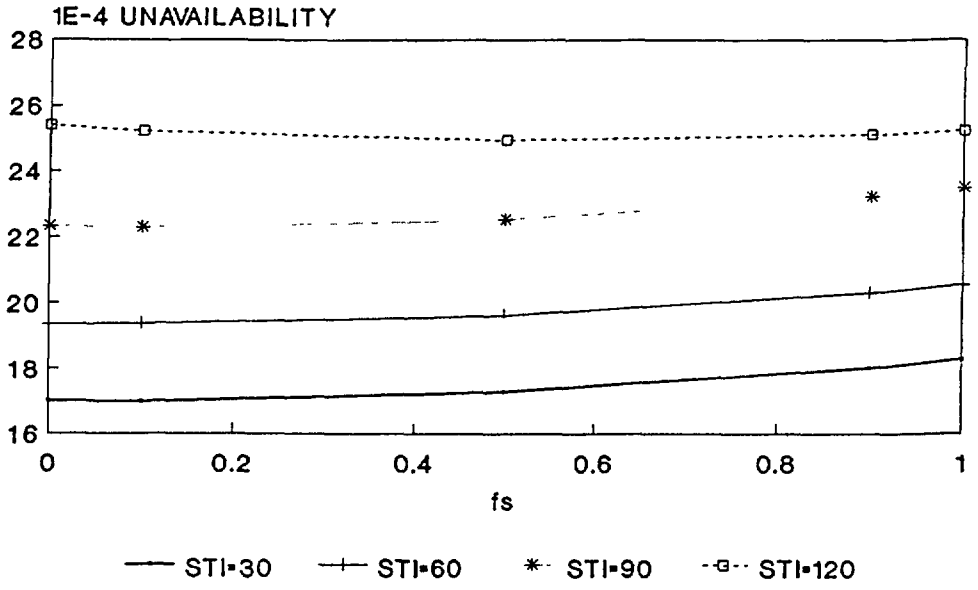


Figure 7. System average unavailability vs f_s

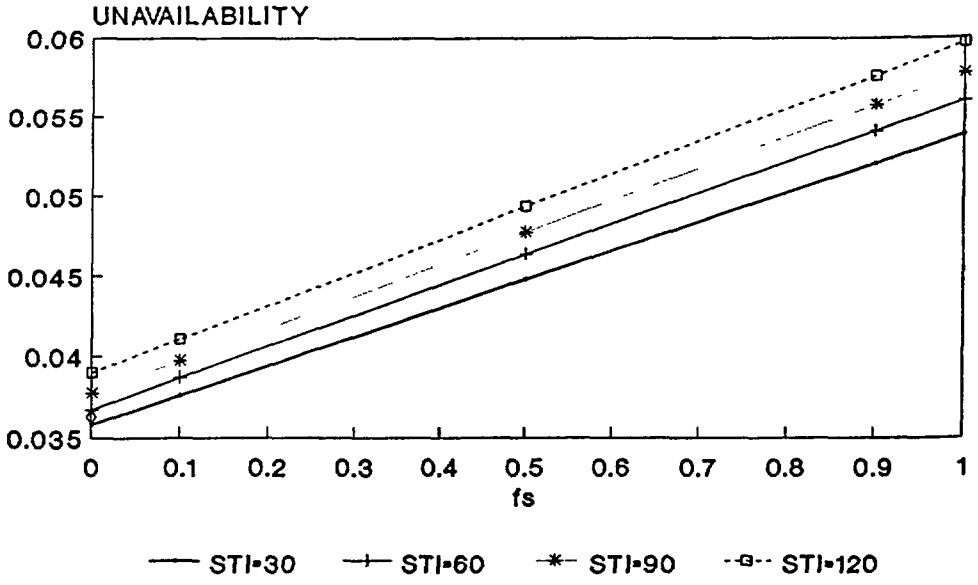


Figure 8. System maximum unavailability vs f_s

Table 1.

STI	Q_s	R(T)	due to failures	due to testing	due to repairs	$R_{max}(T)$
30(days)	(1.70-3)	7.4%	10.14%	4.4%	12.7%	50.33%
60(days)	(1.93-3)	6.15%	7.7%	7.98%	21.67%	52.5%
90(days)	(2.23-3)	5.2%	6.48%	11.88%	28.88%	52.99%

We can conclude that the dependency of the average unavailability system on fraction f_s is not very important; R(T) varies from 5.2 to 7.4 percent, but we observe a strong dependency for the maximum unavailability system (peak); $R_{max}(T)$ varies from 50.33 to 52.99.

Next, we calculate the relative variation on average unavailability systems for the 30, 60, and 90 days STIs, as follows:

$$S_1 = \frac{Q_s(60 \text{ days}) - Q_s(30 \text{ days})}{Q_s(30 \text{ days})} \times 100$$

$$S_2 = \frac{Q_s(90 \text{ days}) - Q_s(60 \text{ days})}{Q_s(60 \text{ days})} \times 100$$

and we obtain:

$$S_1 \approx 12\% \quad \text{and} \quad S_2 \approx 15\%,$$

therefore, if we compare the relative error R(T) related to fraction f_s, with the relative variations S_1, and S_2, we can say for this system, that in STI evaluations, the exactly determination of time related standby failure fraction, f_s, is necessary if we want to accomplish with the STI reevaluation. So, data bases recolection for component reliability data have to be carefully obtained from operational experience in an adequate manner. This is the initial and almost the most important step.

6. Conclusions and comments.

Technical Specifications are related with plant safety and therefore they should be evaluated from a risk viewpoint. In particular, AOT's and STI's requirements into the TS's can be evaluated using PRA methodology. This tool will help engineering judgements to improve plant safety.

This paper do not aim to give a guide for an specific AOT's and STI's revision program. However, it tries to explain a process to evaluate these requirements using PRA procedures. In this way the most important topics that more influence the evaluation are pointed up. They should be taken into account in a revision program together with tools and the scheme used here.

The experience gained in developing PRA level 1 for a Plant is useful when an AOT's and STI's reevaluation proposal is considered. However, part of previous analysis must be adapted for next revision process. Faul trees have to be rebuilt and new data for component reliability included.

In an AOT's and STI's reevaluation by PRA procedures the whole process should take into account three sequential steps: qualitative and quantitative analyses and sensitivity studies (Figure 1). Tools and codes exposed in this paper can carry out above analysis, however, other ones are available to do them successfully, and sometimes in a more adequate manner.

It is very important that inputs/ouputs to programs were adapted for automatic and chained execution, in order to improve the calculation time and data management. Also, to have two interrelated operating machines, PC DOS and UNIX systems, is very useful because PC DOS systems improve fault trees and reliability data management whereas UNIX systems improve calculation capacity.

Sensitivity studies related to theoretical models, reliability data and TS's requirements of components are needed to verify conclusions from other analyses. This studies can also help to limit the errors included by models and reliability data. Also, to focus important topics into the whole AOT's and STI's revision process. Some important sensitivity studies have been presented before. Here, the case of study developed focus errors due to reliability data consideration.

Finally the last comment is related to AOT's and STI's reevaluation with above refered tools and process. With such a kind of process, AOT's and STI's evaluation or reevaluation are separatly made. Almost every study develepod up to now was dealt in that way. Thus, the advantage due to AOT-STI interrelation for a component or even in a system or plant is lost. Actually, at the Polytechnic University of Valencia we are developing a way for TS's improvements by considering AOT-STI interaction. It is carried out in a PhD Thesis which was partially developed at Brookhaven National Laboratory (USA). Such a kind of study would start at the bottom of the above proposed scheme, taking advantage of the "base case risk" estimation for actual AOT's and STI's requirements as we have already seen before.

REGULATORY ASPECTS OF THE USE OF PSA TO EVALUATE TECHNICAL SPECIFICATIONS

J. RUMPF
Staatliches Amt für Atomsicherheit und Strahlenschutz,
Berlin

Abstract

Based on experiences gained in PSA activities the regulatory body of the GDR initiated a programme to investigate the feasibility of using PSA for the evaluation of technical specifications. This programme is just under work. In addition, to improve PSA, the GDR takes part in a programme which is aimed at performing plant specific level 1, PSA as well as and which enables operating organizations to carry out PSA on their own.
The most important of some priliminary general findings presented in this paper are:
- Technical specifications form a well established envelope of operational conditions and procedures. A total reevaluation is not considered necessary.
- Probabilistic evaluation of technical specifications should be an integrated part of PSA activities (at least level 1).Single assessment is not considered reasonable.
- Probabilistic evaluation of technical specifications has to be based on plant specific information and realistic accident sequence calculations
- Up to now no quantitative probabilistic criteria for technical specifications have been established up to now.

---

1. Introduction

The safety of NPPs in the GDR is based on a deterministic approach. Thus deterministic requirements have to be met in order to demonstrate compliance with a defined safety level. NPP licensing is also based on this approach. In addition, probabilistic safety assessment is required.According to a decision of the regulatory body each NPP of the GDR has to be evaluated using PSA level 1 methods.

In the near future regulations will be adopted that require a probabilistic reevaluation of each NPP every ten years.
PSA level 1 is required to
- improve the knowledge of the safety significance of plant systems and plant behaviour
- create an additional background for topical safety issues
- provide a quantitative safety scale based on relative evaluations
- identify weak points and to optimize NPP design and operation
- supervise the aging of components based on a quantitative approach
- modify technical specifications including test and maintenace actions
- evaluate backfitting measures
- identify reasonable accident management measures
- train the operating personnel.
In the light of experience gained with PSA for several years the use of PSA for the evaluation of technical specifications will become possible.
Accordingly, the evaluation of technical specifications is considered an integrated part of PSA within the framework of NPP licensing.
Technical specifications comprise a variety of operational conditions and procedures,e.g.
- limiting conditions for the operation of operating and safety systems,
- permissible outage times for safety systems and components,
- test intervals,
- kind and quality of testing,
- extent of testing and
- kind and extent of preventive maintenance.
The evaluation of each of these conditions and procedures requires detailed system and data analyses of different kinds.

2. Evaluation of Technical Specifications

To facilitate an appropriate use of PSA the regulatory body of the GDR initiated a research programme. One objective of this programme of this programme is to investigate the feasibility of

basing technical specifications on probabilistic analyses. This includes the investigation of PSA based modifications of technical specifications. Related activities are mainly done by the utility and the regularory body.

Based on preliminary results the following conclusions can be drawn:

- Technical specifications (operational, test, maintenance and repair specifications) are generally well established. They are verified by the licensing organization. Therefore a total PSA based revision is not considered necessary. In some cases where weak points are identified by safety analyses or operational experience or where operational features require temporary changes of the technical specifications a reevaluation is necessary. PSA can then be used to receive additional information on safety and reliability.
- PSA level 1, appropriately done can result in determining the weak points of technical specifications.
- Modifications of technical specifications can be evaluated by probabilistic methods. This procedure has to be based at least on PSA level 1. An isolated probabilistic analysis at a lower level (system level) is insufficient. PSA level 1 findings have to be taken into account. Thus a reevaluation of PSA is considered necessary when technical specifications are modified.

Therefore the GDR takes part in a research project which is aimed at developing and applying computer aided PSA which the utility can use for the evaluation of plant modification. Finally the operating organization should be enabled to perform PSA work on its own.

- Decisions on the modification of technical specifications cannot only be based on PSA but also on deterministic criteria which include e.g.

the determination of components which can be repaired from the point of view of spatial acccessibility (technological conditions, radiation protection) or

the necessary repair time.

- Modifications of technical specifications are related to two different classes
  - permanent modifications
  - temporary modifications.

The first class can be based on supplementary PSA. The second class require more sophisticated methods (living PSA). The use of living PSA as an operator aid is not yet generally accepted by the regulatory body. However, research and development work was started for the applicability of living PSA to NPP of the GDR.

- The use of PSA for the modification of technical specifications requires very detailed plant specific system information as well as realistic accident sequence evaluations (best estimate codes). So the success criteria of the safety systems strongly depend on the uncertainties of the accident sequence evaluations. Conservative calculations will result in stronger system performance requirements (parameter values, number of trains). Consequently there will be stronger restrictions related to technical specifications (e.g. permissible outage times).
- Up to now no appropriate probabilistic criteria were found to be compared with technical specifications assessment. Moreover, due to great uncertainties involved in PSA no absolute criteria seem to be reasonably achievable.

The use of relative quantitative criteria (e.g. changes of core melt frequency) require investigations also in respect of the influence of model uncertainties.

- An investigation of repair and maintenance records did not provide appropriate results. The main shortcomings were related to

  the actually necessary repair times
  component boundaries
  causes of failures and description of failures.

To get appropriate results the plant personnel must be able to record specific reliability information which can be used in PSA.

3. Conclusions

The use of PSA for the evaluation of technical specifications requires further research and development activities. Especially plant specific information has to be improved. Methods for the verification of computer codes for accident sequence evaluation have to be used. Estimations of uncertainty ranges should be taken into account.

The feasibility of establishing probabilistic criteria for the evaluation of technical specifications has not yet been proved. Plant specific living PSA could form an appropriate basis for the probabilistic evaluation of technical specifications.

FEASIBILITY ASSESSMENT OF A RISK-BASED APPROACH TO TECHNICAL SPECIFICATIONS*

B. ATEFI, D.W. GALLAGHER
Science Applications International Corporation,
McLean, Virginia

M. WOHL, R. LOBEL
Office of Nuclear Reactor Regulation,
Nuclear Regulatory Commission,
Washington, D.C.

United States of America

Abstract

To assess the potential use of risk and reliability techniques for improving the effectiveness of the Technical Specifications, the United States Nuclear Regulatory Commission (USNRC) initiated an effort to identify and evaluate alternative approaches that could bring greater risk perspective to these requirements. Among alternative approaches studied, a risk-based approach was chosen as the most promising for controlling plant operational risk using Technical Specifications. Technical and institutional issues associated with this approach were analyzed to assess the feasibility of implementing such an approach for determining Technical Specification requirements. Preliminary analysis shows that at this time there are no major obstacles to development of this approach. In order to further study all the practical issues associated with implementation of this approach, a pilot program would be useful.

Introduction

To assess the potential use of risk and reliability techniques for improving the effectiveness of the Technical Specifications to control the risks of operating a nuclear power plant, the United States Nuclear Regulatory Commission (USNRC) initiated an effort to identify and evaluate alternative risk-based approaches that could bring a more exacting risk perspective to these requirements (1). This effort represents one of several initiatives in the United States and other countries for improving the Technical Specifications requirements using risk-based approaches (2-4).

*This work has been performed for the U.S. Nuclear Regulatory Commission, Office of Nuclear Reactor Regulation under Government Contract No. NRC-03-87-029.

The first phase of the USNRC-sponsored effort identified four alternative risk-based approaches for improving the Technical Specifications requirements (1). These are: 1) a risk-based approach, 2) a reliability goal-oriented approach, 3) a data-oriented approach, and 4) a configuration-control-oriented approach. Among these, the risk-based approach is the most promising for controlling plant operational risk using Technical Specifications. This approach utilizes the most comprehensive plant risk model currently available and, as such, it accurately accounts for the level of redundancy, diversity, and importance of various components and systems.

Risk-Based Approach

The primary characteristic of a risk-based approach to Technical Specifications is that the decisions on plant operation are based on the effect of plant configuration changes on a plant's instantaneous risk. The impact of configuration changes on such instantaneous risk can be made in real time, if a fast-response software for analyzing the plant risk model is developed, or in semi-real time using a plant risk model and currently available PC-based software. In either case, the plant risk model can be used for planning such routine daily activities as surveillance tests or preventive maintenance, or in response to unplanned component outages for setting allowed outage times (AOTs). Using either approach, the AOTs for different components are based on the importance of the component to the plant risk and the plant configuration at the time a component is declared inoperable. Thus, contrary to current Technical Specifications, the AOTs for different components are not fixed. Rather they are calculated in real time on the basis of the current configuration of the plant, that is, on the basis of what other components or systems are available at the time a particular component is declared inoperable. To assess the characteristics of a risk-based approach to Technical Specifications, a set of risk-based criteria for calculating AOTs and surveillance test intervals (STIs) were developed, and, for two reference nuclear power plants, the current AOTs were compared with the risk-based AOTs.

Risk-Based Criteria

In the proposed risk-criteria, the AOT associated with the unavailability of a component or system can be calculated using the following relationship:

$$\Delta R \bullet T \leq A \qquad (1)$$

where:

- ΔR is the increase in plant risk as result of the unavailability of a component or system
- T is the allowed outage time, that is, the duration of time that the component or system can remain out of service before the plant has to be shut down
- A is the dimensionless fixed limit that applies to all plants

The fixed limit A can be thought of as the highest acceptable plant risk level integrated over the duration T. The initial trial of this relationship was based on using change in the frequency of core melt instead of change in plant risk, that is, on the basis of calculating the AOTs from the relationship:

$$\Delta CM \bullet T \leq B \qquad (2)$$

where:

- ΔCM is the increase in the plant's core melt frequency as a result of the unavailability of a component or system
- T is the allowed outage time
- B is the dimensionless fixed limit that applies to all plants

The best way to explain the meaning of the constant B is to note that the plant core melt frequency varies throughout the year with the status of various equipment. At any given time, the core melt frequency can be substantially different than the average core melt frequency as calculated in plant probabilistic risk assessments (PRAs). The concept of specifying a constant value of B for all plants is based on the reasoning that an increase in the plant core melt frequency above an accepted safe level would be tolerable for only a limited period of time. The higher the increase in the core melt frequency above the acceptable levels when a piece of equipment is taken out of service, the less time the plant would be allowed to operate. Constant B represents the highest acceptable core melt frequency integrated over the duration T, which is specified by the AOT. Thus, B can be thought of as the highest acceptable core melt probability that is tolerable over a given AOT.

Figure 1 depicts this concept. In this figure, the reference plant has an average core melt frequency that is lower than the accepted baseline goal. On the basis of this concept, if the removal of equipment from service results in a small increase in the core melt frequency, there would be a willingness to allow a relatively long period of time for the component to be repaired. But if the increase in the core melt frequency is very large as a result of the removal of equipment from service, the concept dictates a very short time for fixing the problem before that plant would have to shut down. Constant B is essentially the area of each of the two rectangles. In addition to setting limits like B, which would control the one-time increase in the plant's core melt frequency as a result of unavailability of one or more components, there might be a need to control the total amount of time, or the number of times a component can be out of service during a fuel cycle. Another alternative might be to control the total risk contributed by all component outages.

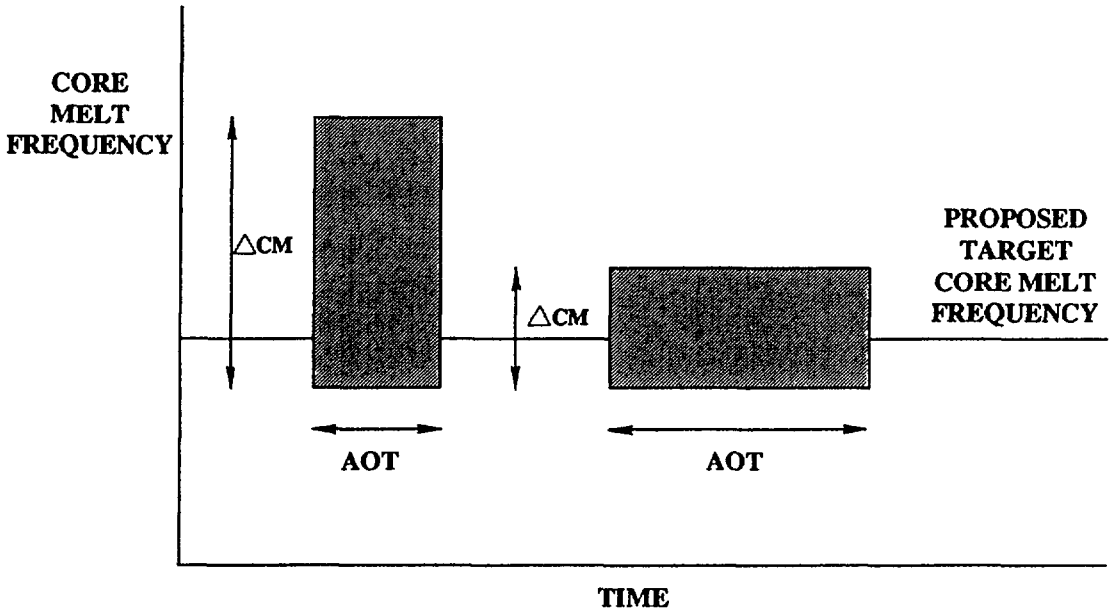


Figure 1 Pictorial Representation of the Risk-Based AOT Limits Based on Increase in Core Melt Frequency

There are a number of ways to set the fixed limit B in Equation 2. One approach is based on the limit of 1.0E-4/year individual plant core melt frequency (5). If, as a result of the unavailability of one or more components, the core melt frequency increases by an order of magnitude to 1.0E-3/year, the increase in core melt frequency is sufficiently high that the plant should be shut down in a very short period of time. To allow for very minor

fixes that could remove the plant from the high-risk range, a four-hour limit for shutdown under these circumstances could be suggested. On the basis of these arguments and assumptions, the fixed limit B is calculated as 5.0E-7.

The current USNRC-proposed safety goals are based on limits on early and latent fatalities and the frequency of a large release (6). Our objective in developing a sample numerical criterion was to try to show in sufficient detail the effect of setting AOTs and STIs using a plant-level criterion. Core meltdown is an easier plant-level criterion to use for this purpose than the probability of a large release or limits on early and latent fatalities. A separate approach for setting the constant B in Equation 2 was attempted by Brookhaven National Laboratory (BNL) with the end results quite comparable to the above proposed values (2).

Sample Calculations

To test this criterion, the PRA model used two of the plants analyzed as a part of the staff's effort as reflected in NUREG-1150 (7, 8). The NUREG-1150 effort was initiated by the USNRC to analyze the risk for five different U.S. light-water reactors (LWRs) using the state-of-the-art methods (9). For a series of cases involving unavailability of one or more components in these plants, AOTs were calculated using the real time risk-based approach and were compared to the current AOTs for these components. Results are shown in Tables 1 and 2.

For the first reference plant, the risk-based AOTs are in some cases higher than in the current Technical Specifications and in other cases are lower than the current Technical Specifications. For example, the risk-based AOT for outage of one diesel generator is shorter than the current AOT for this equipment, whereas the risk-based AOT for the lower pressure injection (LPI) pump is higher than the current AOT for this component. This points out the risk or core melt significance of the diesel generator versus the LPI pump for this plant. Also, the risk-based calculations allow a much shorter AOT for the turbine-driven auxiliary feedwater (AFW) pump than for motor-driven AFW pumps indicating the importance of the turbine-driven AFW pump compared to motor-driven AFW pumps because of the large contribution from station blackout sequences to this plant's core melt frequency. Even for the motor-driven AFW pumps, the risk-based AOTs are different because the plant's design for the motor-driven AFW trains is not identical.

Table 1. Comparison of Risk-Based AOTs and Current Technical Specifications AOTs for the First Reference Plant (7)

	Components/Systems Unavailable	Core Melt Frequency (Per Year)	Change in Core Melt Frequency (Per Year)	Risk-Based AOT* (Hours)	Current AOT (Hours)
1.	None (Base Case)	2.5E-5	0	--	--
2.	One Accumulator	5.2E-4	5.0E-4	8	4
3.	One LPI Pump	3.2E-5	7.5E-6	584	24
4.	Motor Driven AFW Pump 3A	3.6E-5	1.1E-5	371	72
5.	Motor Driven AFW Pump 3B	4.4E-5	1.9E-5	223	72
6.	Turbine Driven AFW Pump	7.2E-5	4.7E-5	92	72
7.	Two Motor Driven AFW Pumps	5.6E-5	3.1E-5	141	6
8.	One Motor Driven (Pump 3B) and the Turbine Driven AFW Pumps	6.8E-4	6.6E-4	6	6
9.	Diesel Generator 01	2.7E-4	2.5E-4	16	168
10.	Diesel Generator 03	3.0E-4	2.8E-4	16	168
11.	Diesel Generator 01 and 03	8.4E-3	8.4E-3	0.5	2
12.	Diesel Generator 03 and AFW 3A	5.1E-4	4.9E-4	7	--
13.	Diesel Generator 03 and Turbine Driven AFW	6.8E-4	6.6E-4	7	--

*Based on Eq. 2; $CM \cdot AOT \leq 5.0E\text{-}7$.

Table 2. Comparison of Risk-Based AOTs and Current Technical Specifications AOTs for the Second Reference Plant (8)

	Components/Systems Unavailable	Core Melt Frequency (Per Year)	Change in Core Melt Frequency (Per Year)	Risk-Based AOT* (Hours)	Current AOT (Hours)
1.	None (Base Case)	8.2E-5	0	--	--
2.	One Accumulator	5.8E-4	5.0E-4	9	1
3.	One LPI Pump	2.1E-4	1.3E-4	34	72
4.	Motor Driven AFW Pump A	1.3E-4	4.8E-5	91	72
5.	Motor Driven AFW Pump B	1.3E-4	4.8E-5	91	72
6.	Turbine Driven AFW Pump	1.2E-4	4.0E-5	110	72
7.	Two Motor Driven AFW Pumps	2.6E-3	2.5E-3	2	0
8.	One Motor Driven Pump and the Turbine Driven AFW Pumps	1.2E-3	1.1E-3	4	0
9.	Diesel Generator A	1.4E-4	5.4E-5	80	72
10.	Diesel Generator B	1.4E-4	5.4E-5	80	72
11.	Diesel Generator A and B	1.2E-3	1.1E-3	4	2
12.	Diesel Generator A and AFW B	1.8E-4	1.0E-4	45	--
13.	Diesel Generator A and Turbine Driven AFW	4.0E-4	3.2E-4	14	--

*Based on Eq. 2; $CM \cdot AOT \leq 5.0E\text{-}7$.

For the second reference plant, the risk-based AOTs and current AOTs are quite comparable, despite the fact that the core melt frequency of the second plant is higher than that of the first reference plant. The primary reason for this result is that the core melt frequency in the second reference plant is more evenly distributed among many dominant accident sequences. This implies that compared with the first reference plant, the second plant is not as vulnerable to failure of some components relative to others.

It is important to note that the risk-based approach is capable of generating AOTs for multiple component failures which is a major advantage of this approach compared with the current approach to Technical Specification requirements. Existing Technical Specifications do not have AOT requirements for failure of combinations of components, which most likely constitutes the majority of component outage scenarios with highest contribution to the increase in core melt frequency. Thus, the conclusion of the first phase of the study was the recommendation of a real time or semi-real time risk-based approach using the risk criterion discussed above.

In the second phase of the USNRC-sponsored effort a study was initiated to: 1) identify major technical and institutional issues associated with implementation of a risk-based approach, 2) provide a preliminary resolution of issues identified, and 3) assess the feasibility of implementing a pilot program to look into detailed characteristics of such an approach to Technical Specifications (10). To achieve these objectives, the USNRC formed a working group comprising personnel from the USNRC Office of Nuclear Reactor Regulation (NRR), Science Applications International Corporation (SAIC), the USNRC Office of Nuclear Regulatory Research (RES), Brookhaven National Laboratory (BNL), and three volunteer utilities, namely, Pacific Gas and Electric (PG&E), Southern California Edison (SCE), and the Philadelphia Electric Company (PECo). The working group met several times during this course of this project to discuss various technical issues and provide comments and guidance on the progress of the project. In addition, to gain insights into operational experience with the current Technical Specifications, each utility was asked to collect data on plant configuration changes as components were taken out of service to be tested, or maintained, or because they failed. These change data were then used by each utility in plant-specific PRAs to calculate the corresponding changes in plant core melt frequency. This information combined with an analysis of the results of the Accident Sequence Precursor (ASP) Study (11) formed the basis for some insights about the effect of current Technical Specifications on plant operational risk and the potential for improvement through the use of a risk-based approach to Technical Specifications.

The technical issues associated with potential implementation of a risk-based approach to Technical Specifications that were identified and analyzed include: 1) characteristics of the required plant risk model, 2) requirements of the proposed software for calculating real time changes in plant risk due to plant configuration changes, 3) approach for setting risk-based criteria, 4) Technical Specifications for components not included in the PRA, 5) elements of a reliability-centered surveillance concept for setting STIs, and 6) major elements of cost associated with implementation of a pilot program. In the identification and resolution of these issues, the study has focused primarily on the assessment of any technical or institutional issues that could interfere with the conduct of a successful pilot program. In addition, using actual operating data from the three participating utilities and the results of the ASP, an attempt was also made to gain insights into the impact, from safety and availability points of view, of a risk-based approach to Technical Specifications on plant operation. The primary focus of actual plant data analysis was to assess if plants currently can enter into areas of high operational risk without violating any Technical Specifications, and if there are plant configurations that the plants are avoiding due to potential Technical Specifications violations that do not result in a large increase in plant operational risk.

Even though many of the issues and characteristics of a risk-based approach to Technical Specifications have been identified and analyzed in this study, there are still more practical issues that can only be addressed during a pilot program. The primary objective of such a pilot program would be to address and resolve the remaining technical issues, to better understand some of the practical issues associated with implementation of such an approach to Technical Specifications, and to gain confidence about the ability of this approach to Technical Specifications to minimize plant operational risk and maximize plant availability. Three options are identified for developing a pilot study: 1) a semi-real time approach, 2) a real time approach, and 3) a combined approach.

In the semi-real approach, the plant PRA is used in a semi-real time basis to assess the impact of changes in plant configuration on plant operational risk, and provide advisory information to the plant maintenance and operating staff on the impact of planned maintenance activities or unexpected component failures on plant risk. This will be done by using an existing plant PRA and making some initial adjustments to prepare the model for the proposed pilot Technical Specifications application. The objective of the pilot study

would be to keep a complete log of the changes in plant configuration. Each time a component is taken out of service or returned to service, the changes would be entered into the plant PRA and the new core melt frequency profile of the plant would be calculated. For those situations that result in entering a limiting condition for operation (LCO) action statement and a corresponding AOT based on current deterministic Technical Specifications, the proposed risk-based criterion would be used to calculate the recommended AOT. Alternatively, if plant maintenance personnel would like to take a component out of service but are prohibited because of a restrictive AOT, the risk-based criteria should be used to assess what would be recommended if a risk-based system were in place.

The second option for the pilot study is the real time approach. The pilot program for the real time approach to Technical Specifications includes all the activities of a semi-real time approach described above plus development of fast-response software. In this approach, the major task is to initiate development of the required software discussed in detail in Reference 9. In parallel with the software development, some effort will be made to modify the plant PRA to the format most suitable for use in the software.

The final option for the pilot program is the combined approach. In this option, the semi-real time approach would be initiated as soon as possible. In parallel, the software development activity would also be initiated. After 12 to 18 months, when the software is ready and properly tested, the pilot program would switch from the semi-real time approach to the real time approach. In this way, during the first 12 to 18 months a great deal of information about the characteristics of risk-based approaches to Technical Specifications will be gathered, and a large number of technical and practical issues can be resolved.

Conclusions

Based on analytical and actual plant operational analysis, it is concluded that a risk-based approach to Technical Specifications has the potential to improve both plant safety and availability. Furthermore, detailed analysis of major technical and practical issues identified in this study shows that at this time there do not appear to be any technical or institutional obstacles that could prevent initiation of a pilot program to assess the characteristics and effectiveness of a risk-based approach to Technical Specifications for controlling plant operational risk. Limited analysis of actual plant operational data using

input from the three participating utilities has shown that plants can enter configurations that result in a large increase in plant risk without violating current Technical Specifications. Alternatively, these data included a case in which a plant was forced to shut down due to a Technical Specifications requirement where the resultant increase in plant risk due to this configuration was negligible. Finally, each of the three participating utilities, prior to this project and independent of this study, had started to look at their plant PRA as a tool to control plant operational risk. Although the approaches taken by each utility are different, the ultimate goal in all cases has been to prevent entering high risk configurations, regardless of whether or not a Technical Specifications violation results.

It appears that a risk-based approach to Technical Specifications has the potential to better control plant operational risk compared to the current deterministic requirements. This approach also offers more flexibility to plant operators in dealing with component outages, which could result in higher plant availability.

REFERENCES

1. Atefi, B., et al., "Alternative Approaches to Risk-Based Technical Specifications," Final Report, SAIC-87/3110, June 1988.

2. Samanta, P. K., et al., "Analysis of Approaches and Strategies for Risk-Based Configuration Control Systems," Brookhaven National Laboratory Technical Report A-3230, October 1989.

3. Wagner, D. P., et al., "Case Studies: Risk-Based Analysis of Technical Specifications," ANS/ENS International Topical Meeting on Probabilistic Safety Assessment and Risk Management, Zurich, Switzerland, September 1987.

4. Laakso, K., "Optimization of Technical Specifications by Use of Probabilistic Methods, A Nordic Perspective 1985-1989," Draft Report NKA/RA 5450, Technical Research Center of Finland, November 1989.

5. "Safety Goal for Nuclear Power Plant Operation," NUREG-0880, Revision 1, May 1983.

6. "Safety Goals for the Operation of Nuclear Power Plant; Policy Statement; Correction and Republication," Federal Register, Vol. 51, No. 162, August 21, 1986.

7. "Analysis of Core Damage Frequency from Internal Events: Surry, Unit 1," NUREG/CR-4550, SAND 86-2086, November 1986.

8. "Analysis of Core Damage Frequency from Internal Events: Sequoyah, Unit 1," NUREG/CR-4550, SAND 86-2084, February 1987.

9. "Reactor Risk Reference Document," NUREG-1150, Main Report, 1989.

10. Atefi, B., et al., "Feasibility Assessment of a Risk-Based Approach to Technical Specifications," SAIC-90/1033, March, 1990.

11. Minarick, J. W., et al., "Precursors to Potential Severe Core Damage Accidents: 1984, 1985, 1986," NUREG/CR-4674, ORNL/NOAC-232, Volumes 1-6.

APPROACHES FOR ASCERTAINMENT OF ALLOWABLE OUTAGE TIMES (AOTs)

K. THEISS
Technischer Überwachungsverein Norddeutschland e.V.,
Hamburg, Federal Republic of Germany

Abstract

On the background of the requirements of German Nuclear Safety Criteria of NPP the KTA-report 1407 was established as a guideline to represent methods concerning the ascertainment of allowable outage times of safety systems during NPP operation. The methods descibed are based on both probabilistic and deterministic approaches and have been used in former times in licensing procedures of NPP.

---

1. Requirements of Nuclear Standards

In the German Nuclear Safety Criteria of NPP it is required that safety systems have to fulfil the single failure criterion during maintenance action as well. The safety system functions are related to the following incidents:

- reactor shutdown due to all incidents
- heat removal after loss of coolant accident (LOCA)
- heat removal with unavailable main heat sink
- heat removal after loss of offsite power
- containment isolation function in the demand of LOCA

In this context some precisions have to be made. Maintenance actions of safety systems during NPP operation are permitted if the single failure criteria is fulfilled. In case of inspection this criteria is excluded if the function of the affected subsystem can be restored at a given time when demanded.

Generally duration of maintenance during NPP operation has to be determined in respect of the reliability of safety systems. For that reason allowable outage times are defined within reliability analysis and are laid down in operation handbooks.

On this background the KTA-report 1407 /1/ was established as a guidline to represent approaches concerning the ascertainment of allowable outage times in NPP. Following approaches mentioned in this report will be described:

- Reference-Method
- Risk-Method
- Matrix-Method

2. Application of Probabilistic Approaches

2.1 Reference-Method

The Reference-Method was first used within the licensing procedures of NPP. According to this method the allowable outage time T_R is ascertained while the maximum unavailability $U_{R,max}$ during maintenance will not differ more than a factor f in comparison to the maximum unavailability U_{max} of the system without maintenance.

$$U_{R,max}(t=T_R) = f \cdot U_{max}(t=T_P)$$

with T_P = inspecting interval

This approach takes into account the requirement that the unavailability level of safety equipments will not exceed a defined boundary value at any time of NPP operation (Fig.1).

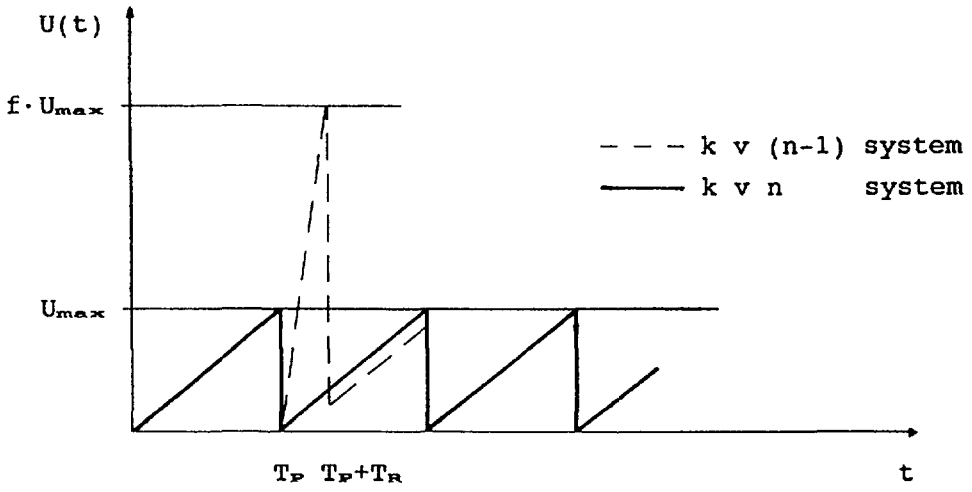


Fig.1 Time dependent unavailability of a standby system

Fig.1 shows the time dependent function of a standby system periodically tested. At given time T_P one subsystem was running out so that the time function changes as illustrated. The factor f is limited to 5 with the argument that such a high reference value will not influence the mean unavailability of the system because of shortness of outage time in comparison to the period of observation (i.e. one year).

Because of the simple mathematical approach the method is confined to a system related ascertainment of outage times with the advantage of including a direct evaluation of the current plant condition.

Following disadvantages have to be mentioned:

- the lower the unavailability of systems the lower the allowable outage times,
- determination of factor f is an arbitrary act,
- the frequency of maintenance cannot be considered.

2.2 Risk-Method

Similar to the Reference-Method the Risk-Method was developed using mean unavalabilities and additionally considering the frequency of maintenance F(n) of n-subsystems.

$$F(n)\cdot(\ T_R\cdot U_R + (T_P-T_R)\cdot U_{PR}\ ) = f\cdot T_P\cdot U$$

with:

$$U_R = 1/T_R \int_0^{T_R} U_R(t)\ dt$$

$$U_{PR} = 1/(T_P-T_R) \int_{T_R}^{T_P} U_{PR}(t)\ dt$$

$$U = 1/T_P \int_0^{T_P} U(t)\ dt$$

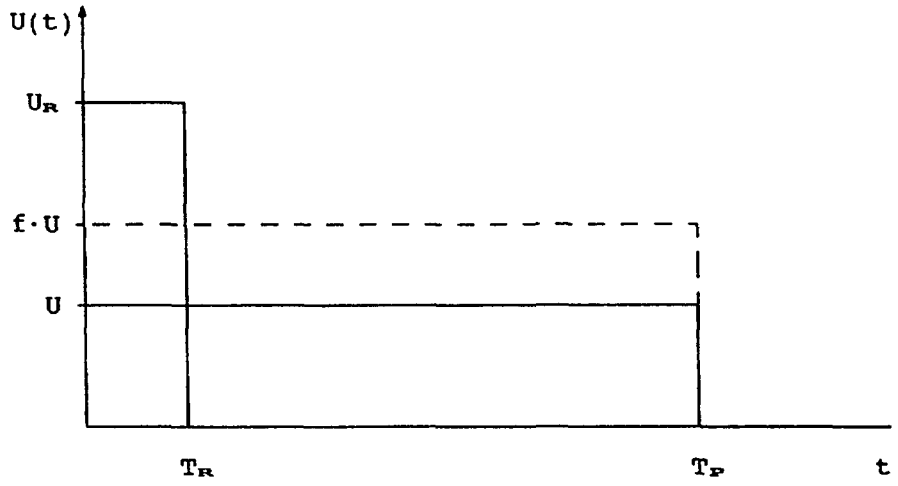


Fig.2 Mathematical approach of Risk-Method

The other mentioned disadvantages of the Reference-Method still exist; the ascertainment of outage times is not possible for a single failure event.

2.3 Possible Extension

The methods described so far ascertain the allowable outage times on a system specified level. While entering a higher level, the sequence level, outage times can be evaluate in dependency of the changing of sequence probabilities. According to that approach the risk influence of the various safety equipments is considered.

The disadvantage of this approach is that changes in risk due to the considered outage times will normaly be low in comparison to data uncertainty. For that reason this approach has to be treated as an extension of a possible foundation of evaluation in connection with other methods operating on the system specified level.

3. Application of Deterministic Approaches

The frequency of initiating events as an additional factor of plant risk is used to determine allowable outage times in the so-called Matrix-Method. The initiating events of a plant are classified (first parameter E) and according to their frequencies structured in a matrix (Table 1). The second parameter of the matrix is the system's remaining redundancy k during a maintenance action.

Table 1: Intervals of allowable outage times

E \ k	0	1	2
2	24 h	2WE	2WE - 2MO
3	24 h	2WE - 2MO	2MO
4	2WE - 2MO	2MO	ROUT
5	2MO	ROUT	-

ROUT = until next refueling outage
MO = month
WE = week

The sum of the input parameters E+k is assigned to an interval of allowable outage times. This is done by taking into account the operation experience and rules set down in licensing procedures.

Table 1 has the following logical structure :

- the interval of allowable outage time enlarges with the value of E+k,
- all diagonal fields of the matrix posses the same interval of AOT's in dependancy of the value E+k = const. (except the field E=3,k=0),
- if E ≤ 3 and k = 0 the interval of allowable time is defined as 24 hours because the single failure criteria cannot be considered,
- if the value of E+k ≥ 6 no restriction of allowable outage time is necessary.

The classification of initiating events is performed in relation to a KTA-report /2/. The spectrum of considered events is illustrated in table 2.

This matrix is simple to apply and is today the basis of allowed outage times of modern NPP in FRG.

4.0 Summary

The methods introduced in this paper represent the frame of evaluation of allowable outage times in FRG. The probabilistic safety analysis (PSA) performed nowadays in all nuclear plants can be considered as a suitable foundation for continuation and further development of these methodical approaches.

Table 2: event-classes of event sequences of PWR and BWR

Nr.	initiating events	event-class E
1.	leakage and fracture in the steam line system (SLS)	
1.1	fracture of connecting pipelines	3
1.2	leakage between containment and isolation valve	4
1.3	total fracture of steam line	4
2.	loss of offsite power	
2.1	short-dated (< 30 min)	2
2.2	long-dated (> 30 min)	3
3.0	loss of feed water system (FWS)	
3.1	loss of main FWS-pumps	2
3.2	fracture of FWS-pipelines	3
4.0	incorrect change of reactivity and efficiency distribution	2
5.0	leakage of primary coolant (LOCA)	
5.1	small leakage	3
5.2	large leakage	4
5.3	steamgenerator tube fracture	3
5.4	fracture of connecting pipeline	3
6.0	loss of main heat sink	2
7.0	external events	
7.1	safety earth-quake	4
7.2	aeroplane crash, external explosion	5

References

/1/ Regelvorhaben KTA 1407 (KTA-GS-55):
"Methoden zur Ermittlung von zulässigen Instandhaltungszeiten in Kernkraftwerken"

/2/ Statusbericht zum Konzept (KTA-GS-47):
"Klassifizierung von Ereignisabläufen für die Auslegung von Kernkraftwerken"

VVER PLANT PROBABILISTIC SAFETY ASSESSMENT

V.A. VOLKOV, E.P. LARIN
All-Union Research Institute
for Nuclear Power Plant Operations (VNIIAES),
Moscow, Union of Soviet Socialist Republics

Abstract

This paper adresses the ways of probabilistic safety assessment for VVER-1000 reactors in operation. Probabilistic analysis is supposed to be used to optimize operational documentation, to assess weaknesses and enhance safety and efficiency of the operating plants.

Probabilistic safety assessment (PSA) is a necessary part of safety justification for NPPs both operating and under design. To practically implement the task much effort is needed to process information, prepare computers codes, to do calculations and adopt the results. Operational experience shows that VVER plants can be improved by improving stability, reducing the number of shutdowns, labour consumption as well as improving operational documentation and taking account of all hypotetical transients. The best possible way to achieve this goal is to use PSA.

In this paper PSA performance programme adopted in VNIIAES is described.

PROBABILISTIC SAFETY ASSESSMENT AS A TOOL OF TECHNICAL-ECONOMIC APPROACH TO DEAL WITH OPERATION MATTERS

The following tasks are supposed to be performed for PSA:

- implementation of justified computer codes to analyze all possible processes all over the plant (including auxiliary systems) taking account of actual dynamic characteristics of systems;
- selection of information and analysis of NPP operation under unforseen circumstances;
- classification of events and information processing in the way allowing subsequent analysis of events which did not occur but have a certain probability to occur;

- implementation of programmes to assess reliability and establish fault trees and event trees;
- preparation of technical information including NPP system performance, time lag data and etc.;
- process calculations proper, assessment of the event probability consequences and finally risk assessment and identification of weaknesses.

Analysis results would allow to optimize operational documentation, improve design and adress technical problems of backfitting. In particular this analysis would allow:

- to develop optimum technical specifications which can answer the question of "what to do" when any deviation from normal operation occurrs;
- to develop validated operational procedures and training documentation for the operations personnel which can answer the question of "what to do" in all cases including beyond-design-basic situation;
- to develop operator "advisor" taking account of current processes and the so-colled "human factor";
- to address system-related technical problems providing for assessment of both effect on safety and on economic efficiency.

The following PSA study for the operating NPPs is being carried out in VNIIAES:

- preparation of request for proposal to classify events and faults.
- collection of plant operational data including events and faults;
- event analysis;
- development of dynamic calculation codes;
- analysis of partial solutions affecting saffety and stability using probability method.

The first practical steps in PSA study were calculations and analysis of failures of secondary steam discharge systems and improvement of RPS on degradation of the pressure boundary. Optimal practical solutions which meet both safety and economic efficiency requirements have been found.

Optimization of plant operation with uncontrolled leakage has been analysed i.e. optimum risk of core damage during mitigation of accident consequences was identified. The impact of scope and quality of the commissioning thermal hydraulic testing was assessed.

PSA study for VVER-1000 plants (V-302, V-320) is of most interest since this type of reactor is more powerful and more thermally sensitive as compared with VVER-440 plants. A number of interlokings and protections for VVER-1000 is twice as much as that for VVER-440. Besides the first series of VVER-1000 plants (V-302) has a reduced number of protections and interlokings as compared with the later series (V-320).

Analysis shows that a number of unforseen initiating events for V-320 is 25 % per reaktor-year higher as compared with V-302 series which results from insufficient optimization of protections.

The following practical tasks can be addressed using PSA study:

- determination of core melt probability, assessment of weaknesses, development of optimum recommendations when this probability exceeds 10^{-5} per 1 reaktor-year;
- determination of reactor vessel brittle failure probability, probability of containment damage and radioactive release into the environment, development of recomendations when this probability exceeds 10^{-7} per 1 reaktor-year;
- assessment of risk of equipment failure, development of technical specifications and operating procedures;
- assessment of system-related technical solutions which influence safety, stability and efficiency;
- optimization of conditions for unit stability on the one hand and safety conditions on the other;
- optimization of conditions to reduce probability of reactor vessel brittle failure with emergency core cooling conditions unchanged;
- development of optimum strategy of repair;
- development of optimum technical specification.

To complete the work considerable effort and expertise are still required. The operating NPPs require some modification and improvements. Unit stability can be significantly improved by using an integrated protection system which can assess the existing situation, its evolution, equipment failures, operator actions, priority etc. (fig. 1). An integrated protection capable of self-diagnosis and rejection of signals must select the opnimum mode to eliminate dangerous operational limits.

PSA study is supposed to determine characteristics of this protection which meets the safety requirements and produces minimum effect during transients. "Human factor" analysis showed the necessity to develop mode diagnostics as an operator support system. This system can be part of an "integrated protection". Fig. 2 shows the flow chart of possible operator support system.

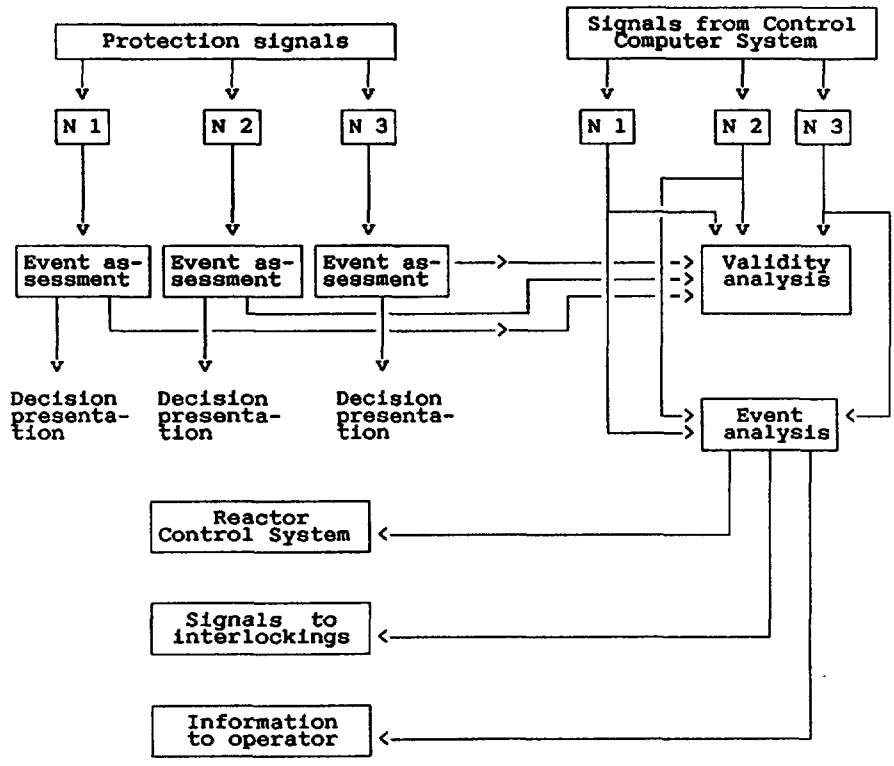


FIG. 1. Interlockings and protections flow chart.

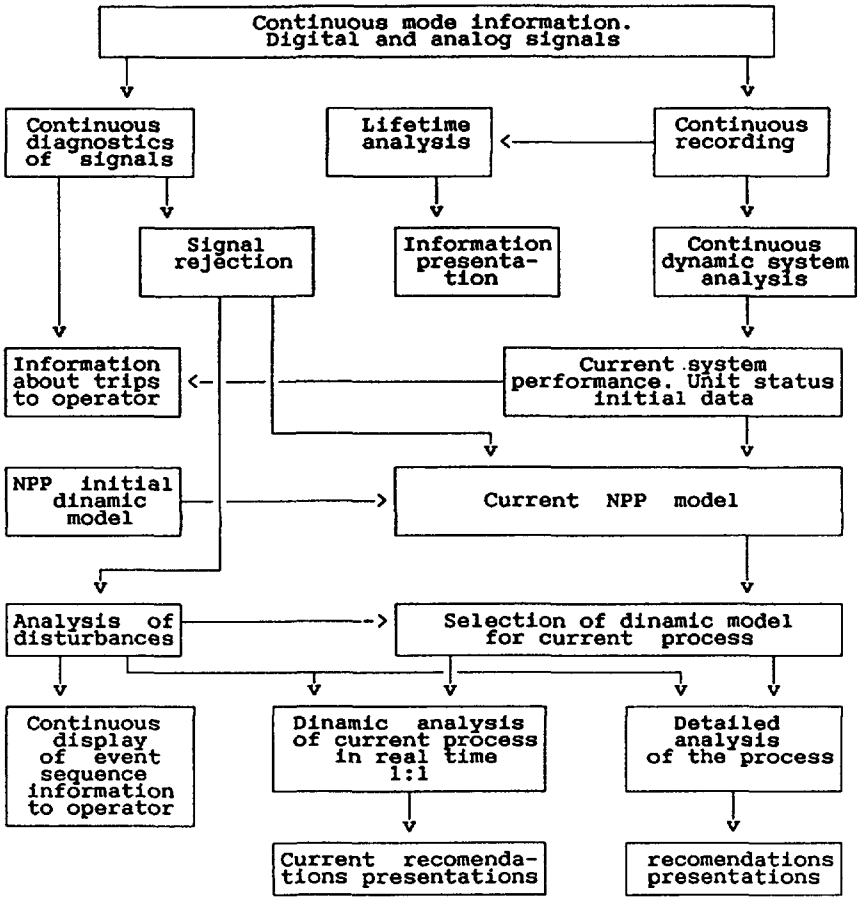


FIG. 2.

Such systems require:

- availability of highly reliable processor;
- mobile but reliable plant dynamic models;
- reliable communication between systems (cables, connections, sensors etc.);
- organization of analysis including self-diagnosis, program management, control system feedback, system response etc.

WAYS OF PROBABILISTIC ANALYSIS IMPLEMENTATION

Probabilistic analysis is supposed to be more comprehensive as compared with PSA which can be used to validate acceptable risk of radioactive release. Fig. 3 presents the algorithm of PSA performance. Without collection, classification and summary of reliability data, being the basic element of the algorithm, it is impossible to perform the analysis. Besides, to perform PSA initiating events probability data and the data on system

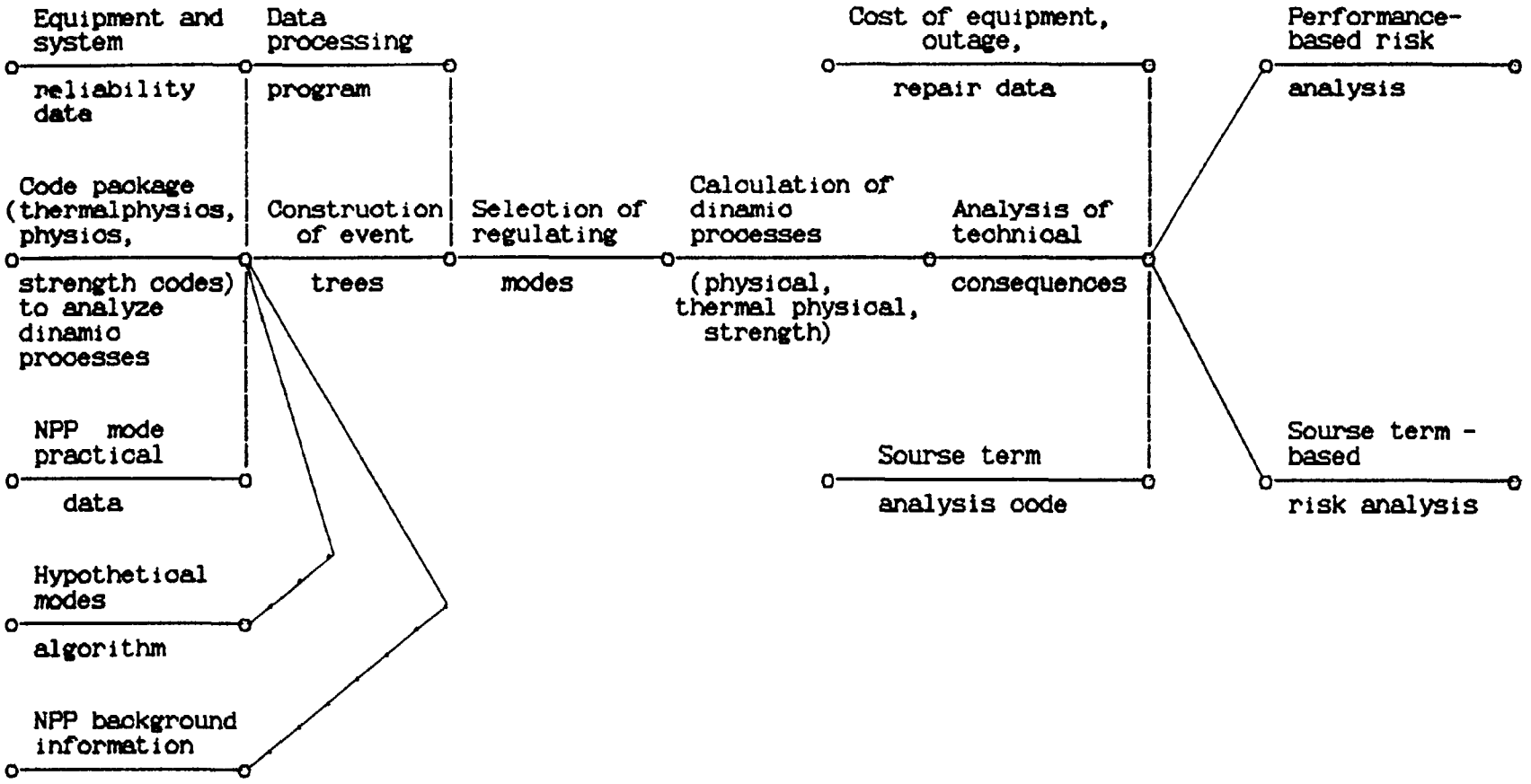


FIG. 3. PSA algorithm.

reliability during dynamic processes are required. The main failure probability component of any system can be identified by the failure to respond during dynamic processes.

To systematize information initiating events must be classed. This type of classification for VVER-1000 plant (V-320 type) (Fig.4) takes account of all possible disturbances:

- design;
- actual;
- hypothetical.

This classification allows for differences between physical processes, event consequences, frequency and systems affecting the reactor.

Based on this classification event trees covering all possible processes affecting safety and stability are established.

To summarize the data on failures on demand over 500 events which actually occurred at NPPs and had not been envisioned by the operations personnel were analysed. In each case the fact of system actuation or failure would be determined.

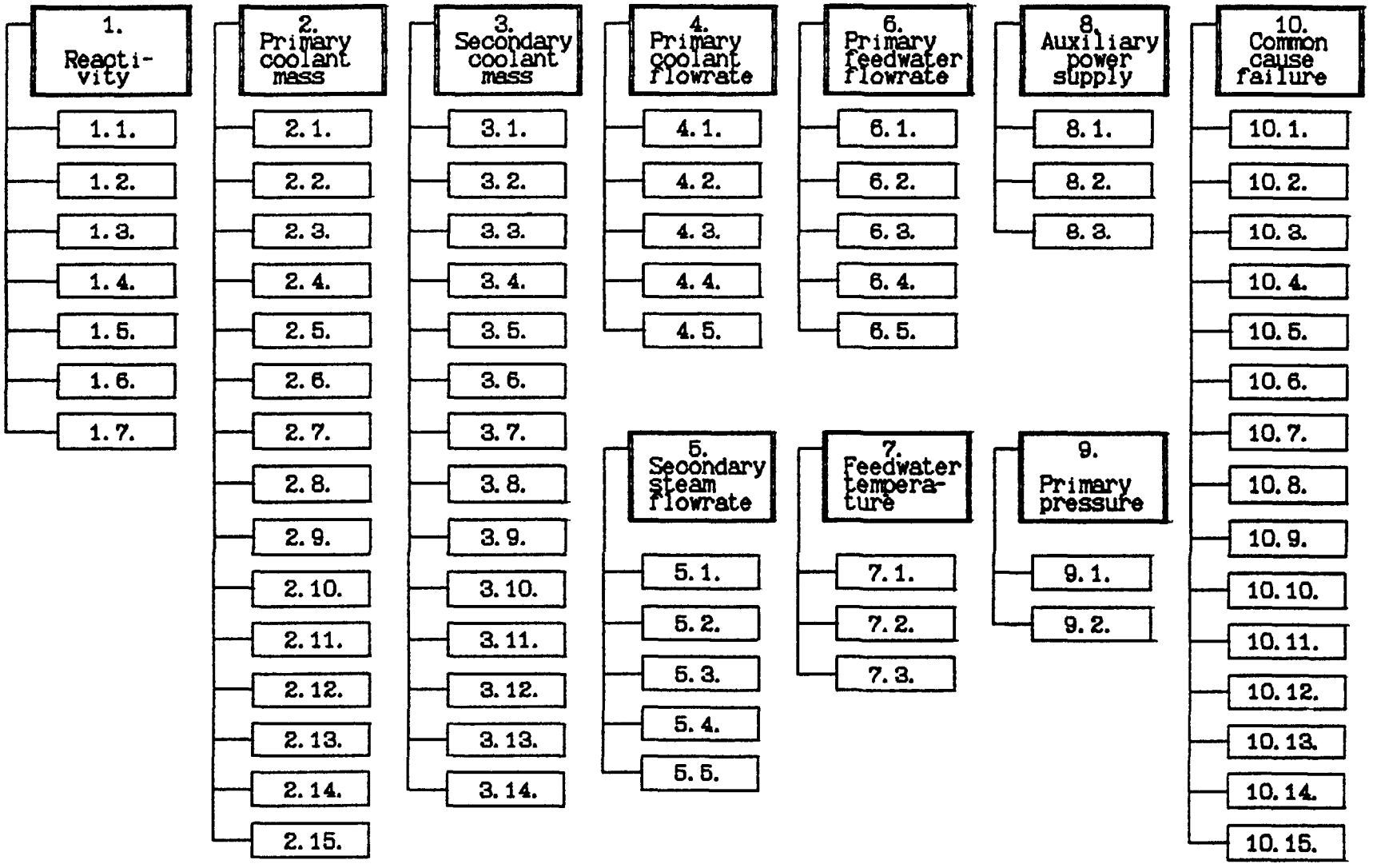
Automation of assessment of the processes and safety has only been planned. Therefore actual events were considered given the lack of objectiveness and information deficiencies.

Lack of information is compensated by experts experience who can assess process evolution using time factor, separate parameters, event consequences. Experts can assess probability of system actuation (failure to actuate) etc. Table 1 presents one of analysis results - frequency distribution of the initiating events (the numbering is consistent with Fig. 4).

The results concerning failure to operate on demand must be analysed annually allowing for modifications. This is of special importance for the systems not often involved in the process.

Fault tree analysis based on component reliability data provides for additional practical information and sometimes additional independent assessment. This type of analysis is performed for the systems involved in disturbances in accordance with Table 1.

To solve the problem besides component reliability data information on component functional features, characteristics and parameters as well as effect of control and interaction systems


1. Reacti-vity
1.1.
1.2.
1.3.
1.4.
1.5.
1.6.
1.7.
2. Primary coolant mass
2.1.
2.2.
2.3.
2.4.
2.5.
2.6.
2.7.
2.8.
2.9.
2.10.
2.11.
2.12.
2.13.
2.14.
2.15.
3. Secondary coolant mass
3.1.
3.2.
3.3.
3.4.
3.5.
3.6.
3.7.
3.8.
3.9.
3.10.
3.11.
3.12.
3.13.
3.14.
4. Primary coolant flowrate
4.1.
4.2.
4.3.
4.4.
4.5.
5. Secondary steam flowrate
5.1.
5.2.
5.3.
5.4.
5.5.
6. Primary feedwater flowrate
6.1.
6.2.
6.3.
6.4.
6.5.
7. Feedwater tempera-ture
7.1.
7.2.
7.3.
8. Auxiliary power supply
8.1.
8.2.
8.3.
9. Primary pressure
9.1.
9.2.
10. Common cause failure
10.1.
10.2.
10.3.
10.4.
10.5.
10.6.
10.7.
10.8.
10.9.
10.10.
10.11.
10.12.
10.13.
10.14.
10.15.

1. Reactivity

1.1. RPS spurious actuation
1.2. Change of boric acid concentration
1.3. RPS rod failure
1.4. Control & monitoring system failure
1.5. Change of in-core coolant temperature
1.6. Xenon oscillations
1.7. RPS failure to actuate

2. Primary coolant mass

2.1. Leak in MCP cold leg
2.2. Leak in MCP hot leg
2.3. Leakage from reactor
2.4. Leak from primary to secondary
2.5. Make-up blowdown flowrate
2.6. MCP seal water flowrate
2.7. Air flowrate primary
2.8. Pressurizer protective membrane flowrate
2.9. Pressurizer leak
2.10. Flowrate from TQ14
2.11. HP to LP flowrate
2.12. ECCS valve leakage
2.13. Auxiliary pipe leak in the primary
2.14. Auxiliary system boundary valve leaks
2.15. Outside boundary valve leak

3. Secondary coolant mass

3.1. Scale of steam pipe damage
3.2. Feed pipeline rupture
3.3. Deaerator casing leak
3.4. Auxiliary power
3.5. Atmospheric pressure relief valve flowrate
3.6. SG safety valve flowrate
3.7. SG blowdown flowrate
3.8. SG casing leakage
3.9. HP heater leak
3.10. LP heater leak
3.11. Main condensate pipeline leak
3.12. Condenser leak
3.13. Separator leak
3.14. Other events

4. Primary coolant flowrate

4.1. MCP shaft sticking
4.2. MCP shaft break
4.3. MCP trip
4.4. Grid frequency oscillations
4.5. MCP supply interruption when switching to stand-by power sourse

5. Secondary steam flowrate

5.1. Turbine stop valve closure
5.2. Turbine control valve closure
5.3. Fast acting check valve closure
5.4. Abrupt stop-control valve opening
5.5. Main steam valve closure

6. Primary feedwater flowrate

6.1. Secondary feedwater flowrate
6.2. Turbine driven feed pump trip
6.3. Failure of condensate feed to D-7
6.4. Closure of isolating valves
6.5. Loss of circulating water

7. Feedwater temperature

7.1. HP heater trip
7.2. HP heater start
7.3. Auxiliary feedwater pump spurious actuation

8. Auxiliary power supply

8.1. Deenergizing of 1 and more 6 kV auxiliary power buses, MCP start
8.2. Loss of safety system (SS) AC supply
8.3. Loss of DC supply

9. Primary pressure

9.1. Spurious injection
9.2. Electric heater start, trip

10. Common cause failure

10.1. Deficiency of reactor equipment manufacture
10.2. Fire
10.3. Earthquake
10.4. Aircraft crash
10.5. Flood
10.6 Tornado
10.7. Hurricane
10.8. Frost
10.9. Explosion near NPP
10.10. Violation
10.11. Sabotage
10.12. Reactor vessel rupture
10.13. Loss of power
10.14. Design deficiency
10.15. Other events

FIG. 4. Classification of initiating events at the VVER-1000 plant.

Table 1.

Initiating events at VVER-1000 plants

Number	Classification number	Initiating event	Number of initial events %	Notes
1	2	3	4	5
1	5.1	Closure of stop valves of turbine	21,03	
2	4.3	Trip of one ore more than one MCP	14,81	
3	5.2	Turbine control valves closure	8,98	
4	6.1	SG feedwater controller failure	8,59	
5	6.2	Turbine-driven feed pump trip	5,82	
6	8.1	Deenergizing of auxiliary power bus	5,06	
7	6.5	Loss of circulating water	4,67	
8	9.1	Pressurizer spurious injection or failure to terminate it	4,28	
9	8.2	Safety system power loss	3,91	
10	1.1	RPS spurious actuation	3,11	
11	5.3	Fast acting check valve closure	2,72	
12	3.2	Feedwater pipeline rupture	2,32	
13	5.4	Stop control valve abrupt opening (elektro-hydraulic control system, hydraulic control system)	1,93	
14	6.3	Loss of condensate supply to deaerator	1,93	
15	1.3	Controls failure	1,16	
16	3.4	Auxiliary power	1,16	
17	2.4	Primary to secondary leakage	0,91	
18	5.6	Turbine bypass valve opening (spurious)	0,76	
19	1.4	Control cyctem failure	0,77	
20	3.7	SG blowdown flowrate	0,77	
21	3.8	HP heater leak	0,77	
22	3.1	Steame line damage scale	0,33	
23	7.1	HP heater trip	0,38	
24	2.1	MCP cold leg leakage	0,38	
25	2.2	MCP hot leg leakage	0,38	
26	2.5	Blowdown flowrate	0,38	
27	2.8	Pressurizer protective membrane flowrate	0,38	
28	2.9	Pressurizer leak	0,38	
29	2.13	Auxilliary pipeline leakage	0,38	
30	3.6	SG relief valve flowrate	0,38	
31	3.10	LP heater leak	0,38	
32	3.13	Separator leakage	0,39	

is required. The lack of unit design as a single whole makes it necessary to coordinate separate data including experimental data, circuits, component characteristics etc.

The necessity to develop NPP dynamic model makes it necessary to collect information on component characteristics such as length, volume, time, cross section, pressure loss etc. Since NPP unit design does not provide complete information package, documentation available at NPP is used for the analysis. Fig. 6 gives an example of fault tree construction for TQ13 system (Fig.5) as well as the result of its analysis using PSA PACK code.

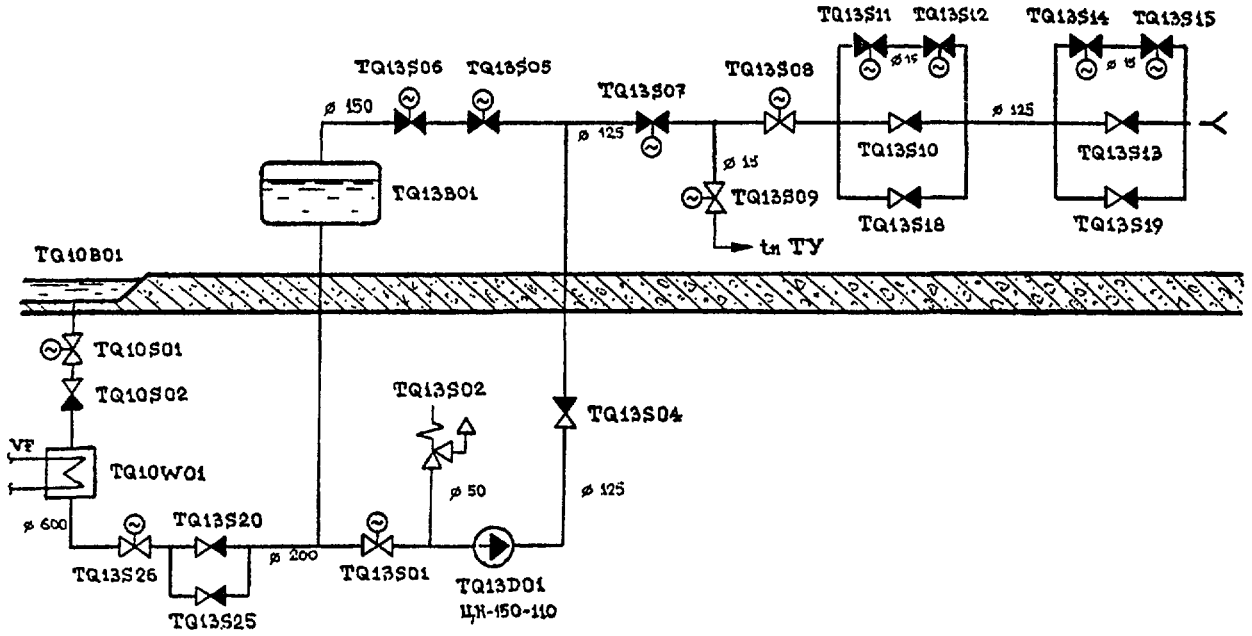


FIG. 5. High pressure emergency core cooling system (TQ13).

```
MCS OF  FAULT TREE  TQ13   ENVIRONMENT >> NPROB TOT >> 1.252E-002

     1  0.96E-03  512-VSADE-OD
     2  0.46E-04  504-VCAOB-T8
     3  0.24E-03  505-VMAOI-T
     4  0.36E-04  509-VMVDS4
     5  0.10E-01  566-PMHSA-OD
     6  0.12E-02  565-PMHRA-T1
     7  0.36E-04  508-VMVDS3

MCS OF  FAULT TREE  TQ13   ENVIRONMENT >> NPROB TOT >> 1.252E-002

     1  0.96E-03  -TQ13S02
     2  0.46E-04  -TQ13S04
     3  0.24E-03  -TQ13S07
     4  0.36E-04  -TQ13S08
     5  0.10E-01  -TQ13D01S
     6  0.12E-02  -TQ13D01R
     7  0.36E-04  -TQ13S01
```

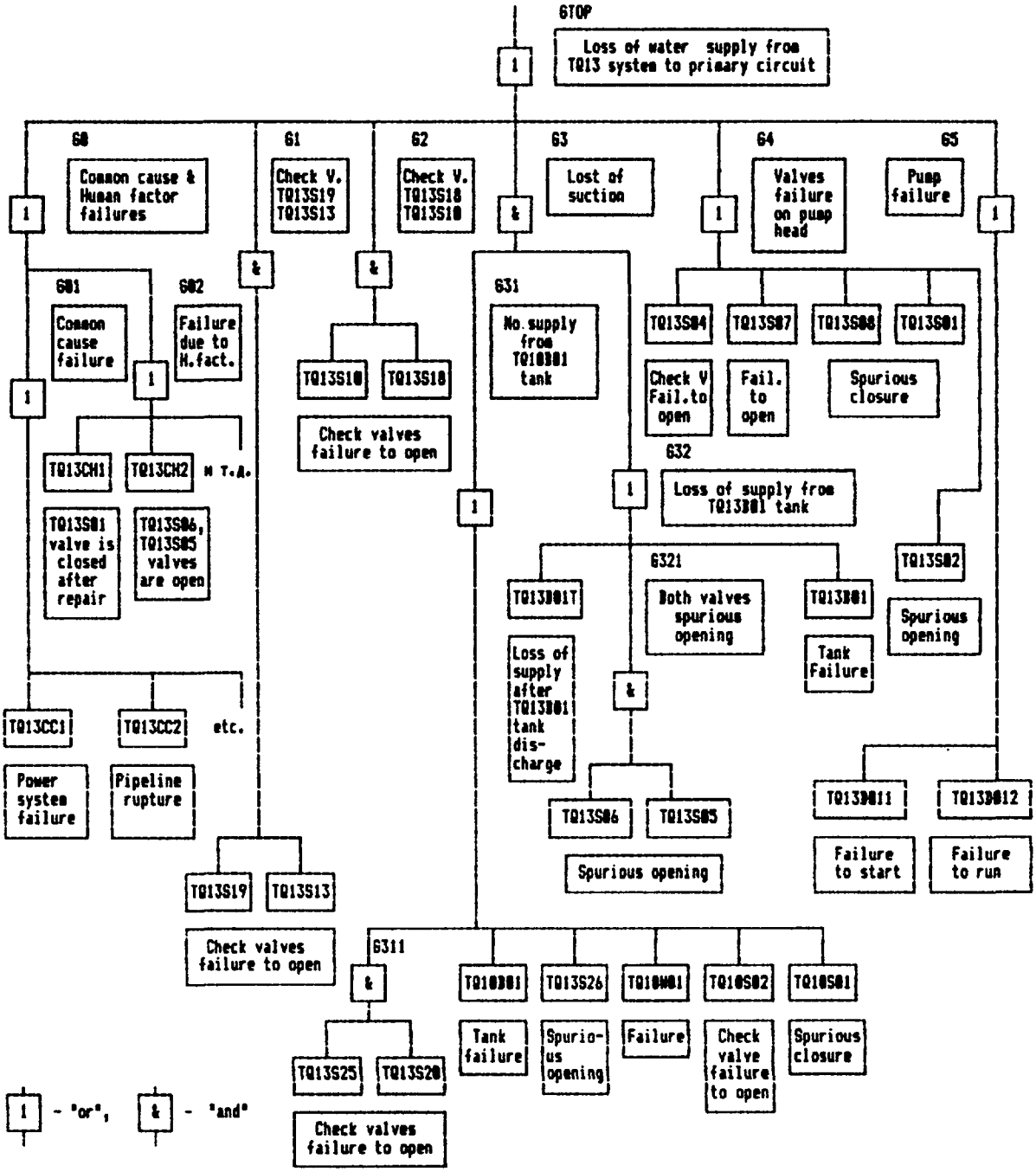


FIG. 6.

The next phase of the analysis is optimization of event trees. For this purpose it is necessary to identify criteria of consequences for their subsequent analysis.

Event consequences are assessed using dynamic computer codes based on advanced codes used in "DYNAMIKA", "TECH-M", "MOST-10" projects and KIPR code package. Computer codes must be improved using codes related to systems affecting processes in the reactor and containment. It is necessary to develop codes for severe accidents. The codes must be well grounded. The appropriate efforts are under way but there are problems with code justification.

Parallel effort using alternative codes developed by leading companies are needed which may significantly speed up the solution of the above problems.

When using codes developed for PWR reactors it is necessary to adjust them for VVER reactors and assure experience feedback for specialists.

UNCERTAINTY ANALYSIS IN THE PROCESS OF RELIABILITY ESTIMATION

J. HOLÝ
Nuclear Research Institute,
Řež, Czechoslovakia

Abstract

This paper deals with the uncertainty analysis as an important line of reliability analysis. In the first part of material the framework of uncertainty studies performed in NRI Řež is provided (fault tree method, lognormal distribution, error factor, modularization). In the second part of this one the interesting general results (behaviour of error factor) are published, studied and commented. An original attempt at time dependent uncertainty analysis is presented.

Introduction.

Since 1985, Czechoslovakia has been participating in the coordinated research programmes, sponsored by IAEA. This paper concentrates on performance and results of so called uncertainty studies, incorporated in two research contracts (contract No. 4032 and contract No. 4355).

The fulfilled activities of research contract No. 4032 "Risk Criteria for the Nuclear Fuel Cycle" included:

a) review of methodology for reliability analysis of PWR safety systems
b) selection of two safety systems for reliability analysis with (i) few human interactions and (ii) many human actions
c) performance of reliability analysis to obtain availability upon demand of both systems and comparison of results treating all human actions as independent
d) re-analysis one of the two systems assuming that human actions are dependent acts
e) repeat (a) - (d) above using input data with uncertainties

Because of various types of primary events, we had to prepare partly new methods to include these nontrivial types into analysis. It will be briefly comment in my paper.

The contract No. 4355 "PRA for Research Reactor LVR-15" was commenced in March 1986 and the final report was completed in September 1988. A complete description of the present status of the LVR-15 reactor was given with the emphasise on the safety related systems. Event trees for seven initiating events and (relative simple) fault trees for nine top events were assembled. All these fault trees were evaluated including uncertainties of input data (probability characteristics of primary events). A simplicity of these fault trees made possible in a simple manner to confirm some general rules of uncertainty propagation through the fault tree, which will be mentioned in following of paper.

I. Uncertainty analysis and fault tree method (gen. principles).

Mathematical model (fault tree) including uncertainties, is a substantial generalization of classic model with qualitatively higher level of abstraction. In classic model (without uncertainties), each primary event is connected with a known and fixed value of probability of its occurence. In the generalized one, this value is substituted by a random variable with probabilistic distribution. From mathematical point of view this model is uncomparably more complex. In the most complicated case, a continuous function is attributed to each event instead of a single value, i.e. a prescription, giving an instruction for calculation of uncountable number of values. In more simple cases (discrete random quantity) a function defined on integers (on a countable number of values) or on a finite subset of integers (finite number of values) is being attributed. The original, classic model with the probability p of occurence of an event can be included here as a special case. The corresponding random variable acquires value p with probability 1 and all other values with probability zero.

The basic methods of analysis of uncertainties require independence of primary events. This is a very strong assumption which simplifies the necessary mathematical apparatus used, but usually is not fulfilled. On the other hand, a number of models of real systems with the assumption of independence violated reflect reality quite well.

Selection of distribution is another complicated and comprehensive problem the solving of which the classic model is exempted from. Choice of distribution of probabilistic characteristic of a failure would be based in every concrete case on a rational considerations. In most cases, one of the following five distributions is selected as the competent one: uniform, log-normal, log-uniform, gamma, and S_B-distribution.

Selection of the lognormal distribution is motivated mainly by good agreement of the models, based on the lognormal distribution, with the data, obtained in some of the cases for which the data were available. The selection of the lognormal distribution has, nevertheless, at least two drawbacks: (i) - the density of log-normal distribution is non-zero in the interval $(0,\infty)$ whereas the probabilistic characteristic in use are certainly greater than some $\varepsilon>0$ - therefore, there exist a surrounding from the right of zero, where the density is positive, but the corresponding random quantity acquires the values from this surrounding with zero probability; (ii) - the distribution is long-tailed, which does not correspond to the data in many cases. These problems can be avoided by introduction of the log-uniform distribution. Its density is non-zero only in the interval (A,B), where $0<A<B<\infty$.

S_B-distribution has turned out to be a close approximation of top event distribution of complex systems, a better approximation than the lognormal distribution. Using this one, we have to be in waiting for some problems owing to its complexity and because of a lack of in detail created methodical processes (computer codes).

At the derivation of probabilistic characteristics of secondary (and mainly the top) events the model of uncertainties is already unambiguously more complex than the original classic one. The following statements are frequently applied at the derivation:

If X_1 is a random variable with density $f_1(x)$, and X_2 a random variable with density $f_2(x)$, and if X_1 and X_2 are independent, then the random variable X_1X_2 has a density $f_1(x)f_2(x)$.

If X_1 is a random variable with density $f_1(x)$, and X_2 a random variable with density $f_2(x)$, and if these quantities are independent, the density of the variable X_1+X_2 is given by convolution of densities $f_1(x)$ and $f_2(x)$.

Therefore the evaluation of density of the variable Y in second case is relatively awkward and very often leads to numerical integration.

The methods proposed for model of uncertainties lead to getting either histogram as an approximation of distribution of top event probabilistic characteristic, or to several representative characteristics of distribution.

Monte Carlo method is a simulation method widely used at solution of many of mathematical and engineering problems. Its advantages can be well employed at the analysis of uncertainties. The characteristics of primary events have some probabilistic distribution. By means of a generator of pseudo-random numbers, each probabilistic characteristic is assigned a pseudo-random value in accordance with the given distribution. Using the structural function of the system, random value of the top event probabilistic characteristic is obtained from random values of all primary event probabilistic characteristics. By this way, one trial is realized. From a sufficient number of such trials, a comprehensive statistical sample of values of top event probabilistic characteristics is obtained. This sample enables us to reconstruct the distribution of the top event probability characteristic: either several significant parameters of the distribution or the complete histogram.

Method of moments is relatively simple, applied most frequently in cases, when the input quantities are independent and have the same distribution. Experience with similar models and work with available data enables us to estimate approximately the type of distribution of top event probability characteristic, or to determine the set $\mathcal{F}$ of distributions, to which the distribution of our top event will belong. An element of the set $\mathcal{F}$ will be a distribution, represented by some density function $f(\phi)$ depending on a parameter ϕ. The Moment-Matching method provides an estimate of parameter's ϕ value from the moment's equations.

Two computer codes are used in NRI Řež performing uncertainty analysis. Computer code SAMPLE is an ancient programme (published already in the Reactor Safety Study) based on Monte Carlo method. In spite of its limited facilities is widely used for the analyses of small fault trees with simple modelled primary events. Computer code COSMOS takes method of moments to study uncertainty propaga-

tion. Derivation of moments of top event probabilistic characteristic from the moments of primary events probabilistic charecteristics forms the main part of calculations.

II. A typical outputs of the analysis.

Uncertainty analysis provides outputs of very various formes. In this paragraph we will discuss three of them.

Histogram of some distribution connected with uncertain probability characteristic describes uncertainty in a grafical manner and provides complete, well-arranged information about the shape of distribution. It is useable as a final product of the analysis. However, it can be hardly used for step by step exact analysis (modularization).

Confidence α-interval represents a pair of numbers, determining a part of real axis, contained with probability α exact value of the evaluated probability characteristic. In the risk studies main attention is directed on the right boundary of interval, being additional information in comparison with classical reliability analysis (without uncertainties).

To concentrate the information into a single parameter, the error factor is a very suitable means. It turns out, the time dependent error factors modell very well the contributions of uncertainty coming from both parts of the data file, that are component failure rates and human errors probabilities, to the uncertainty of system top event's probability - as will be show below in detail. Being defined for the lognormal-distributed variables as a quotient of 95% percentile and median of distribution, error factor F has following practical interpretation:

F = 1-3 ... a very credible estimate with low level of uncertainty
F = 5 ..... an estimate with medium level of uncertainty
F = 10 .... an estimate with high level of uncertainty
F > 20 .... a very aproximate estimate.

This interpretation is of great importance in case of intuitive estimation by a team of investigators - a standard manner, how to establish error factors connected with uncertainty of probability characteristics of primary events.

III. Uncertainty analysis of LPIS safety system and the general conclusions coming from.

1. Preassumptions of the analysis.

The following principles are accepted for the strategy of uncertainty analysis of low pressure injection system: 1. For the simulation of probability characteristic was used a log-normal distribution. 2. In the first stage a preliminary analysis of inspected elements was performed including development of original methods. 3. A modularization was carried out before of whole system analysis. 4. Computer code COSMOS was used for the numerical uncertainty propagation analysis.

Distribution of probabilistic characteristic of the top event of the LPIS fault tree with the log-normal distributed inputs has not exact lognormal character, however. If we want to use top event of some subsystem as an input into higher level gate, we commit by using of log-normal distribution an innacuracy for this input. Nevertheless there are a lot of reasons for holding of the conception, as follow: (i) two-parameters log-normal distribution is flexible enough and a set of log-normal type density gives sufficiently correct approximation of the subsystem characteristic distribution density, (ii) distribution of probabilistic characteristic of the subsystem, represented by a subtree, simulates essentially the same class of real word phenomena as a distribution of primary probability characteristics (relative little probability phenomena, theirs estimation is affected by major uncertainty) and it can be simulated by the same manner therefore, (iii) calculations simulated a probability characteristic distribution of subsystem by means of more close-fitting four-parameters Johnson's S_B-distribution indicate that in many cases a two-parameters log-normal distribution is convenient - as a special case of the above mentioned one and the results of computations using both distributions are in good coincidence.

2. Theoretical analysis of general uncertainty behaviour.

Some general conclusions had been acquired for uncertainty analysis before we have evaluated LPIS system. Very interesting is especially one argument:

Uncertainty of probability characteristic of the fault tree top event depends very substantially on the fault tree structure.

and the second argument connected with the first one:

The error factor of probability characteristic of the fault tree top event is usually considerable lower than error factors of primary events probability characteristics.

At the study of general regularity of uncertainty behaviour the following conclusions were acquired (using at the uncertainty analysis of periodic inspected components): (i) error factor of output from the gate "AND" is higher than error factors each of its inputs; error factor of output from a gate does not depend on the mean values of its inputs; there is a simple explicit relationship for expressing of the error factor of output in dependence on the error factors of inputs, (ii) error factor of output from the gate "OR" depends on the relation of the mean values of its inputs; error factor of the gate with a small difference the mean values of its inputs is considerably less than the error factors of both inputs into the gate; at the difference in order between mean values of inputs into the gate, the error factor of output equals about to an error factor of the input with higher mean value; error factor of output is possible to determinate explicit from the values of the error factors of inputs and mean values of inputs, (iii) error factor of the top event decreases rapid with an increasing number of minimal cutsets (with about the same parameters of distribution); error factor connected with one minimal cutset increases sharp with the order of this one.

3. Preliminary analysis of periodic tested components.

Note once again, that the probability characteristics (failure intensities, probabilities of human errors) are considered to be random variables with some probability distribution.

The first task of the preliminary analysis of periodic tested components was to determine (and put equal to mean value of the distribution) their instantaneous unavailability in the time points, in which a mean value of system unavailability will be further calculated. Instantaneous unavailability of periodic inspected components can be determined from very general relations /1/, in which all the types of significant human errors at the periodic inspections are included.

The main task of preliminary analysis of periodic tested components was to determine an error factor of the distribution of

instantaneous unavailability from the error factor of failure intensity as well as from the error factors of human errors probabilities, when "as good as new" approach was accepted.

The first step in a calculation of investigated characteristic is to find the time period, to which a given time belongs (operation, inspection, repair) because of the difference in models. But an inverse sequence was accepted for the above mentioned analysis - it was elected several time points connected with operation and several another time points connected with inspection. The elected time points cover in both cases equidistantly the cycle time between refuellings.

Description of the method and an appropriate calculation of instantaneous unavailability error factor is very detail investigated in /2/. The proposed method is based on a general behaviour of uncertainty given in previous part. It is a new possibility, extended a state of art of exact uncertainty analysis. The accomplished calculations of error factors of the periodic inspected components indicate that its value is determinated usually by an error factor of the component failure rate. The error factors of probability of human errors influence the resulting error factor rather exceptional.

Conclusion: *The changes of credibility of the given human errors probabilities influent only in a very limited manner credibility of computed instantaneous unavailability of periodical tested component.*

4. Some results of the analysis.

Besides of the periodic inspected components, LPIS includes also "standard elements", i.e. the elements which are not inspected between refuellings. Their aging, such as during an analysis performed by classical method, is simulated by exponential distribution of time to the failure occurence with a constant failure rate. Failure rate, within uncertainty analysis is considered as a random variable and in the case of LPIS, a log-normal distribution is always accepted for it.

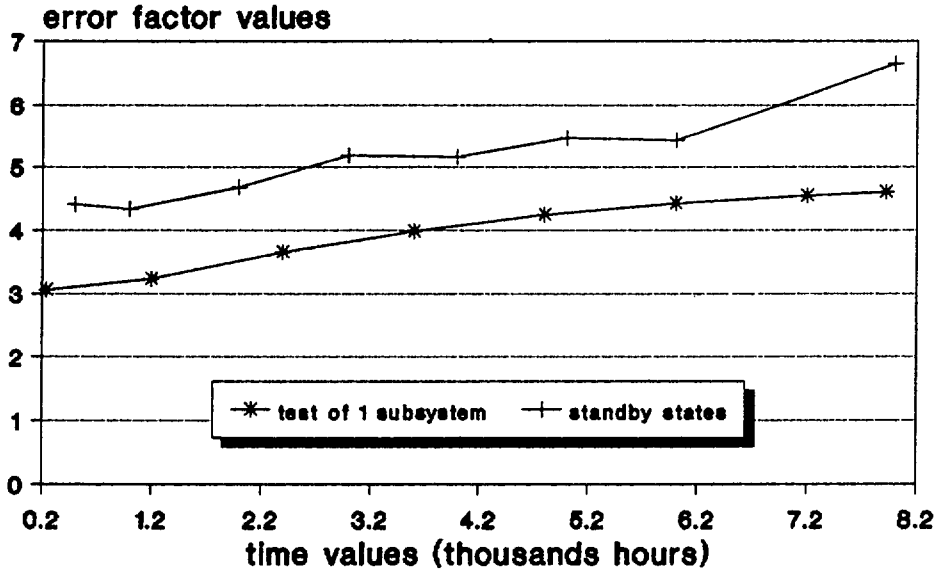
The LPIS system has three independent subsystems, regularly periodical tested. During a short time period are available only two subsystems of the LPIS system, therefore. In spite of these periods are relatively short, from our point of view can't be neglected. Therefore a special attention must be devoted to the inspection step during reliability characteristic calculations as

well as at uncertainty analysis. No special attention was devoted to the time interval determinated for a renewal, because the reliability characteristic in this interval do not differ from those used in the stand-by data.

Instead of complete review of the results we were obtained, some interesting results with respect to time-dependent behaviour of error factor will be presented below.

A typical example of error factor's changes in time for some safety system with many human actions is graphically presented on the figure 1. We can draw some inferences from this one:

1. Mean value of the instantaneous unavailability of un-inspected components with constant failure rate is increasing during the analysed time period, whereas a mean value of instantaneous unavailability of inspected component is changing periodically. The influence of error factors related to un-inspected components with constant failure rate increases with increasing time because in each "OR" gate an input error factor with a higher mean value is dominating. This fact indicates an error factor convergence to the limited value. In this concrete (but typical!) case , the error factors of un-inspected components are greater than the error factors (resulting from preliminary analysis) of the components under inspection, therefore the resulting system's error factor is increasing.



LPIS system of NPP Mochovce

FIG. 1. Error factor as a function of time.

Conclusion: *The credibility of computed system unavailability on the beginning of the period between refuellings and at the finishing of the period between refuellings may very differ, a value of system unavailability is usually considerable more credible for the time points near the starting point.*

2. For the time points from the inspection intervals, the growth of error factor is substantially monotonous, whereas for time points in standby intervals is instabil. The instability for time points in standby intervals is caused by the fact that individual components with different error factors, considered as inputs into "OR" gates have various time distance from the start of contemporary time period. These mean values changes of instantaneous unavailabilities of components inputing into "OR" gates have dominant importance for the error factor of output from "OR" gate. In "OR" gates consisting of the inputs with periodic inspected components, in several cases a prevail influence can carry out a component with small error factor, while in other cases is decisive a component with high error factor. At the calculations with time from inspection period of one subsystem, there are the distances of time from start of contemporary period at resisting (un-inspected) subsystems ever the same, and no irregularity can occur.
Conclusion: *The credibility of evaluated unavailability considerably depend on the time point location with respect to the accepted strategy of inspection and repair.*

3. During the period to the first inspection, the characteristics of individual inputs are quite different from the others periods (no error factors of human errors affect on the resulting error factor, no dominant effect appears over the error factors of un-inspected components). This fact is expressed in given case by somewhat higher error factor value (by breakage of monotonicity also for calculation time from the inspected period).
Conclusion: *In the time period to the first inspection, the behaviour of resulting error factor may differ from that during other time period.*

4. Due to the fact of one LPIS subsystem unavailability during the inspection time, different fault trees for stand-by time of all the subsystems and for inspection time of one subsystem are accepted. According to the conclusions of the previous paragraphs, fault tree structure influences considerable a value of

error factor. It results in this case in a significant lower value of error factor for every time point in the inspection interval.

IV. Summary and conclusions.

A history of uncertainty analysis in Nuclear Research Institute was presented. The framework of those studies was described. A fundamental elements of this one is fault tree method, probability characteristics (unavailability on demand) of primary events holding as lognormal distributed random variables, error factor quantifying the spread of these variables, two numerical method to evaluate uncertainty propagation through fault tree and computer codes SAMPLE and COSMOS corresponding to them.

Some interesting properties of error factor and time-dependent behaviour of this one for a typical medium-size safety system under inspection and repair (possibility of human errors, discontinuous unavailability on demand as a function of time, "as good as new" approach) were studied.

A new methods to estimate error factor of time-dependent unavailability of component under inspection and repair including human factor were mentioned.

Various arguments against PSA studies are often concentrated in doubtes of credibility of the results connected with rare input data. An intuitive approach leads to the impression as following: "The larger and more complicated fault tree with the inputs the given uncertainty, the more uncertain the resulting system probability characteristic". The results of the study described in this paper doesn't confirm this statement, even more support rather opposite insight.

References.

/1/ Hojný V., Holý J.: Inspections of Standby Systems, Rep. NRI, Řež 8018-T, 1987 (in Czech)

/2/ Holý J.: Uncertainties in Reliability Analysis of LPIS of LPIS of the VVER-440 Reactor ECCS in NPP Mochovce, Rep. NRI, Řež 8505-T, 1988 (in Czech)

/3/ Hojný V.: Reliability Analysis of the Low Presure Injection System of the VVER-440 Reactor ECCS in NPP Mochovce, Rep. NRI, Řež 8284-T, 1987 (in Czech)

THE USE OF PROBABILISTIC SAFETY ANALYSIS METHODS FOR PLANNING THE MAINTENANCE AND TESTING UNAVAILABILITIES OF ESSENTIAL PLANT AT HEYSHAM 2 AGR POWER STATION

B.E. HORNE
Technology Division,
Nuclear Electric plc,
Barnwood, Gloucester,
United Kingdom

Abstract

The Paper describes the development of the practice adopted at Heysham Power Station for the control of the removal of essential plant for maintenance and testing. This has been based on the definition of two operational categories derived from probabilistic and deterministic fault criteria, and uses an advanced interactive computing facility to demonstrate compliance with these criteria. This facility, the ESSM, contains a "living model" of possible failure modes of the essential systems which is continuously updated by the operator as plant is removed for planned maintenance and testing and as systems are reconfigured. The ESSM is also used to plan plant outages so as to minimise the operational risk during maintenance. The overall strategy adopted at Heysham 2 has resulted in simple operating instructions and increased flexibility in planning plant outages for maintenance and testing.

1.INTRODUCTION

Maintenance and testing of the essential cooling plant at Heysham 2 are planned in a systematic and comprehensive manner to minimise risk and and to maximise flexibility using a specially developed on-line computing facility known as the Essential Systems Status Monitor (ESSM). This facility uses advanced probabilistic safety analysis methods to provide the Station operator with a risk management tool which he continuously updates to provide a "living" probabilistic model of the essential plant conditions.

Traditionally, methods of planning the removal of essential plant for maintenance and testing have been provided by defining,(in a hardcopy format or computerised spreadsheet form), prior to reactor power operation, the various combinations of plant unavailability which are "acceptable". The definition of these combinations was previously part of the design process and has required demonstrations that each combination is consistent with the reliabilities and fault tolerant capabilities required for overall objectives to be satisfied. The highly redundant, and interconnected, design of the essential systems of a modern nuclear power station however means that there are a very large number of such combinations of plant unavailability which can be demonstrated to be acceptable. Any method of describing all these combinations individually to a power station operator will therefore be complex unless this large number is reduced. This has been achieved in the past by introducing conservatisms into the definitions so that some of the more complex combinations are described as operationally unacceptable even though they could have been demonstrated as acceptable.This pessimistic approach to the control of plant unavailabilities in the essential cooling systems has resulted, not only in unnecessary restrictions in overall station operation but also, in restricted flexibility in planning the maintenance and testing of the plant. The inevitable occurrence of plant faults complicates the situation further.

The strategy adopted at Heysham 2 Power Station has been to develop a method of planning plant unavailability which removes the restrictive practices resulting from the traditional approaches, and which removes the onerous requirement to define, prior to licensing, a large number of acceptable plant unavailabilities. This method uses an advanced computing facility which enables the Station operator to interactively assess and plan the acceptability of plant

unavailabilities whilst the reactor is at power, rather than prior to reactor power raise. The facility, the Essential Systems Status Monitor (ESSM), allows the maintenance and testing of the essential plant to be planned in the presence of any plant faults that may exist so that specified reliabilities and fault tolerant capabilities are always satisfied. The facility also provides advice on the replacement of faulted plant whilst maintenance and testing of plant is taking place. The ESSM contains a "living model" of possible failure modes of the essential systems which is continuously updated by the operator as plant is removed for planned maintenance, testing, or becomes unavailable due to faults, or as systems are reconfigured operationally.

This Paper describes the overall strategy for planning the maintenance and testing of essential plant at Heysham 2 in detail, summarises the development of the ESSM, and describes the benefits that have been achieved from the first year of operational use.

2. SAFETY OBJECTIVES

2.1. Overall Objectives

The overall safety objective for the planning of maintenance unavailabilities of essential plant at Heysham 2 is that, during operation, they should always ensure conformity with the arguments set down in the Station Safety Report. This Report assesses the design features of the essential cooling systems against detailed safety criteria and demonstrates that these criteria have been adequately satisfied by the design features provided. The overall objective of the maintenance strategy is to demonstrate that these same criteria are adequately satisfied during the lifetime of reactor power operation.

2.2. Safety Criteria

In the U.K. the safety criteria for the correct operation of the essential plant are expressed in terms of probabilistic criteria and deterministic criteria.

The probabilistic criteria are stringent and address both single accident events as well as the combined effects of all such accident events over a year period. One of these criteria specifies that, as a target, the total frequency of all accidents leading to an uncontrolled release of radioactivity to the environment should be less than 10—6 per reactor year. In practice this target is related pessimistically to accidents which are beyond the design basis of the plant, and in particular to the conditions of all plant available. A target of around 2x10—6 is used for conditions which include the expected unavailabilities of plant.

The deterministic criterion is generally an overriding criterion which limits the magnitude of any short term increases in risk.This ensures that following any trip or credible fault,and taking account of planned unavailability of plant, the essential systems should at all times perform their overall function assuming a single credible failure.

The effects that the occurrence of internal and external hazard events could have on the availability of the essential plant are considered in relation to the deterministic and the probabilistic safety criteria.

Overall the safety objectives consist of a balanced consideration of probabilistic and deterministic criteria and this requires complex assessments to be carried out in order to demonstrate adequate compliance.

2.3. System Features

The essential systems at Heysham 2 provide the primary gas cooling function for the reactor core, the heat removal function for the boilers, and all the necessary supporting functions required to ensure the safe removal of the fission product decay heat from the reactor following a reactor trip condition, as shown in Table 1. Each system contains in-built redundancy of plant in order to achieve high levels of reliability in operation. Diverse systems are also provided. The systems are powered from common redundant and diverse electrical distribution systems and controlled from redundant pneumatic and electrical systems. The systems are therefore highly interdependent and interconnected. The removal of plant for testing or maintenance in these systems therefore requires controls which ensure that the claims for high reliability derived from the availability of this interconnected redundant plant are not compromised.

TABLE 1. ESSM — ESSENTIAL SYSTEMS MODELLED

Post trip sequencing equipment
Pressure support system
Start/standby boiler feed system
Emergency boiler feed system
Essential electrical system
Decay heat boiler feed system
Reactor sea water system
Inlet guide vane system
Gas circulators
Circulators auxiliaries cooling system
Circulators auxiliaries diverse cooling system

2.4. Fault Conditions

The range of fault conditions for which the safety objectives are to be satisfied is extensive. The conditions range from those which result in a normal pressurised intact reactor circuit situation to fault conditions which potentially result in damage to the station plant, e.g.internal and external hazard conditions. Satisfying the safety objectives means that probabilistic and deterministic criteria are to be considered for each initiating fault condition, and that demonstrations of adequate compliance are required in each case. Some thirteen initiating fault categories are considered in the Station Safety Report in this way, including external and internal hazard conditions. These categories are shown in Table 2 in terms of groups of faults. The removal of plant in the essential systems for maintenance therefore requires controls which ensure that the remaining operational plant is always adequate for demonstrating compliance with the safety criteria over this whole range of fault conditions. In the Station Safety Report this means carrying out a separate fault sequence probabilistic and deterministic analysis for each fault condition and summing the results of all the probabilistic assessments to provide the overall figure required for demonstrating the compliance required. During power operation of the Station therefore similiar assessments are required unless some bounding pessimistic approximations can be made to reduce their extent. For such approximations to be valid in the presence of other plant failures, the definitions of acceptable plant unavailability conditions which result can be very restrictive on plant operation, and very restrictive on the flexibility of planning the maintenance of the plant.

2.5. Computerised Assessment

The complexity of the considerations required for the stringent control of the unavailability of essential plant due to maintenance is such that some form of computer assisted assessments is essential. A very limited number of these assessments are carried out,prior to operation, for the Station Safety Report as part of the demonstration that the design safety criteria have been adequately satisified. For these assesssments traditional computer codes are used. These codes are prohibitively expensive and time consuming for a large number of very detailed runs, and particularly so for the large number of computer runs that would be required to provide comprehensive advice for the control of the unavailability of plant prior to actual

TABLE 2. ESSM — CATEGORIES OF INITIATING EVENTS

1	Spurious R-trip
2.	Feed system faults Steam system faults
3	Water ingress faults
4	Primary coolant faults
5	Reactivity faults
6	Loss of grid connection faults
7	Depressurisation faults
8	Faults in essential systems

operation Such advice would require that the assessments address every possible combination of plant availability For such an approach to be viable therefore, some approximations would be required in order either to limit the number of computer runs carried out, or to limit their detail Even then there must always remain the possibility that, with the very large number of items of plant in the essential systems, some combinations of plant unavailability could be encountered during operation which have not been explicitly addressed in advance by these assessments In such a situation, the results of bounding conditions would have to be used , with the inevitable pessimisms in discounting acceptable conditions and the consequent limitations in flexibility of operation.

3. THE METHOD ADOPTED FOR PLANNING PLANT MAINTENANCE

3.1. Overall

During the construction stage of Heysham 2 Power Station, it was decided that a method of planning plant unavailability would be provided to the station which allowed the operator the maximum flexibility and which removed the pessimisms from the traditional methods previously provided in the U K.. It was clear that several alternative approaches could be considered which progressively reduced the limitations and penalties of the previous methods provided It was also clear that in order to provide a method to the operator which was comprehensive for all plant unavailability conditions then some form of interactive means of computer based assessment was required.

A second decision taken was that the combinations of planned plant unavailabilities should be considered in simple terms only, i e as acceptable or unacceptable This meant that variable timescale factors would not be considered ,so that it would not be possible to have a particular planned plant unavailability condition deemed as acceptable for a defined short period of time but unacceptable if it existed for a longer period of time

Notwithstanding this decision, it was recognised that if during planned maintenance a plant fault occurred which resulted in a condition which would have been unacceptable, had it been planned, then some temporary limited dispensation would have to be permitted to the allow

the station operator some minimum time to take restorative action. For this purpose a temporary, i.e. time limited, category was defined for these unplanned plant unavailability conditions. This category was termed an "urgent maintenance" category and was restricted to a continuous time period of 36 hours. It was also recognised that the number of these periods should be controlled. For this purpose an annual audit of such periods was identified as a requirement of the strategy adopted.

Overall, an objective to be demonstrated from the results of controlling the planned plant unavailabilities, and from time limiting the unplanned conditions which exceeded the controls applied, was that the total assessed risk when summed over a 12 month period should not be significantly different from the Station Risk Assessment for the the Safety Report.

3.2. Plant Unavailability Categories

Three conditions of plant unavailability were defined;

i). acceptable plant unavailability conditions which could exist on a near continuous basis, i.e. all planned conditions, and these were defined as "normal maintenance" conditions

ii). acceptable plant unavailability conditions which could exist on a temporary basis up to a limit of 36 hours,
i.e. unplanned conditions, and these were defined as "urgent maintenance" conditions,

iii). unacceptable plant unavailability conditions which required some short term action by the operator to restore plant or to implement a controlled reactor shutdown.

Clearly for the operator to be able to take some restorative action in the short term, when unacceptable plant conditions existed, then the appropriate advice had to be readily available to him in a form that could be quickly understood and not misinterpreted. This was therefore seen as a desirable feature of any computer based facility that was provided to the operator for assessing the acceptability of the plant unavailability conditions.

3.3. Planning Maintenance

The method of control of plant unavailability due to planned maintenance could now be defined simply as ensuring that the unavailabilities complied with the "normal maintenance" conditions.

Traditionally this control has been achieved by providing in hard copy form, a series of operating instructions, known as Identified Operating Instructions. These instructions defined all the plant unavailabilities that could be considered as "normal maintenance". One objective of these instructions was that they were easily understood and unambiguous. They were therefore very much simplified and were defined for each system, generally in isolation from other systems. They defined bounding conditions on those conditions of plant unavailability which could be considered as acceptable. They were therefore pessimistic.

For the strategy that had been adopted at Heysham 2 Power Station a computerised facility was required which enabled the planning of maintenance in a highly flexible and non pessimistic manner ,and in the presence of any possible plant unavailabilities due to faults. The facility should also provide planning advice in relation to all the probabilistic and deterministic criteria identified. In practice this has been provided by a facility specially developed by Nuclear Electric for this purpose known as the "Essential Systems Status Monitor" ,("ESSM").

4. IMPLEMENTATION OF PROBABILISTIC ANALYSIS METHODS FOR PLANNING MAINTENANCE

4.1. Types of Computerised Operator Aid

Prior to the development of the ESSM it was identified that there were several approaches that could be used in the design of the operator facility required. In general terms these differed in the flexibility of their application, the comprehensiveness of the information provided, the extent of the plant operating conditions to which they could be validly applied, and the amount of development required to implement the approach at Station.

The simplest approach identified was to define, in advance of operation, a large number of acceptable plant unavailability conditions and to allow the operator to use the computerised facility to access and search these interactively. This required that all the plant unavailability conditions that it was anticipated could occur in practice on the Station be identified , and each one be assessed for all the fault conditions for which the safety objectives are to be satisfied in terms of both probabilistic and deterministic criteria. Each condition would then be allocated to one of the three plant unavailability categories and this information stored on the computerised facility. This approach had the merit that very little development would be required for the implementation of the facility at Station. However, the approach had the disadvantages that it was extremely inflexible to any changes, either to the plant systems or to data that might be updated, that its application was limited to the plant unavailability conditions that had been assessed, and that it was limited in the comprehensiveness of the information it could provide. In implementing this approach in practice it was recognised that it could be prohibitively time consuming to assess every condition completely and that some approximations would be necessary. This could then limit further its applicability to the plant conditions that actually could be encountered at Station.

The second approach identified was to use the results of a very large probabilistic assessment carried out prior to operation and to use a computer to modify these results to follow the plant unavailability conditions as they occur during Station operation. This method provided a significant improvement over the simplest approach in that it was now not necessary to identify, prior to Station operation, all the plant unavailability conditions that would be encountered. However, due to the complexity of the plant systems being considered, and the state-of-the-art of probabilistic computer programs, there was a significant limit to the size of the assessment that could be carried out prior to operation. In practical terms this restricted the application of the approach to plant unavailability conditions when only a small number of plant items were unavailable simultaneously. The approach could potentially provide more comprehensive information than previously, e.g. in providing advice on significant plant to restore, but it was inflexible in accommodating any changes to the system or to data.

The third approach identified was to develop some special computer software for carrying out the assessments, interactively, as the plant unavailability conditions occur at Station. This approach would use the same probabilistic models used in the Safety Report, i.e. the same fault trees used for the assessments required for the previous approach, but instead of carrying out the assessments prior to Station operation they would be carried out interactively during Station operation. This meant that the assessments could be tailored to each plant unavailability condition as it occurred. The approach would therefore be extremely flexible in application and would readiliy accommodate the operating changes in systems as they occurred. It was anticipated that this approach should be able to provide the advice on significant plant to restore, as previously identified. This third approach was the one adopted for the design of the ESSM operator aid provided at Heysham 2, i.e. an approach which used a "living model" of the systems. In practice it was found that this "living model" could be used for the deterministic assessments as well as the probabilistic assessments. The facility could therefore be used for demonstrating adequate compliance with all the safety objectives required for planning the unavailability of plant for maintenance.

4.2. Plant Operating Categories

Having adopted the approach which used a method of carrying out probabilistic assessments interactively, this meant that potentially the plant unavailability categories could be defined by simple probabilistic criteria rather than by a large number of previously defined acceptable conditions of plant unavailability. Whilst this has been found to be adequate for the "normal maintenance" category of plant operation it has not been found to be sufficient for defining the limits of the "urgent maintenance" category. These required a balanced assessment of both probabilistic considerations and the overriding deterministic considerations. This was achieved by defining a limited set of rules describing plant availability conditions which were acceptable for continued Station reactor operation, albeit time restricted. The resulting plant availability categories are as shown in Figure 1. These were defined as follows;

i) normal maintenance conditions ; plant unavailabilities for which the maximum acceptable degradation in the point frequency is a factor of 10

ii) urgent maintenance conditions ; plant unavailabilities for which the overriding deterministic considerations are satisfied and for which the maximum degradation in the point frequency is a factor of around 100

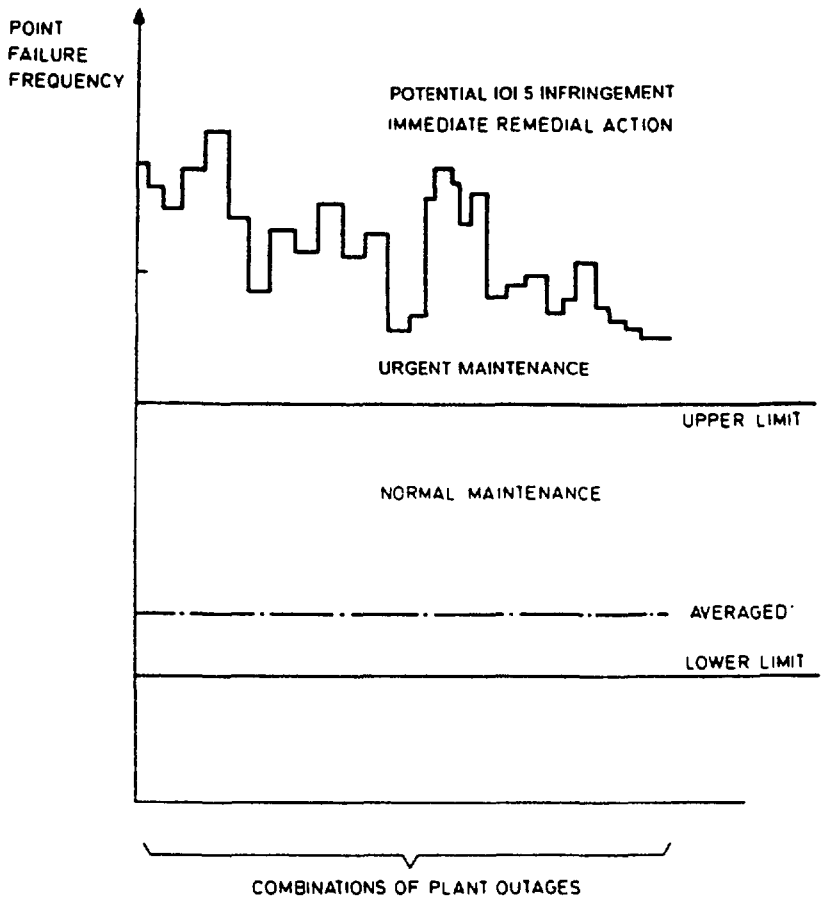


FIG. 1. Probabilistic/deterministic operating conditions.

iii) infringement conditions ; for which the overriding deterministic considerations are not satisfied

4.3. ESSM Description

The ESSM (Ref.1) is a computer based facility which solves failure models of systems over a wide range of initiating fault conditions in a fast and efficient manner. The computing times it achieves of around three minutes per overall assessment compare with the computing times of tens of hours required for the more traditional assessments using conventional codes. It achieves this, firstly, by using a specially developed computer software algorithm which quickly determines all significant combinations of plant failures which would result in a failure to provide the overall safety required. Secondly, it generates the information required to determine the possible combinations of plant failures in an efficient manner by discarding information which is not significant to the overall result. These features mean that the ESSM is particularly suited to an operator aid. The ESSM focusses its assessments directly on the information that is of interest to the operator, by generating an overall result which contains only the dominantly contributing factors in a consistent manner over all the initiating fault events.

The ESSM contains failure models of systems in datafiles, and uses these models for both the deterministic and the probabilistic assessments. This ensures a self consistent updating of the models as the Station plant availability conditions change and, in practice, allows advice to be provided to the operator on what plant should be restored to service from either the deterministic or the probabilistic considerations. The ESSM contains a feature which modifies the failure models to follow system configuration changes as they are selected by the operator on the plant. This is regarded as an important feature of the flexibility of the "living models" of the ESSM.

The deterministic rules in the ESSM at Heysham 2 Power Station are modelled for assessing the plant conditions against the single failure criterion and against the effects of internal and external hazards. This means that a demonstration of adequacy aginst the effects of hazards is not carried out probabilistically and included with the other probabilistic assessments in the ESSM. This demonstration is part of the assessment against the deterministic rules which have been defined to accommodate this. This approach is consistent with that used in the Station Safety Report.

The system features of the ESSM are shown in Figure 2. The ESSM is contained in a stand-alone minicomputer, or workstation, and at Heysham 2 power Station there are terminals for both reactors,in the control room, and terminals in the Planning Office and Computer Room. The software is contained in two separate modules and these are accessed separately from different terminals, thus providing the different levels of security required. Failure data are contained on the datafiles and these can be updated as required.

4.4. Assessment Procedure Provided by the ESSM.

The structure of the assessments carried out by the ESSM is as shown in Figure 3. The Station procedure is that when some plant unavailability occurs, either planned or unplanned, the operator enters this information into the ESSM. The software is currently menu driven and the operator selects the assessment mode. The ESSM firstly assesses the plant unavailability conditions against the defined deterministic rules and provides advice on compliance, or otherwise, with these rules. This very quickly establishes whether the plant condition is acceptable. The ESSM then assesses the plant conditions against the probabilistic criteria, and therefore determines whether the plant conditions comply with a time restricted category, i.e. "urgent" maintenance, or the normal "planned" maintenance category.

A more detailed description of the operation of the ESSM is shown in Figure 4. It is shown that the advice for plant replacement may be generated on the basis of either the deterministic or the probabilistic assessments. Illustrations of actual assessments carried out for some selections of plant unavailability are shown in Figures 5 and 6. The detailed numerical probabilistic information is not presented to the operator, but details of the deterministic assessment can be selected so that the results can be checked against hard copy rules and thereby provide an assurance to the operator of the integrity of the computing.

5. OPERATIONAL BENEFITS FROM THE USE OF THE ESSM

The ESSM has been in use at Heysham 2 Power Station as an operator aid since before power raise, i.e. some two years. The operational benefits anticipated at the design stage from the use of probabilistic analysis methods on-line, (Ref.2), have been realised in practice. In summary these are,

i) A simplification of the operating instructions for planning plant maintenance/testing

ii) Increased flexibility in planning plant unavailabilities for maintenance/testing

iii) Increased flexibility in restoring plant to service

iv) The capability of accommodating large, highly redundant, interconnected systems in a comprehensive manner

The ESSM at Heysham 2 is currently completing an enhancement programme resulting from the experience gained in its early use. The enhancements relate to improvements in computing speed, increasing its comprehensivenes in application, and providing additional hard-copy information facilities. The design of the ESSM is adaptable to such features and for further developments.

Although the numerical probabilistic results of the assessments carried out by the ESSM are not displayed to the Control Room operator ,various logs in the ESSM contain this information and these may be accessed from the appropriate terminals. This information is now being used for the annual audit, previously identified, to derive the averaged risk over a period of a year for direct comparison with the Safety Criteria. Effectively this provides what may be described as a "Level 1 PSA" type assessment operationally.

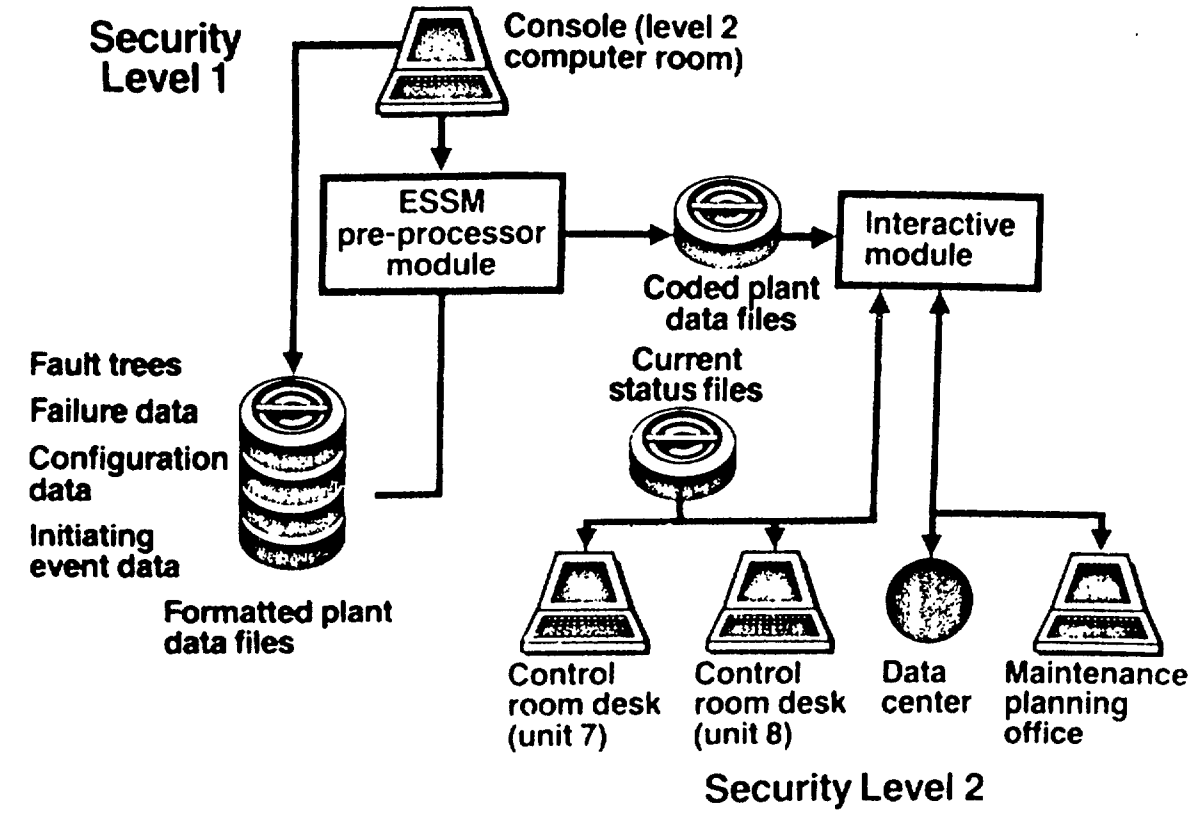


FIG. 2. ESSM computer system.

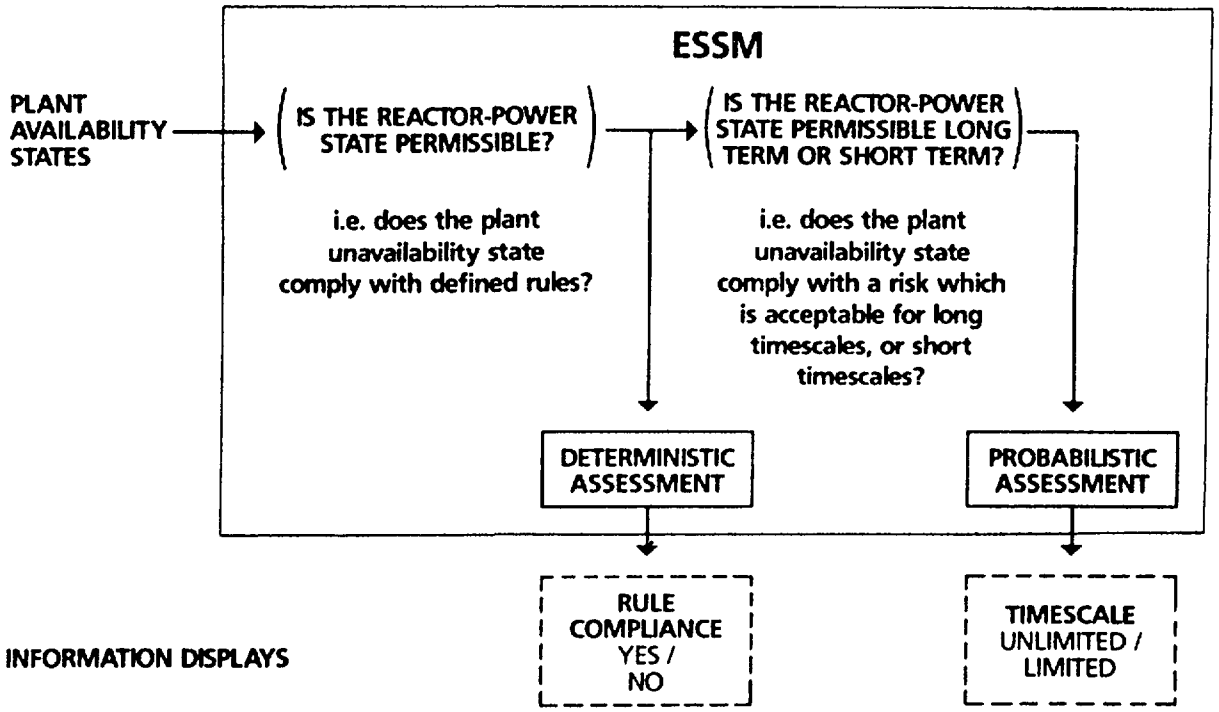


FIG. 3. ESSM assessments.

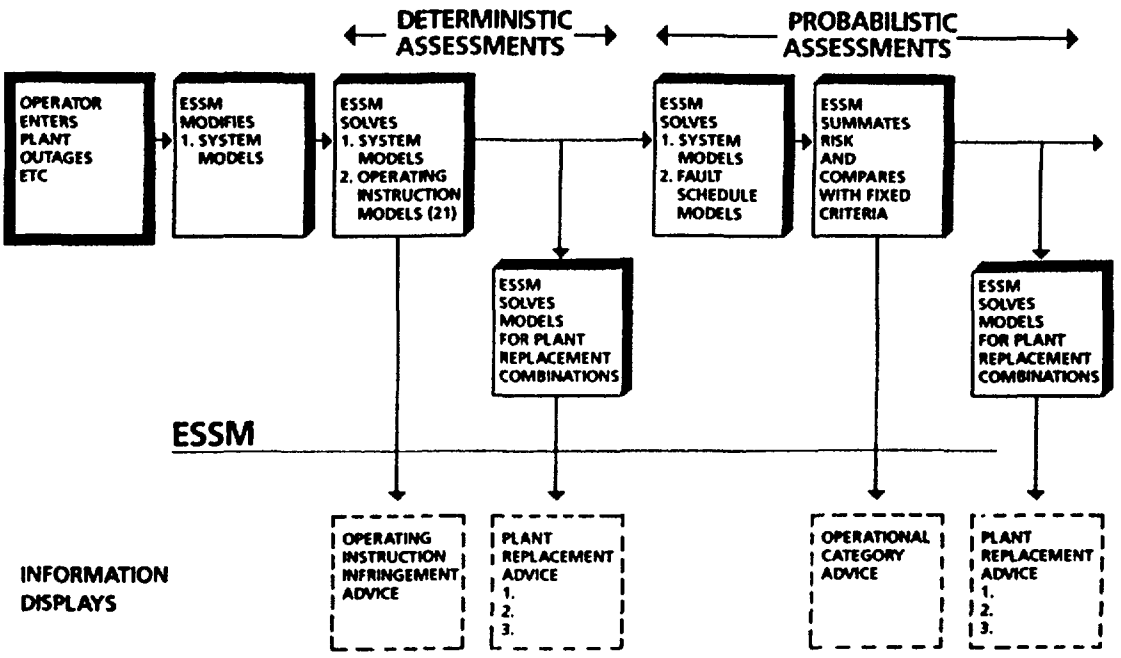


FIG. 4. ESSM operation.

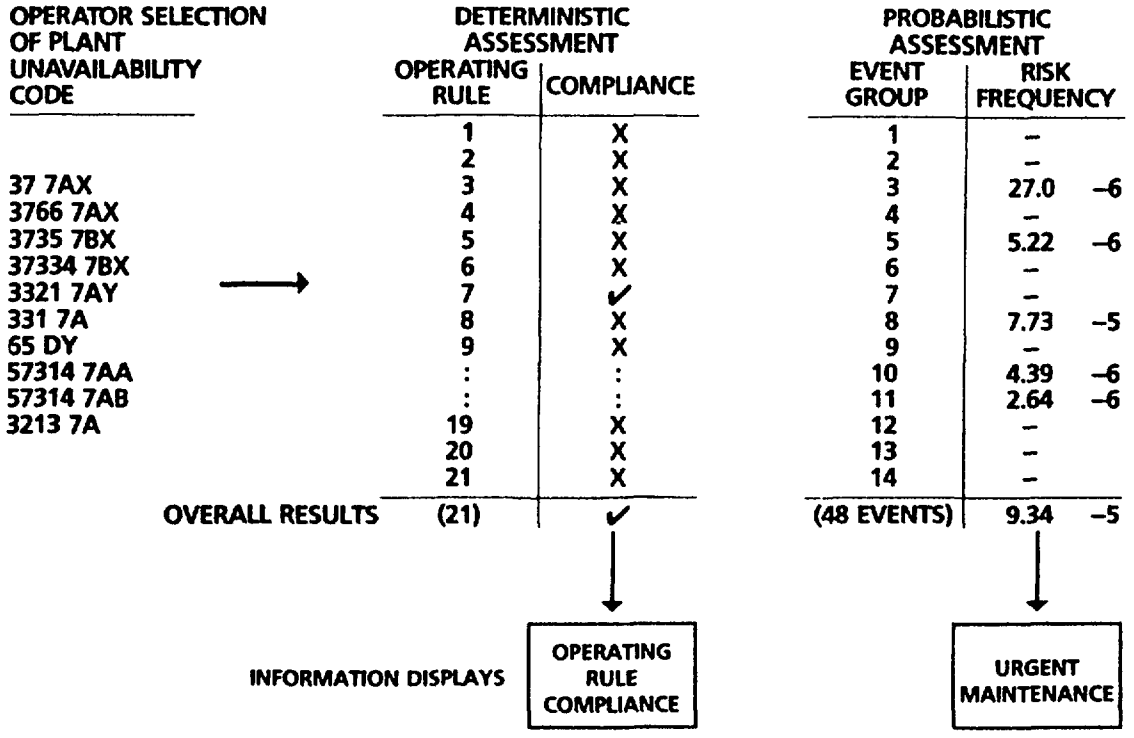


FIG. 5. ESSM assessment procedure — plant unavailability conditions complying with the deterministic criteria.

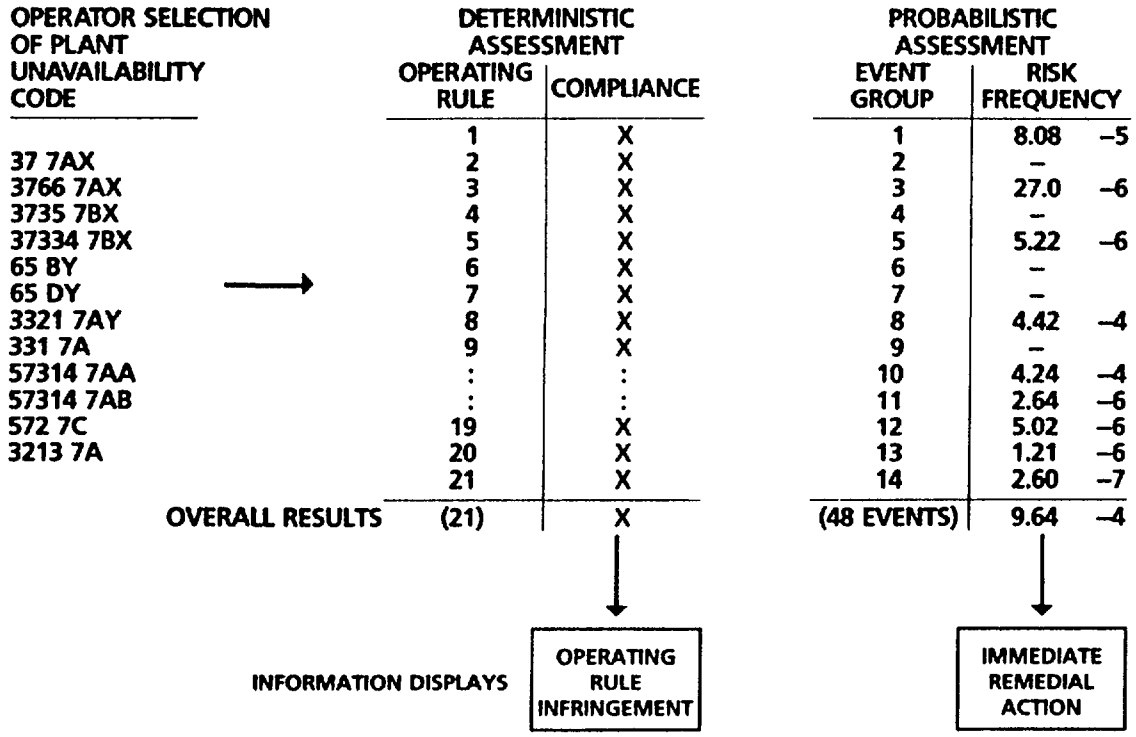


FIG. 6. ESSM assessment procedure — plant unavailability conditions not complying with the deterministic criteria.

6. CONCLUSIONS

The significant benefits from the use of probabilistic analysis methods on-line for the planning of maintenance of essential plant at Heysham 2 Power Station have been identified. Nuclear Electric has achieved the development of a computerised facility, the ESSM, which allows this strategy to be successfully implemented. Overall this has provided a more comprehensive assurance of compliance with Safety Criteria than has previously been practicable, and has introduced an effective and highly flexible "risk management" strategy.

ACKNOWLEDGEMENT

This Paper is published by permission of Nuclear Electric PLC, UK.

REFERENCES

1. "The Essential Systems Status Monitor":
International ANS/ENS Topical Meeting on Probabilistic Safety Methods and Applications: Feb. 1985: San Francisco.

2."The Introduction of Probabilistic Evaluations into the Operation of a CEGB Nuclear Power Station using the "ESSM" Facility:
International Topical Conference on Probabilistic Safety Assessment and Risk Management: Aug. 1987: Zurich.

METHODS OF EVALUATION AND SERVICE RELIABILITY OF UNIQUE DEVICES AND PLANTS

(Summary)

I.I. FEDIK, M.P. GOLUBEV
Scientific Industrial Association 'Lutch',
Podol'sk, Union of Soviet Socialist Republics

In the present report we shall give the results of approbation and choice of methods of probability analysis of service life and reliability estimation of unique products, atomic power plants (APP) among them.

In practice we see that information on APP elements and assemblies, their properties is very non-uniform. To perform elements tests and investigation of all kinds influence is usually impossible. There are data on particular tests, e.g. a reactor cassette, on some service life tests of fuel elements (besides, having a different time-table of the company), on fuel tests with deviations, on uncompleted tests, on fuel element deformation measurements, on cladding strength, etc. There are also data on analogous tests.

The aim of this work is development of a methodological approach and an effective algorithm of processing of these different data for reliability estimation of the product at the stage of design and development.

Let us consider the following typical situations.

1. Separate fuel elements and other elements are tested on service life (less or more than demanded).

2. Some elements are tested on all processes leading to breakdown (ONE), the others are partially tested.

3. There is a quantity information of a number of product parameters or a quality information of their being within tolerances.

4. The tested elements have construction differences.

5. Test conditions differ from each other, there are accelerated tests, etc.

The authors approved more than one hundred different methods of data and their combinations processing on the basis of numerical experiments. As a result of investigation we chose a number of methods which (in dependence of initial data combinations their number changes from 5 to 35) from the adaptive algorithm allowing to use practically all the information at research and development stages.

Effective use and processing of the information are performed in the following way:

1. Description of the development object (APP) by means of structural functional configuration (SRC) and obtaining the structural formula.

2. Separation of all the data (quantitative and qualitative) according to objects of prediction (product - assembly - element) into "portions". The data portions were given the corresponding attributes vector (AV).

3. SFC elements and portions are given the attributes (from AV) corresponding to the processes taking place in them and leading to breakdown. Attributes are: a breakdown type, full or partial influence of ONE, test conditions, product construction variants, data types (operating time, probability, a physical parameter).

The above-mentioned differences are described by the attributes vector for every data portion.

Then data processing and union take place:

1. Sorting and formation of "n'-data files according to the attributes vector.

2. Control of inhomogeneity, definition of its type and choice of the method (formula) for data portion union (from the matrix).

3. Choice of the SFC level and operating time for obtaining final estimations. Detection of missing data, estimation of final estimations sensitivity to the missing data.

4. Estimation extrapolation on the demanded service life and the object on the whole. Processing of the calculation results. Detection of "critical" elements (from the point of view of sensitivity maximum, information absence, load-strength, etc.). Making a list of necessary tests and investigations.

The main features of the proposed algorithm:

1. Algorithm adaptation according to the information being in the disposal.

2. Use of particular methods (in the algorithm structure) in the range of automodelity and the greatest effectiveness.

3. Use of information having a different physical nature.

4. Simultaneous use of qualitative and quantitative information, temporary halts, etc. (e.g. deformation measurements, etc).

5. Creation of physical statistic models according to the investigation results of check specimens, service-tested elements, etc. allows:

   - to unite, e.g. investigation results of pipe-lines, welds, kinetics of crack developments, etc.;
   - to obtain a provability prediction of parameters, to estimate sensitivity coefficients, etc.

6. Use of concepts on processes lending to breakdown, range of parameter change.

7. Simultaneous and independent estimation prediction with subsequent union according to:

   - SFC elements;
   - ONE;
   - breakdown types.

In addition, the above-mentioned peculiarities practically allowed to eliminate the systematic prediction error and to decrease a casual one of all probability characteristics.

The present approach has been used for three types of nuclear power plants and gave a good result.

Nowadays the work on creation of a unique program package for calculating a reliability function for IBM PC is being performed.

FEATURES OF METHOD AND PROGRAM PRODUCT USED FOR PROBABILISTIC SAFETY ANALYSIS OF NUCLEAR PLANTS

A.N. RUMYANTSEV, V.V. KARPOV, D.N. MIKHAJLYUK,
V.I. VASIL'EV, A.L. VASIL'EV, M.M. GLAZYRIN,
Yu.A. OSTROUMOV, L.M. VEKSLER, E.A. TSYGANKOV
I.V. Kurchatov Institute of Atomic Energy,
Moscow, Union of Soviet Socialist Republics

Abstract

The paper presented a method of PSA based on the formalized representation of a probabilistic model of an NPP process flowsheet in the form of the multi-component systems and elements having branched linkages, including loop (feedback structures like networks), and considered as abstract discrete automatons of the "input-output" type. If the probabilistic models investigated did not contain any loop linkages of events, this method reverted to the traditional methodology of "fault trees".

An analysis of the probabilistic characteristics of failure events is complemented with the analysis of the confidence levels of the results obtained by using the enthropic methods of error handling. Probabilistic characteristics of the failure events are described in terms of functional dependencies of time. All initial data used for determination of probabilities are accompanied by error intervals.

A method for analyzing the probabilistic characterictics of NPP design and operational safety has been developed in I.V.Kurchatov Institute of Atomic Energy. The method is based on the formalized representation of a probabilistic model of an NPP process flowsheet in the form of the multicomponent systems and elements having branched linkages, including loop ones (feedback structures like networks), and considered as abstract dicrete automatons of the "input - output" type. If the probabilistic models investigated do not contain any loop linkages of events, this method allows the interpretation in terms of the traditional methodology of "fault trees", but without application of the technique of detection and processing of so-called "minimal cut sets". The method developed makes it possible to consider explicitly the uncertainties in the probabilistic characteristics of failure events and to calculate the probabilistic characteristics of rick determining the safety.

Each component of the system element is considered to be a finite abstract automaton of the "input-output" type responsive to various input actions.The automaton is defined by the transition functions.

The transition functions are defined in the form of tables or 2-dimensional matrixes. Their lines represent the sets of input event states giving rise to the incompatible states of an output event. The tables are determined either for failure or success state of the output events. Each line in the table of the transition function defines the AND relation of the input events. Each pair of lines in the table defines the OR relation of two different sets of the incompatible states of the input events.

The probabilistic characteristics of the failure events are described in terms of the functional dependencies on time taking into account the state of the system element (continuous action, action on demand, nonavailability because of scheduled maintenance operations, etc.).

The analysis of the probabilistic characteristics of failure events is complemented with the analisis of the confidence of the results obtained by using the entropic methods of error handling. These methods are based on use of well known Shennon theorems and implement a substitution of the real, known, as a rule, with an uncertain accuracy, probability distribution of an event described by a flat curve extending indefinitely on both sides of the expected value by a step-like distribution, uniform within some interval on both sides of the expected value and equal to zero beyond this interval. Thus, the introduced entropic confidence interval subject to the equality of the conditional entropies (entropies of error) for both distributions allows the description of the probabilistic characteristics of the event with the same information (or misinformation) content as that in using the real probability distribution.

As regards the initial events it is assumed that the probability distribution in the failure state may be approximated by a lognormal distribution and by a loguniform one in the success state. The resulting distributions for the output failure events range from the loguniform to lognormal distributions. Alongside the determination of the limits of the entropic confidence intervals the expected values of the upper probability limit of failure events are found for the uniform and loguniform distributins of the upper probability limits.

The final data on the probabilistic characteristics of failure events (an accident) involve the expected (mean or median) values of the failure probability, the limits of the entropic confidence interval within which the maximum and minimum values of the failure probability are determined, and the limits of the upper and lower expected maximum and minimum values of the failure probability used for the assessment of risk.

PSA method decsribed has been implemented in a software complex BAMC which contains two software packages - BAMC-EC and BAMC-PC, differing in assignments and type of computers used.

The BAMC-EC is applied on EC and IBM-compatible main frames. This package is used for an analysis of NPP design safety and permits to develop various probabilistic models with different levels of NPP scheme structure details. The main assignment of the BAMC--EC is a variant analysis of safety and reliability of NPP design and justification of basic safety features. More over, the BAMC-EC is used for development of a "compressed" NPP probabilistic model for PC.

The BAMC-EC is developed in the operational environment the IBM-compatible main fraimes comprising an operational virtual computer system (SVM), a multiple-access database management system KVANT, a database maintenance system MIS, a multiple-access repository maintenance system SPICHKA.

The BAMC-EC containing about 40 thousands of statements in the PL/1 language consists of following basic components:

- an interactive system of initial data origination, input, check and editing;
- a BAMC database maintenance system;
- an application program system for determination and analysis of the safety characteristics with support of the intaractive modes of application program execution control;
- a system for development of a "compressed" probabilistic model for use on PC.

The BAMC-PC package is used on PC which are compatible with IBM PC/AT. The BAMC-PC is assigned for operational safety analysis on NPP ("living" PSA). A NPP probabilistic model used is created by the BAMC-EC and transferred into PC. This model is supplemented on PC by graphic and textual reference data being required by NPP personal. In a framework of this model the BAMC-PC permits to redefine any probabilistic data for initial and initiated events and its range of variation from 0 to 1, and to make a "tuning" of design probabilistic model to real NPP configuration and reliability data. Properties of the BAMC-PC permit to fix any "current" configuration of NPP equipment and systems, and perform an operational safety analysis upon NPP personal requests, including changes in schedules of control and maintainance procedures, in initial reliability data, changes in configuration of equipment and systems, etc.

The BAMC-PC package is developed in the operational environment comprising an operational system MS/DOS, a system for treatment of graphic and textual data being functionally analogue of the WINDOWS package, a specific file treatment system for manipulation of a probabilistic model and support of interaction with NPP personal

The BAMC-PC containing about 30 thousands of statements in the "C" language consists of following basic components:

- an interactive system of initial data origination, input, check and editing;
- a system for "fixing" of "current" configuration of NPP equipment and systems;
- a graphic, textual and numeric database maintenance and visualization system;
- an application program system for determination and analysis of the safety characteristics with support of the interactive modes of application program execution control.

Both packages, BAMC-EC and BAMC-PS, use the same basic calculation algorithms.

The determinate state is described in the form of a control and recovery action schedule and a maintenance schedule implemented with the element being off. The time is counted off from the moment of startup or termination of the last scheduled control action of the given equipment and systems. As to this control action, it is assumed that all controlled and maintained elements are put completely in the operable condition, i.e. "renewed".

If there are no data on the determinate state, the event states are accepted to have random distributions in time and the probabilities of the events in the failure state are characterized by a certain type of distribution (mainly, by an exponential type) with a failure rate and a range of its variation preassigned.

The probabilstic characteristics of the initiated events involving both the time-independent and time-dependent components are specified in the form of so-called "beta"-factor wich determines the conditional probability of occurrence of a dependent (initiated) event.

The BAMC-EC and BAMC-PC packages make it possible to analyze the probalistic safety characteristics of an object as a whole, its system in various modes, to analyze the effect of individual failure events and their sets on the probability of occurrence of the output events of interest, its differencial contribution to and differencial sensitivity of the output events.

The analysis of the probabilistic safety characteristics is followed by the determination of the entropic confidence intervals from the expected, maximum and minimum values of the probability of failure events (an accident) obtained by using the entropic methods of handling errors in the initial information on equipment failure rates, errors of the NPP personal, etc.

The potentialities of the current version of the program products BAMC-EC and BAMC-PC (1990) allow one to analyze the probabilistic characteristics of the NPP models describing correspondingly as many as 30 and 5 thousands of initial, initiated and output failure events the linkages of which involve an arbitrary number of feedback structures.

The maximum and minimum values for the upper limit of the entropic confidence interval and the expected values for this limit taking into consideration the width of the error range in the initial data are determined in the course of calculations with the aim of analyzing the definiteness measure of the PSA results and their sensitivity to the errors in the source data on the failure rate and probability.

The results of the calculations contain data on the maximum predicted values of the probabilities and their expected values.

The maximum predicted values coincide with the expected ones for the equipment and the systems which fall in the course of the campaign beyond the periods between the scheduled control and recovery actions. These equipment and systems undergo the control and recovery action during the planned and preventive maintenance (PPM) of NPP.

For the equipment and the systems the periodical control and recovery of which is performed in the course of the campaign the maximum predicted values can differ from the expected ones.

The maximum predicted values of the probabilities are always calculated as of the end of the scheduled control period.

This means that at any moment of time the condition of the equipment corresponds to that just prior to the control and recovery action, i.e. to the condition with the nonfailure operating time from the previous control and recovery action equal to the scheduled control period.

The expected values are determined at a given (preassigned) moment of time on the basis of the actual nonfailure operating time of the equipment and the systems from the moment of termination of the previous control and recovery action.

The differences between the maximum predicted and expected values indicate the measure of dependence of the probabilistic characteristics on the uncertainty in the observance of the control and recovery action schedule.

The following probabilistic characteristics of the maximum predicted and expected values for each event analyzed are considered as results of the calculations :

P_{max}^{ul} - maximum value of the upper limit of the entropic confidence interval for the accident event probability at the lognormal probability distribution;

$P_{max}^{(p)}$ - expected value of the upper limit of the entropic confidence interval for the accident event probability at the uniform distribution of limits within the confidence interval;

$P_{max}^{(lg)}$ - expected value of the upper limit of the entropic confidence interval for the accident event probability at the loguniform distribution of limits within the confidence interval;

P_{max}^{ll} - minimum value of the upper limit of the entropic confidence interval for the accident event probability at the loguniform probability distribution;

P_o - expected (mean or median) value of the accident event probabity (without allowance for the influence of the error range, i. e. the 'point' value ignoring the error in its determination).

With the above values of probability used the risk defined as a product of the damage by the accident event probability is calculated from the following relationships :

$$R_{eff}^{max} = P_o * (P_{max}/P_o - P_o/P_{max}) / (2 * \ln (P_{max}/P_o))^{(p)}$$

for the maximum risk commitment due to accident event per unit damage and per unit time;

$$R_{eff}^{min} = P_o * (P_{max}/P_o - P_o/P_{max}) / (2 * \ln (P_{max}/P_o))^{(lg)}$$

for the minimum risk commitment due to accident event per unit damage and per unit time.

R_{eff}^{max} R_{eff}^{min} determine the limits of varying the risk per unit damage with allowance for the errors in the determination of the initial failure rates and probabilities (experimental ones and those obtained by the expert judgement methods).

The width of the error range can be found as a maximum of the ratio of the maximum failure rate or probability to the expected one (mean or median) or else the expected failure rate or probability to the minimum one, i.e. the width of the error range shows how many times the maximum or minimum (what is higher) value of the failure rate or probability exceeds the expected value.

The width of the error range for available initial data varies in the considerable limits. The maximum and minimum values at the limits of the error range for the initial data on the failure rate and probability, for example for the NPPs with the VVER reactors (PWR type) differ 1.5 to 10 times from the expected (mean or median) ones.

At wider error ranges and sufficiently complicated probabilistic models it is necessary to take into consideration the fact of the loss of confidence of the 'point' probabilistic estimates based only on the expected (mean or median) values and the need for the analysis of the confidence interval.

The use of the 'point' estimates based on the expected values of probability can lead to more rough results of the comparative analysis of the efficiency of the arrangements on upgrading the NPP safety than the estimates using the values of risk and the entropic confidence internal.

It is evident that the backfitting of the safety systems at the expense of the addition of newly-developed elements and systems offering no representative data on the failure rate and featuring a wide error range in virtue of their novelty has a centain limit beyond whith the further arrangements on improving the safety systems can in practice reduce it.

The method of increasing the confidence of the PSA results involves the narrowing of the initial data error range by means of performing the representative statistical study of the NPP equipment and system reliability and the nonadmission of putting into operation at the NPP the equipment and systems with have a too wide range of error in the parameters determining the failure rate

As an example, some rezults of PSA for core melt frequency per year for one of VVER-1000 "paper" design are presented below. The initial variant of VVER design has not been considered as safe enough. Therefore some additional safety systems have been designed and analised by PSA methods with use of BAMC-EC package. There were 5 variants of additional safety systems differing in design and number of newly developed elements, which had no experimental data on actual reliability. For such elements the mean values for failure rate had been selected from the information on analogues equipment. But the error range had been prescribed at level of 10.

Design No	Probability of core melt,(1/y) (mean)	Risk of core melt, (1/y) min Reff and max Reff
Basic var.	6.8E-4	7.6E-4 - 1.3E-3
Variant 1	2.1E-5	2.2E-5 - 2.3E-5
Variant 2	2.1E-5	3.8E-5 - 4.9E-4
Variant 3	2.1E-5	2.8E-5 - 4.2E-5
Variant 4	2.1E-5	2.2E-5 - 2.3E-5
Variant 5	2.1E-5	3.3E-5 - 1.1E-4

Rezults of PSA presented above show that being practically identical in terms of expected core melt frequency, various designs are differing in terms of risk which had been calculated with taking into account the range of uncertainties of failure rate.

Taking into account the values of risk, the preference of design variants may be listed in order 1, 4, 3, 5, 2.

DEVELOPMENT OF BASIC SOFTWARE FOR PSA BASED TECHNICAL SPECIFICATION EVALUATIONS

M. BORYSIEWICZ
Institute of Atomic Energy,
Otwock-Świerk, Poland

Abstract

The recent findings concerning PSA application to the technical specifications evaluations indicate that general puprose PSA level 1 computer programmes need to be extended to provide an efficient tool for PSA-based Technical Specifications evaluation. In the Institute of Atomic Energy, świerk, the effort is focussed on:

(i) development of a software environment (itegrated package of codes and structured data bases) that faciltate computing various risk measures as functions of AOT's and STI's parameters, with minimum reanalysis of minimum cut sets that may already exist from PSA studies,

(ii)implementation of detailed component unavailability models and MCS probability calculation algorithms that account for three individual segments of component unavailability cycle (i.e. test, repairand between tests) and different testing and maintenance schemes of plant items represented by MCS elements.

The general conclusion from the work to date is that the use of selected PSA micro-computer codes and data bases integrated with mainframe versions of codes with capabilities of SETS, SEP and SOCRATES may ensure achievement of goals (i) and (ii).

Generally, complexity of modelling and numerical difficulties limit the use of the Markovian process in safety and reliability analyses to relatively small systems. The areas of TS techniques, where is going to be better identified.

---

1. INTRODUCTION

A number of problems with Technical Specifications (TS) such as Limiting Conditions of Operations (LCO), Allowed Outage and Surveillance Times AOT and STI have evolved over the years. First, as nuclear power engineers have become more and more specialized in various technical areas, TS have grown in detail and become voluminous documents. This development tends to divert attention away from the principal safety parameters while focusing on detailed surrveillance of lower importance systems, an undesirable trend which should be reversed in the interests of safety.Another problem is that it has become difficult to change TS quickly.

The voluminous TS have become burdensome and costly to utilities in a way that does not contribute to safety. Also, the numerous detailed TS issued today have equally numerous action statements with time limits. Thus, a utility may have a large number of clocks tickinng,each with its own deadline, with a technician assigned to monitor them for different actons required to prevent TS volations. Moreover it has not been in the past discriminated between utilities with excellent preventive maintenance programs, who may not need prescriptive TS, and utilities with poor preventive maintenance programs who may need them. Rather, it has concentrated on standardized specifications which would be applied to utilities uniformly to protect against the worst performers.

Nowdays techniques and concepts applied in Probabilistic Safety Assesment (PSA) and System reliability Analysis (SRA) can provide a uniform and balanced approach to TS evaluation. Different PSA measures of risk importance can be established and used as a basis for establishing concepts of optimal TS parameters and methodology which would be capable to make use of existing PSA data for performing futher quantitative analyses [10-13].

To optimize a plant's existing TS one goal can be to establish AOTs that reflect components importance to risk. The risk achievement worth represents the increased plant risk status when a component is out for Test and Maintenance (T&M). By quantifying all risk achievement worths for components regulated by the plant's TS aquantitative ranking can be established. This quaantitative ranking can be compared to a corresponding ranking in the present plant TS.

Another parameter of interest for this analysis can be the shutdown risk increase. Certain components may have short AOTs which force plant personel to shut down the plant upon detection of a component's outage based on LCO. However, the loss of the component may actually compromise the plant's shutdown cooling capabilities to the point of increasing plant risk during shutdown. The measure of this risk inrease may be called, the shutdown risk achevement worth.

Thus to determine the optimal AOT, two importance measures must be defined:

- a components Accident Sequence risk Achievement worth (ASA) with respect to the risk characteristics determined by a PSA study

- the Shut Down Risk Achievement (SDA) by the PSA by usind only the set of accident sequences that represents sequence of events developing from a manually initiated shutdown

It may be expected that with respect to SDA and ASA we can distinguish the following component groups

- none or negligible SDA. The ASA decides the AOT.The plant risk status has changed in such way that the plant should be shut down according to the indicated AOT.
- small or medium SDA. The ASA decides the AOT. The plant risk status has changed in such way that the plant should be shut down according to the indicated AOT, but in specific cases when the AOT is too short and an extension of AOT is discussed,an extension may be preferable.
- medium or high SDA. The AOT indicated by the ASA alone must be modified due to the SDA. The plant risk status has change in such way that a shut down at this point probably will increase the risk status further.

With SDA and ASA calculated and groupped for different accident sequences the AOT for a NPP system can be analysed and conclusion drawn regarding possible changes of AOT.

The PSA studies are very much bound to the Fault Tree(FT) - Event Tree (ET) techniques. One of the important result of such studies is collection of Dominant Minimal Cut Sets (MCSs) contributing to:

- system unavailablity
- function unavailability
- core demage sequence occurence
- radionucklide release sequence occurence

In standard PSA studies the computer codes used for quantification of FT and accident sequences calculate the probability of a MCS, say M, as product of averaged over a time interval probabilities of components that define M,ie:
if $M = A \circ B \circ C$ then the probability of M, Pr(M)
is set to:

$$\overline{Pr(A)} \circ \overline{Pr(B)} \circ \overline{Pr(C)}$$

where

$$Pr(x) = \frac{1}{T} \int_0^T dt\ Pr(x)(t)$$

Moreover, the formulae used in PSA studies to calculate $\overline{Pr(x)}$ make use of simplified models of dependence of a cmponents unavailability in time,that do not adequately portray component

characteristics and T&M strategies. Therefore general purpose PSA Level 1 software needs certain upgrading to serve an efficient tool for PSA based TS evaluation.

These improvements should be concentrated on
- development of software enviroment (programs, and structured data base that facilitate to calculate different risk measures as function of AOT and STI parameter, with minimum re-analysis of MCSs that may already exist from PSA studies
- development of sophisticated component unavailability models that may be easily handled by time averaging algorithm for calculating MCSs probabilities

The advantage of using Markov processes in reliability problems have been recognized since the inception of the reliability discypline. Generally, numerical difficulties, limit the use of the technique to relatively small systems.

Hovewer recent developments have made the Markovian modelling relevant both for PSA studies and seperate NPP system TS evaluation.

Brief review of the software development at the Institute of Atomic Energy, Świerk, for both approaches to TS evaluation(FT-ET and Markovian modelling) is presented in the following sections.

2. FAULT TREE METHODOLOGY AND CODES

The advantage of fault tree methodology as an analysis tool is that it can explicitly model each component within a system, thereby making it ideal for assessing the impact of STIs and AOTs, as well as for periodic reverification of system performance.

The following five items can be explicitly modeled in each fault tree:

- Unreliability of components due to random failures
- Unavailability of components due to test
- Unavailability of components due to maintenance
- Operator errors
- Common Cause Failures

Thus in frame of the FT-ET methodology the impact of icreased STIs, AOTs, andequipment bypass can be determined and compared to the reliability of the system considering present day test and maintenance practices.

The increases in the surveillance intervals and test and maintenance times can be determined by considering hardware performance, actual time needed by operating plants to perform these activities, and practical aspects of implementation.

For effictive use of FT-ET modeling features in practical TS evaluation it is necessary to develop computer aids capable to

(i) develop update and store FT and accident sequences models
(ii) generate and store MCS for further manipulation MCSs
(iii) develop update and store data sets such as Fault Summary Tables compute
(iv) compute different risk measures for TS evaluations with minimum reanalysis of existing MCSs generated by a "basic" PSA study or a system reliability analyses

Current status of such computer aids developed in the Institute of Atomic Energy is given in Fig. 1. The Tables 1 - 6 present capabilities of various calculational moduli. Some of them go beyond the needs of typical PSA Level 1 and SRA studies. They have been adapted/developed to create certain possibilities of performing analyses typical for the technical specifications evaluation and risk management problems.

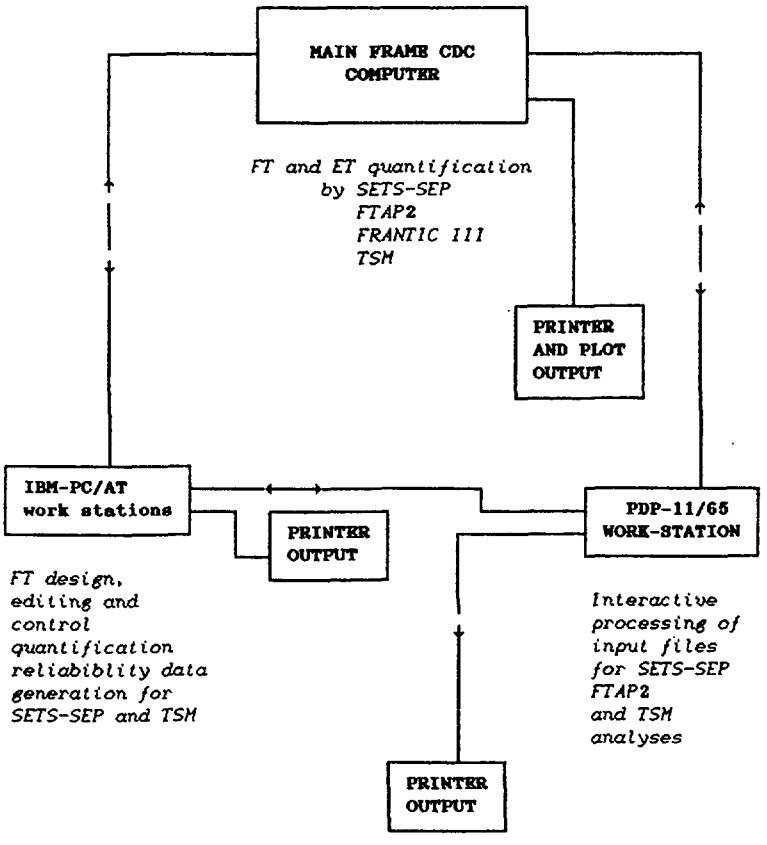


Fig. 1 Computer aids for PSA Level 1 and TS Analyses in the Institute of Atomic Energy, Świerk.

Table 1

MAIN TASKS FOR PC - WORKSTATION

- Developing FTs
- Editing grafic form of FTs
- Transformation of grafic form of FT into input to SETS and FTAP2
- Preparation of reliability date files for SETS-SEP quantification
- Analysis of moderate size FTs by FTAP2
- Fault Summary Tables generation and updating
- Processing of component unavailability model parameters for risk measure calculation for technical specification evaluation by TSM code

Table 2

PC WORK STATION PERMANENT FILES

Main permanent files:

- **PSA-PACK [5]**
- **RELPACK [6]**
- **MARADB RELIABILITY DATA BASE MANAGER [7]**
- **RELDAT** for reliability data sets generation: Fault Summary Tables, Value Blocks for SETS-SEP and component unavailability model parameters processing for generating input data for TSM code

Auxiliary data bases for an analyst developing FT model

- *EASY TOOL-TECHNICAL SPECIFICATION DATA BASE MANAGER* **[8]**
- *BDEJ NPP SYSTEM DESIGN DATA BASE MANAGER* **[9]** *supervising a data base that includes information on:*
  - *design of front line and support systems relevant for PSA studies*
  - *component status monitoring*
  - *location of components and type of enviroment*
  - *type of test, maintenance and calibration procedure*
  - *functional relations between each component of a system and other components and systems*
  - *admissible operational regimes of components and systems*

Table 3

PDP PERMANENT FILES

- Input data for SETS-SEP interpreter
- Generic FT input files
- Processed FT files, containing largest independent subtrees (macroevents) and stems (FT structures expressed in terms of macroevents)
- Minimal Cut Sets files
- Reliability Data Block files for SETS-SEP and TSM

Table 4

RELPACK MAIN FUNCTIONAL MODULI

- MOGOS:
  - FT design
  - FT grafic editor
  - automatic FT input preparation for SETS-SEP and FTAP2
- FT analysis by FTAP2

RELPACK FUNCTIONAL MODULI FOR RISK MANAGEMENT ANALYSES:

- FTAP2 results processing to obtain FT Boolean equation suitable for input to FRANTIC III
- SYSCOM-SYSOP:
  Direct definition, updating and storing Boolean equations for input to FRANTIC III
- Processing of MCS obtained by SETS-SEP or FTAP2 analyses to obtain input suitable for TSM
- FRANTIC III time dependent reliability analysis
- STAGEN-MARELA for time dependent reliability analysis of systems with multistage components

Table 5

MOGOS FT DESIGN AND EDITING CAPABILITIES

. FT generator comprising:
- definition of gates (OR, AND, N/M, NDT, NOR), event type (Basic, Transitive, Developed), event description (57 characters in 3 lines)
- 6 events per one screen
- input lines to gates can be automatically continued on the subsequent screens
- 4 screens are edited on one page of line printer
- any events can be changed or removed
- new inputs can be added to existing events
- 50 screens for one FT

Table 6

RELIABILITY DATA GENERATION (RELDAT)

. Interface with failure rate data base
. Functional modulir for interactive preparation and updating of Fault Summary Tables, that account for component attributes, component unavailability model parameters, fault expose time, maintenance strategy, human error component agregation (super - - components corresponding to system segments)
. Value Blocks generation for SETS and SEP
. Processing of component unavailability model parameters for preparation input data to TSM
. Interface with HRA program package

It has been found that the codes SETS, SEP provides technical means for creating a flexible software enviroments for performing tasks (i), (ii) and in part the task (iii) from the above list i.e.developing , handling and quantification of complex FTs and ETs. These features are particularly important for the first stage of PSA Level 1 studies, when probabilistic models of accident sequences are being developed so that they may be both detailed and

easily handled by available codes and computers. Currently the sofware of computer work station (IBM-PC and PDP based) provides preprocessing and postprocessing and editing functions for main frame computer resident programmes (SETS-SEP, FTAP2, FRANTIC III) and TSM).

The advantages of the SETS code are its generality and flexibility, one example of which is the ability to dynamically manipulate the tree via SETS user programs. The SETS program itself is an interpreter which reads, interprets, and executes SETS user programs. The user writes a SETS user program specifying the processing to be achieved and submits it, along with the required data, for execution by SETS. This program directs the processing of the input and the order in which it occurs. The SETS program uses three different files: the equation file, the block file, and the value block file. The block file is a storage file used to store fault trees and Boolean equations. The equation file is a work file used to process equations. The analysts uses SETS procedure calls for selective processing of the content of the SETS files, depending on the type of analysis desired. This capability gives the user a great deal of control over the processing, a feature which can be especially helpful when analyzing large trees. For example, a SETS user program may be written to decompose the original tree and process it in stages without requiring any changes to the original fault tree input description. An additional feature enables SETS to automatically identify the independent subtrees and select stages for efficient processing of large trees. A packed, bit-level storage scheme and use of auxiliary storage are other SETS features aimed at efficient processing of large trees.

The SETS user is not concerned about entering input data in specific columns or other specific spacing, i.e. a free format of FT input is interpreted by the program. The admissible number of characters of intermediate and elementary events facilitate to accommodate the rules:

. names of intermediate and developed events are readible catenations of letters from words used to define these events in natural language, for example:

LP-SW-S112 - loss of power to service water segment 112;. name of a basic event is of the form A B C, where:

A - string of characters identifying the component on plant drawings,

B - generic type of component according to classification used in the reliability data base,

C - failure mode according to classification used in the reliability data base.

The programs SETS-SEP interpret besides standard OR and AND gates also complemented event and SPECIAL gates, the latter corresponding to intermediate events that are any legitimate Boolean expression of their inputs.

Besides efficient procedures for FT processing, the SETS provides also flexible tools for Boolean equation manipulation such as:

(i) substitute in equation,

(ii) reduce and factor equations,

(iii) compute term values,

(iv) truncate on term value,

(v) delete terms of an equation that are multiplies of terms of another equations.

They are of particular importance for an accident sequence analyses, once truncated MCS equations have been generated for systems relevant for this accident sequence definition. In particular (v) is usefull for consistiency checks of MCS of failed systems with success criteria of unfailed systems.

The original capabilities of SETS for accident sequence analysis are augmented by SEP procedures:

. Generation of a new equations containing only certain terms from an existing equation - these terms are selected on the basis of their order and/or their contribution to the probability values of the existing equation;

. Measuring the importance of events in an equation;
. Improved point estimates of probability values of an equation;
. Determination of the probability distribution for an equation, with additional provisions for common cause failure and test and maintenance events.

Another usefull feature of SETS-SEP programs is a comprehensive error diagnostics and monitoring of essential execution steps during processing the user programme.

To easure performing task (iv) of the list at the begining of this section a code TSM is being developed. The main functional characteristics of the code are similar to those of the code SOCRATES [10] i.e. depending on the nature of the cutsets, TSM will addres:

. safety system or function unavailability
. core damage frequency
. radionuclide release frequency

The code TSM will
. Allow more detailed analysis of allowed outage time and test intervals
. Evaluate AOTs and STIs simultaneously for any group of components
. Allow evaluation of interactions between allowed outage times and test intervals
. Allow different testing shcemes
. Evaluate conditional, unconditional, maximum and cumulative risks.

The program TSM will have a very detailed component unavailability model that allows evaluation of three individual segments of a component's unavailability cycle (see Fig.2)i.e:
. test phase -- a scheduled downtime period for testing or maintenance

. Downtime phase -- an unscheduled downtime period for repair or maintenance

. Between test phase -- the period between scheduled test and maintenace in which failures are not detected.

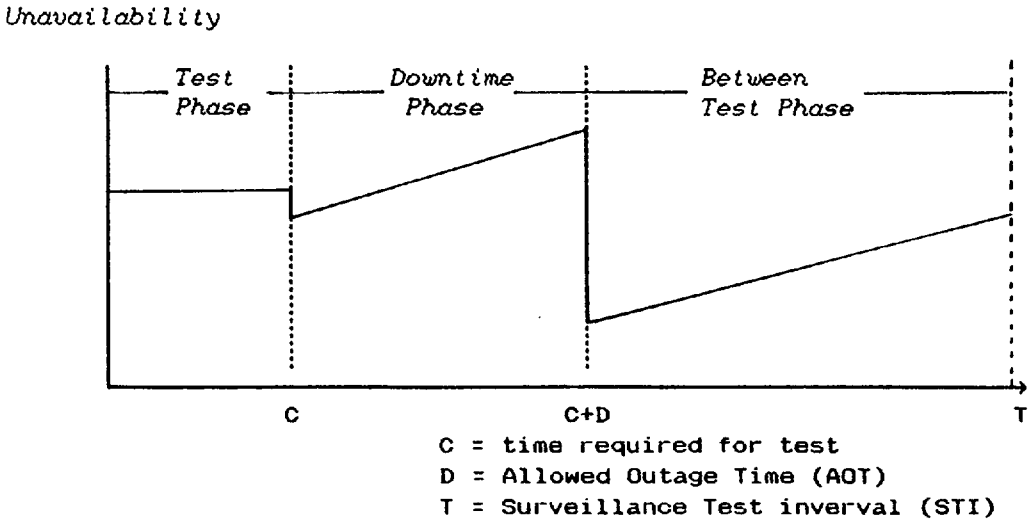


Fig. 2 Component Unavailability Cycle

Table 7 gives details of the component unavailability models in each phase.

The component unavailability model of TSM easily adapts to include:

1. Monitored components
2. Non-tested (non-repairable) components
3. Constant per demand components
4. Components having a constant per demand contribution plus an exponential per hour failure rate.

The codes TSM will handle

. Simultaneous testing where the components test phase, downtime phase,and between test phase coincide

. Sequential testing where the component test phase is offset so that the components are tested immediately after one another

. Staggered testing where the component test phases are offset such that the tests are evenly placed throughout the test interval.

Table 7

COMPONENT UNAVAILABILITY EQUATION

$q(t) = q_o + (1-q_o)\rho + (1-q_o)Q$	$0 \leq t < c$ (test phase)
$q(t) = \rho + \gamma + kQ + \lambda(t-c)$	$c \leq t < c+d$ (downtime phase)
$q(t) = \rho + \gamma f + Qr + \lambda(t-c)$	$c + d \leq t \leq T$ (between test phase)

q_o = probability that the test cannot be overriden on demand

Q = probability the component enters the test failed

γ = probability of a test-caused failure

λ = component failure rate

k = allowed outage time (AOT) occurrence multiplication factor

r = fraction of Q that is not detected during the test and not repaired before the next test

f = fraction of γ that is not detected and not repaired before the next test

ρ = probability of component failure on demand

c = allowed outage time (AOT)

T = total test interval, i.e.,the time from the begining of a test to the begining of the next test.

The input data requirements for the program are in three categories: MCSs generated by SETS-SEP, component unavailability parameters prepared by RELDAT and TS strategies.

3. MARKOVIAN MODELLING AND CODES

The specific areas that the Markov model improves over the current PRA technique (e.g., Fault tree analysis) are the following:

- **Modeling of multiple states for components and system**
- **State dependences**
- **Renewal effect of challenges**
- **Inclusion of the "no core damage" and "core damage" states.**

The Markov model calculates the effect of these characteristics by considering their impact dynamically as a function ot time.

The codes STAGEN/MARELA [14]that are part of RELPACK package perform the followin steps of a Markovian Reliability Analysis:

. STAGEN generates all possible states of a system in the form of a 2-dimensional array. Each row of the array corresponds to a system-stato.. Each elemnt of a row corresponds to a particular component statc. With the help of a user supplied subroutine, the code characterizes each system-state as being an "operating" "up" state or a 'failed" "down" state. further characterization of a system state is possible. That is, non-binary situation can be handled. An example is a safety system of a nuclear power reactor. the system can be up or down while the reactor is on-line or shut down giving rise to four possible kinds of system states.The code next orders the states according to increasing numer of failed components. This ordering makes the generating of matrix A, and the solution of Eq (* *) efficient.

. Given the set of system-states and information on individual component failure, repair and testing characteristics, as well as any dependences of these characteristics on the state of the system, MARELA does two things:

(i) Gernerates the transition Probability Rate Matrix A with $a_{ij}dt$ being the probability of transiting from state i to state j in (t,t+dt) being in state i at time t.

(ii)Solves the equation

(* *) $\pi = \pi(t)A$

The transition rate Matrix A is generated and stored in such a way that only the non-zero elements needbe stored.

Examples of system modelling for STAGEN.MARTELA analyses can be found in App A [11,12].

4. CONCLUSIONS

The general conclusion from the work to date is that the combined use of microcomputer based PSA codes, data bases and generic microcomputer software with main frame version of SETS SEP and TSM significantly facilitate performing PSA Level 1 study am TS evaluations. The microcomputer work stations and related software perform functions of pre and postprocessors for the SETS-SEP and TSM so that the analyst may not be concerned about complexity of large FT and MCS equations input preparation for these codes. This significantly facilitates adequate use of unique features of SETS, SEP and TSM for large FTs and accident sequences analyses.

Model maintenance is a necessity for large reliability modeling projects and PSAs. Models are continually modified during the project and are updated periodically after the initial project is complete.

Model maintainability requires keeping the fault tree models current and documented, keeping the database up-to-date and consistent with the fault tree models, and keeping the cut set files consistent with the fault trees and the data.

The recently developed at the IAE computing aids are particulary suited for effective modeling maintenance.

The main tasks ahead concern:
. better integration of developed software for PSA Level 1 a TS studies,
. further developing functional moduli for utilization of PSA models for TS problems.

Appendix A

Markovian Model for 3 DG station of EPS

In order to assess the average unavailability with the reactor on line and the expected shutdown time resulting from exceeding the AOT for various EPS system configurations as a function of the AOT, a Markovian model can beendeveloped. The model is a K-out-of-N configuration; i.e.; K out of N diesels are necessary for success. The stochastic behaviour of each diesel is simulated by adiscrete state Markov proces with four states. The state transition diagram for this process is shown in Figure A1. The principle of the model is explained further on Figure A2 which shows a simplified state transiton diagram of an EPS with 3 diesels.

An 1 -out-of-3 system is unavailable whenever all three diesels are unavailable, that is whenever the system isin states 4, 4' or 4" (see Figure 2). Assuming that the consequences of a challenge with EAC unavailable and the reactor shutdown are negligible, the unavailability of the system (with the reactor atrisk) is given by

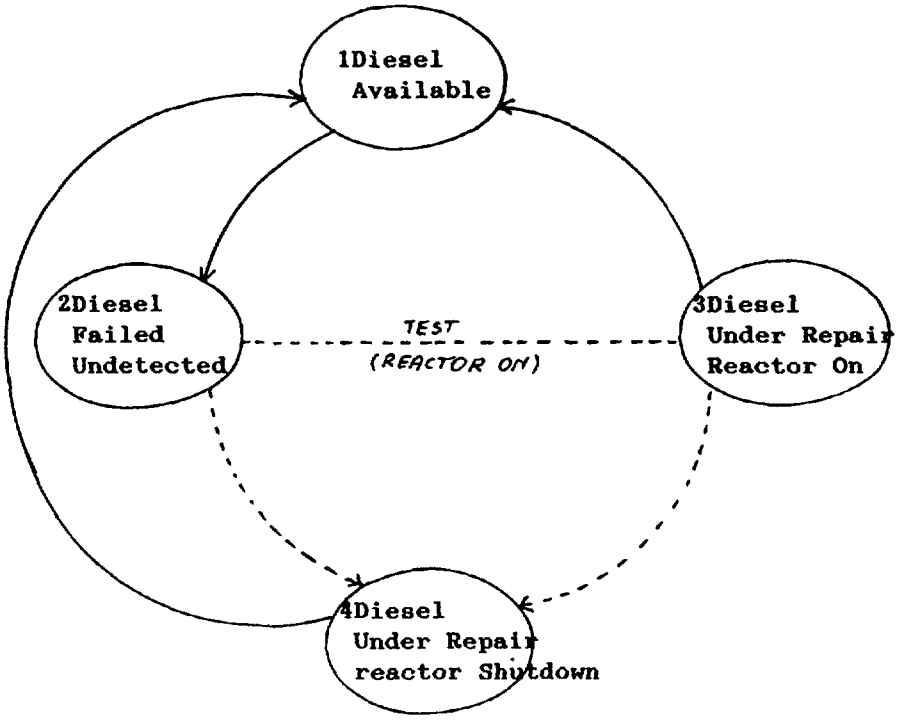


Fig A1. State Transition Diagram for Single Diesel

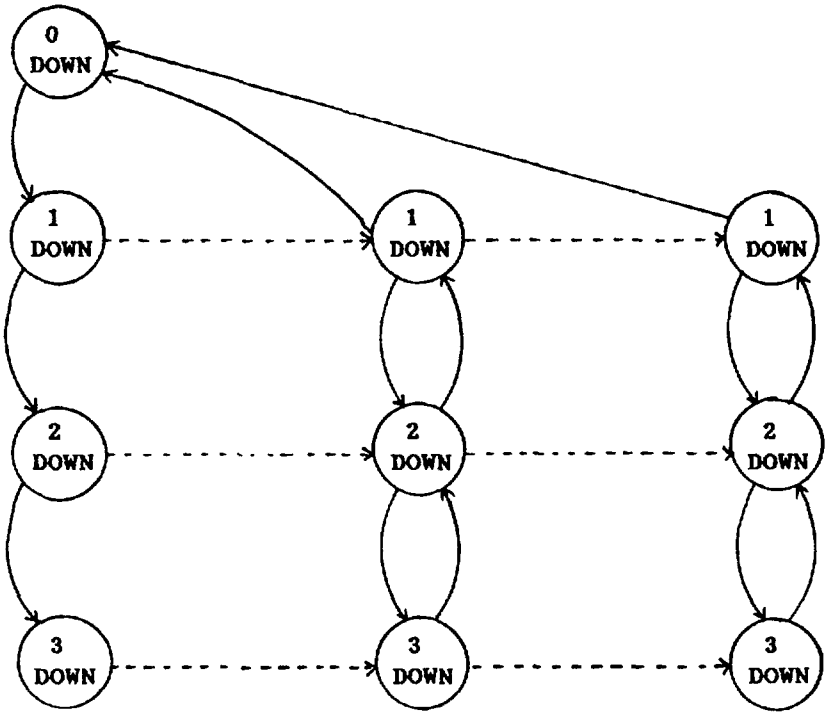


Fig A2. Simpified Transition Diagram for 3-Diesel System

$$U(t) = p_4(t) + p_4'(t),$$

where $p_4(t)$ and $p_4'(t)$ are the probabilities that the system occupies a state of type 4 and 4' respectively at timet t.

On the other hand, the reactor is shutdown whenever the system is in any state of type 2", 3" and 4". Thus, the probability that the reactor is shutdown at time t is

$$S(t) = p_2"(t) + p_3"(t) + p_4"(t),$$

where $p_2"(t)$, $p_3"(t)$ and $p_4"(t)$ are the state probabilities for state-types 2", 3" and 4", respectively.
The probabilities $p_2", p_3", p_4, p_4', p_4"$ can be calculated easily by STAGEN/MARELA.

Transition from state 2 tostates 3 and 4 takes place with probability one, depending on whether the reactor is online or shutdown (this latter distinction is meaningful when two or more diesels are included in the model). Diesel under repair can remain in state 3 only for a fixed predetermined period of time α. If this time is exceeded without completing the repair of the diesel continues (state 4). the transition from state 3 to state 4 takes place with probability one, once α units of time have benn spent in state 3.

In Phase A the diesels may go to failed states 2,3 or 4 but the failed diesels are undetected. In Phase B, after a test, the failed diesels are detected and repair begins, the reactor is up (states 2',3',4'). the systems can reemain in these states only for a predetermined amount of time which oin general depends on the particular states ($\alpha_1, \alpha_2, \alpha_3$). Then it transits to Phase C. In Phase C the failed diesels continue to be under repair but the reactor shuts down (states 2",3",4"). in each phase the system can trasit among the states of the phase due to additional failures and repairs. When all diesels have been repaired the system transist back to state 1 and the reactor is started up again.

Markovian model of a Reactor Protection System

An analog channel of RPS can be represented in the state transition diagram by a five-state component:

State 1: is the operating state

State 2: is the failed state. the failure can be detected in the next test and the component will be put under repair

State 3: is the tripped state. the channel generates a trip signal and it may undergo repair

State 4: is the bypass state related to Satte 1. the channel can be bypassed for the allowable bypass time (ABT). At the end of this period the channel transists instantaneously to state 3

State 5: is the bypass state related to State 2

When the allowable bypass time is small compared to the mean time of channel failure, the two test states (4 and 5) can be omitted by assuming that transitions lin and out of states 4 and 5 occur instantaneously at the time of testingand with appropriate probabilities (see Figure A2).

The state transition diafgram for the logic treain and trip breaker is similar to the one of the analog channel.

The RPS states cash generated by the computer code STAGEN and into following nine groups:

1. RPS available with no tripped analog channel
2. RPS available with one tripped analog channel
3. RPS unavailable
4. Real scram with no core damage
5. Real scram with core damage
6. Spurious scram with no core damage
7. Spurious scram with core damage
8. ATWS with no core damage
9. ATWS with core damage

For the determination of the probabilities of these RPS states the computer code MARELA can be used to obtain numerical values for attributies of interest in the evaluation of the LCO polities:

1. The core damage probability per reactor year
2. The average reactor downtime per reactor year

REFERENCES

1. R.B.Worrell, SETS REFERENCE MANUAL, NUREG/CR-4213.

2. M.D.Olman, Quantitative Fault Tree Analysis Using the Set Evaluation Program (SEP), NUREG/CR-1935.

3. Desmond W.Stack, A SETS User's Manual for Accident Sequence Analysis, NUREG/CR-3547.

4. T.Ginsburg, J.T.Powers, FRANTIC III - A Computer Code for Time-Dependent Reliability Analysis, Div. of RM and Operation Office of NS NRC, April 1984.

5. A.Bojadijev, L.Lederman, H.Vallerga, PSA-PACK, An Event Fault Tree Package for PSA Using PC, Proc. Int. Top. Meet. "Probability Reliability and Safety Assessment, Pittsburgh, April 1989.
6. A.Drożdżal, G.Mandziejewski, W.Zając, RELPACK - An Integrated Package for System Reliability Assessment, Institute of Atomic Energy-Świerk, Int. Report 46/EII/89.
7. E.Piwek, MAEADB - A PC Manager for Reliability Data Base, Institute of Atomic Energy-Świerk, Int. Report 71/E-SCO/88.
8. L.Sumati, EASY-TOOL - A PC Manager for Technical Specification Data Base, Institute of Atomic Energy-Świerk, Int. Report 44/EII/89.
9. E.Piwek, H.Wojciechowicz, BDEJ - A PC Manager for NPP System Design and Operation Data Base, Int. Report 41/E-SCO/89.
10.W.E. Vesely et all - Methodology for risk-based analysis of technical specification, Int. Topical Meeting on Probabilistic Safetymethods and Applications, San Francisco California, 1985
11.A.Papazoglou et all - Probabilistic Evaluation of Limiting Conditions of Operations Outage Times for Diesel Generators, ibidem
12.A.Papazoglou et all - A Markovian Analysis of Limiting Conditions of Operation for the Reactor Protection System, ibidem
13.G.Johanson - Evaluation of Allowed Outage Time Using Pra Results, ibidem
14.A.Papazoglou, A Coole for Markovian Realiability Analysis of Systems, User's Guide

NPP CHANNEL STRUCTURE SAFETY SYSTEM RELIABILITY ANALYSIS

Methods and computer code SHARM-2

E.F. POLYAKOV, E.A. SHIVERSKIJ, G.Yu. LOSKUTOV
Research and Development Institute
of Power Engineering,
Moscow, Union of Soviet Socialist Republics

Abstract

Special investigations on the methods for reliability assessment of safety related systems was performed in accordance with the development of general methodology for the NPP probabilistic safety analysis (PSA) in the USSR. The methods are based on the present-day advances in the field of NPP safety systems reliability and meet the main requirements placed on system analysis in performing the PSA.

The methodical principles are implemented in SHARM-2 computer package used for the RBMK system reliability assessment. The main results of methodology and computer code development also are given.

METHODS FOR RELIABILITY ASSESSMENT

General

Methods are used to assess the reliability of safety grade systems as applied to functions specified by safety requirements.

The reliability indiced are follows:

$\bar{\omega}$ - average value of failure rates as frequency of the initial events (or hazardous failures);

Q_d - probability of failure to function on demand (for short-term safety systems);

Q_f - probability of failure to function on demand (for long-term systems).

There are three stages for performing the reliability estimates of safety systems in accordance with the methodology:

1) Qualitative reliability analysis;
2) Quantitative reliability analysis;
3) Analysis of results and checking the reliability of systems for compliance with the requirements.

This paper is devoted to the second stage of the analysis - safety related systems reliability assessment.

Quantitative Reliability Analysis

Estimation models to be used in the Methodology are based on logic-probabilistic methods that present the structural model of system reliability in the form of boolean algebra to estimate the reliability factors as well as on Markovian chains estimation methods.

Below the description of logic-probabilistic method based on minimal cut sets is given.

The event-system failure Y in the reliability model is a sum of events corresponding to failures of minimal cut sets (MCS) of the system S_i:

$$Y = \sum_{i=1}^{n_s} S_i \qquad (1)$$

where n_s is a number of MCS.

The event: failure of i-th minimal cut set S_i is represented as

$$S_i = \prod_{k=1}^{n_i} X_{ik} \qquad (2)$$

where n_i is a number of basic events X_{ik} in i-th MCS.

The method of minimal cut sets permits to relate the algebraical form of writing the failure conditions to the probabilistic one; in case when $P(X_1)$, $P(S_i)$, $P(Y)$ are low, an expression giving a conservative estimate is derived for $P(Y)$:

$$P(Y) = \sum_{i=1}^{n_s} P(S_i) \qquad (3)$$

Otherwise more accurate equations with greater number of terms for sum of events are used.

The reliability factors of Q, $Q(t_{mt})$, $\bar{\omega}$ are derived as:

$$Q_d = \frac{1}{T}\int_0^T P(Y_t)dt \tag{4}$$

$$Q(t_f) = \frac{1}{T}\int_0^T P(Y_t)dt + \frac{1}{T}\int_0^T \int_t^{t+t_f} P(\bar{Y}_t dY_\tau)dt \tag{5}$$

$$\bar{\omega} = \frac{1}{T}\int_0^T P(dY_t)dt \tag{6}$$

where $P(Y_t)$ - is the probability that the oblect being considered becomes inoperative at instant of time (t); $P(dY_t)$ - is the probability that the given object transfers to the inoperative state on the time interval [t, t+dt] at $dt \to 0$; $P(Y_\tau)$ - is the probability that the object becomes inoperative at instant of time (τ) during its functioning in accident; $P(dY_\tau)$ - is the probability that the object failes on the time interval [t, t+dτ] at $d\tau \to 0$; t_{mt} - is the duration of a period of system functioning during the accident (mission time); T - is the duration of a period between the planned-preventive repairs (PPR) of the system when it is completely restored; $t \in [0,t]$ - is a current moment of time under normal operating conditions; $t \in [t,t+t_{mt}]$ - is a current moment of time on the interval of system functioning during the accident.

The probabilities of $P(Y_t)$, $P(dY_t)$, $P(Y_\tau)$, $P(dY_\tau)$ are expressed in terms of the following factors for minimal cut sets and components of $P(X_t)$, $P(dX_t)$, $P(X_\tau)$, $P(dX_\tau)$.

Specific Features of Reliability Factors Estimation for Safety Systems

The following data are given as an basic information:

1) General system data;

2) Data that are necessary for calculation of basic event probabilities.

The first data group includes: the duration of a period between the planned-preventive repairs (PPR) of the system, mission time,number of independent subsystems (channels) N, type of inspection strategy of the system standby equipment, available time of withdrawing one of the channels for repair in reactor power operation.

The description of the inspection strategies are presented in Table 1.

TABLE 1. SAFETY SYSTEM INSPECTION AND MAINTENANCE STRATEGIES

STRATEGY R = 0	Components of a minimal cut set (MCS) are tested (and mantained if required) in a queue according to their numbers
STRATEGY R = 1	For the same MCS as above the following procedure realizes: a) tests of the first component of MCS and then of the second one are performed. If those are available, the third component can be inspected. b) if any two components of MCS are unavailable, reactor must be shut down; if one component is failed it should be maintained.
STRATEGY R = 2	Tests of MCS components, belonging to different channels, are shifted in time by interval $dT = T/N_k$ (where T_k - inspection period, N - number of channels). If component failure is revealed, it should be maintained.
STRATEGY R = 3 (combination of R = 1 and R = 2)	Tests are shifted as for strategy R = 2. If component failure is revealed during inspection, unscheduled inspection of the rest components must be performed. If If there are no failed components among them, the first one must be maintained. Otherwise, reactor shuts down.

The second data group icludes:

1) types of component failures (n, p, pn, k, kn);
2) failure rates in standby mode a_j;
3) failure rates in the operating mode λ_j (for calculation of $Q(t_f)$ only);
4) repair rates of component μ_j;

5) component inspection periods in standby mode t_{kj} and the inspection duration θ_j;
6) the probability of undetecting the event-failure by the plant personnel during inspection or unappropriate repair;
7) the probability of occurence of event-failure of the component on demand due to start-up conditions q.

The identificator of component failure types (n, p, pn, k, kn) defines the way of failure detection and its repairability during stanby mode, where:

n - unmonitoring and nonrepairable components;
p and pn - periodically tested repairable and nonrepairable components respectively;
k and kn - monitoring repairable and nonrepairable components respactively.

The system failure may occur due to any of the causes, accounted by the mathematical model.

1) failure of the component of n, p, pn, k, kn type in standby mode;
2) failure of the component in operating mode;
3) unavailability of the during inspection (if it is not possible to perform the function in this state);
4) unavailability of the component during it's repairing;
5) failure of the component due to plant personnel error during inspection;
6) failure of the component on demand due to start-up conditions;

The reliability factors of the basic events derived in accordance with Table 2 and by formulae (10)-(12) are used to determine the reliability factors of safety systems Q, $Q(t_{mt})$, $\bar{\omega}$ by minimal cut sets method.

Table 2 presents the formulae for the probabilities of basic events. In the Table:

$$\Delta j(t) = (t-\varphi_j) - E\left\{\frac{t-\varphi_j}{t_{kj}}\right\} t_{kj} \qquad (7)$$

where E(X) - is the integer part of X;
φ_j - shift in time by moment of the beginning the j-th component checking from the moment assigned for the given group of components (with similar inspection period).

TABLE 2. CLASSIFICATION OF COMPONENTS BY TYPE OF INSPECTION AND FORMULAE FOR UNAVAILABILITY CALCULATION

Monitoring 'K'		Periodic 'P'				Uncontrolled 'N'
Repairable	Non-repairable	Repairable		Nonrepairable		
$\mu > 0$	$\mu = 0$	Test doesn't lead to unavailability	Test leads to unavailability	Test doesn't lead to unavailability	Test leads to unavailability	Unrepaired
$\frac{\alpha_i}{\mu_i}$	$\alpha_i t_{av}$	$q_{ot}+q_{ni}+\alpha\Delta_j(t)+\alpha_j t_{kj}^* e^{-\Delta_j(t)\mu_j} * d_j(t)$ $d_j=\begin{cases}1 \text{ at } \Delta_j(t)<t_{av} \\ 0 \text{ at } \Delta_j(t)\geq t_{av}\end{cases}$	$q_{ot}+q_{nj}+\alpha_j\Delta_j(t)[1-C_j(t)]+\alpha_j t_{kj}^* d_j(t)+C_j(t)$ $C_j=\begin{cases}0 \text{ at } \Delta_j(t)<t_{kj}-\theta_j \\ 1 \text{ at } t_{kj}-\theta_j \leq \Delta_j(t) \leq t_{kj}\end{cases}$	$q_{ot}+q_{nj}+\alpha\Delta_j(t)+\alpha_j t_{kj} d_j(t)$	$[q_{ohj}+q_{nj}+\alpha_j t_{kj}^* d_j(t)][1-C_j(t)]+C_j(t)$	$q_{ohj}+\alpha_j t$

SHARM-2 COMPUTER PACKAGE

The above-mentioned methodical principles for estimation of the NPP probabilistic safety systems based on the fault-tree method, were implemented in SHARM-2 code package as an development of the previous program version /1/.

The spesific features of the SHARM-2 code package are as follows:

- the original code for fault-tree (FT) permits to present the fault-tree in the form of matrix composing of four lines with the use of simple formal procedure. The software is used for further development of minimal cut sets, which are presented in the form of bit arrays being the most compact and convenient form of performing the estimates;
- using the majorify operators of "m" from "n" in the fault-tree side by side with usual logical operators of "AND", "OR" as well as modular (fragmental) fault-tree analysis (consisting in selecting the modules interpreted as "conditional components");

- provision of programs blocks for calculation of safety system reliability factors at various inspection strategies (r = 0, 1, 2, 3). In so doing, the method and algorithm for calculation the reliability factors of minimum cut sets are developed for each of the strategies (such developments are absent in the Methodology at present);
- implementation of Monte-Carlo (fiducial) /2/ procedure for interval estimation of safety system reliability factors (upper γ-confidence boundary of failure probability or unavailability factor);
- implementation of Bayesian procedure for joining the appriorian information and real statistics data for system components.

The SHARM-2 code package is structurally composed of two programs:

FIBR - for calculation of reliability factors for normal operating systems and

RASS - for calculation those of safety systems. Fault-tree analysis and randomization blocks and some other ones are common for two programs.

The point estimation block of FIBR program is based on traditional approach to system reliability factors calculations. The RASS program used the original methodical solutions described in Chapter 2.

The computer package is written in PL/1 algorithmic language for ES Series computers.

Evaluating the system unavailability based on minimal cut sets

The evaluating algorithm is based on the list of minimal cut sets, type of inspection strategy and specific conditions of element functioning. The probability of failure to demand $Q(t,\tau)$ is evaluated according to the following algorithm. It's proposed that switch on signal occurs in time moment t, and then system must function during the time τ.

$$Q_{al}(t,\tau) = Q_{\text{§}\,1}(t) + Q_{\text{£}\,1}(t\tau) = Q_{\text{§}\,1}(t) + \int_0^{\tau} W_1(t\tau)d\tau, \qquad (10)$$

where $W_1(t,\tau)$ - failure rate of 1-th MCS (calculated according to the inspection strategy and the conditions of functioning):

$$W_1(t,\tau) = \sum_{k\in æ_1} \omega_k(t,\tau) \prod_{\substack{j\in æ \\ j\neq k}} Q_j(t,\tau) \qquad (11)$$

$\omega_k(t,\tau)$ is as follows:

$$\omega_k(t,\tau) = \lambda_k[1 - q_k(t,\tau)] = \lambda_k P(q_k(t),\tau). \qquad (12)$$

The analytical formulae for parameters $Q_{æl}(t)$ and $Q_{æl}(t,\tau)$ is derived according to the inspection strategies representing in the table 2. The mean value of Q on the standby time interval t_γ is derived by these formulae.

For example, the formulae for the ispection strategy 1 are represented follows:

$$Q^{S}_{æl}(t_\gamma)=\sum_{i\in æ_l} q_{ci}(t_\gamma)\prod_{\substack{j\in æ_l\\ j\neq i}} q_{fi}(t_\gamma)+\sum_{i\in æ_l} q_{ri}(t_\gamma)\prod_{\substack{j\in æ_l\\ j\neq i}}[1-q_{fj}(t_{oj})]q_{fj}(t_\gamma)+$$

$$+\prod_{i\in æ_l} q_{fi}(t_\gamma) \qquad (13)$$

$$W_{æl}(t_\gamma,\tau) = \sum_{k\in æ_l} \lambda_k P_k(q_{ok}(t_\gamma),\tau) \prod_{\substack{j\in æ_l\\ j\neq k}} Q_j(q_{fj}(t_\gamma),\tau) +$$

$$+\sum_{k\in æ_l} \lambda_k P_k(q_{rk}(t_\gamma),\tau)\prod_{\substack{j\in æ_l\\ j\neq k}} Q_j\{[(1-\alpha_{fj}t_{oj})q_{fj}(t),\tau\}+ \qquad (14)$$

$$+ \sum_{k\in æ_l} \lambda_k P_k(q_{fk}(t_\gamma),\tau) \prod_{\substack{j\in æ_l\\ j\neq k}} Q_j(q_{fk}(t_\gamma),\tau),$$

where $$P_k(q_{ind_k}(t_\gamma),\tau) = \frac{\mu_k}{\mu_k+\lambda_k} + \left[\frac{\lambda_k}{\lambda_k+\mu_k} - q_{ind_k}(t)\right]e^{-(\lambda_k+\mu_k)\tau} \qquad (15)$$

index ind can be o, r or f.

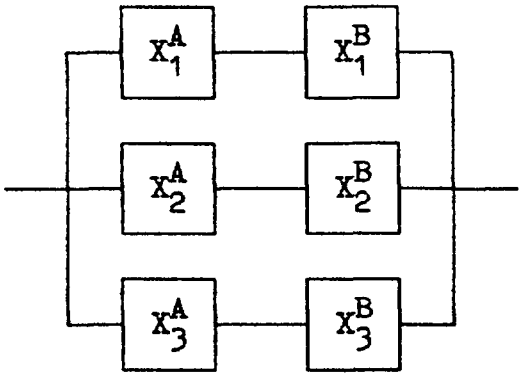
$$Q_j(q_{ind_k}(t_\gamma),\tau) = \frac{\lambda_j}{\lambda_j+\mu_j} + \left[q_{ind_j}(t_\gamma) - \frac{\lambda_j}{\lambda_j+\mu_j}\right]e^{-(\lambda_j+\mu_j)\tau}, \qquad (16)$$

The first item in the formulae for $Q^{S}_{æl}$ W_1 represents the probability of the fact that the elements of MCS failed or they are tested being off line (taking into account that only one element can be tested at given time) during time interval t_γ, or they failed in functioning mode in time moment τ. The second item represents the probability of the fact that the only one element of MCS is repaired in that time moment (taking to account that the another elements would be available during the test), and another failed during standby or functioning mode. The third item represents the all elements' failure probability.

Program Package Validation

Below the results obtained by the program packages SHARM-2 and PSAPACK for few tests are represented.

The reliability diagram of given system is represented in the Fig.1. X_j^A corresponds the failures in standby mode, and X_j^B corresponds the failures in functioning mode.



Fig&1 Reliability diagram of given system

The data needed for the testing involve two data group: static data and variable data, values of which can be modified.

The static data include:

- number of channels N=3;
- preventing repair interval $T=8x10^3$ hours;
- test interval t_k=720 hours;
- test duration θ_k=3 hours;
- functioning interval t_f=360 hours;
- available time for repair t_a=120 hours.

the variable data include:

- event type X_j^A - n, p, k;
- failure rate in standby mode α_j;
- failure rate in functioning mode λ_j;
- inspection strategy type (can be 2 or 3);
- repair rate in functioning mode μ_j.

The results of program package validation are represented in the Table 3. These results show an effect achieving by more accurate methods usage.

TABLE 3. SHARM-2 CODE PACKAGE VALIDATION

Test #	Dynamic data			Unavailability, calculated by	
				SHARM-2	PSAPACK
1	Event type	1 2 3	p k n		2.0E-07
	Failure rate in standby mode	1 2 3	2E-05 1E-05 5E-07		
	Failure rate in functioning mode	1 2 3	0 0 0		
	Repair rate in functioning mode	1 2 3	0 0 0		
	Number of inspection strategy		2	5.9E-08	
2			3	2.6E-08	
3	Event type	1 2 3	P P P		1.8E-07
	Failure rate in standby mode	1 2 3	0 2E-05 2E-05		
	Failure rate in functioning mode	1 2 3	4E-05 0 0		
	Repair rate in functioning mode	1 2 3	5E-02 7E-02 1E-01		
	Number of inspection strategy		2	5.5E-08	
4			3	3.5E-08	

CONCLUSION

The methodology and SHARM-2 code package are the significant components of the NPP probabilistic safety analysis of 0 level.

They are based on contemporary soviet and foreign concepts for reliability system analysis that takes into account the specific features of NPP system functioning. It permits to get out of the excessive conservatism in calculations and to obtain the more accurate reliability estimates.

The RBMK-1000 NPP safety system reliability have calculated by SHARM-2 Code Package. The results were used in RBMK probabilistic safety analysis of 0 level.

REFERENCES

I. Клемин А.И., Шиверский Е.А. Разработка комплекса программ расчета структурной надежности АЭС и ее систем с помощью метода деревьев отказов. "Методические вопросы исследования надежности больших систем энергетики", Иркутск, 1981. Вып.22.

2. Клемин А.И.,Морозов В.Б., Шиверский Е.А. Использование априорной и фактической информации для интервальной оценки надежности контуров теплоносителя АЭС. "Надежность и контроль качества" № 2, 1988 г.

3. Швыряев Ю.В., Морозов В.Б. и др. Руководство по выполнению вероятностных анализов безопасности АС при проектировании. Доклад на семинаре НТЦ ГАЭН по безопасности атомной энергетики, май 1989 г., Москва.

DEVELOPMENT OF TECHNICAL SPECIFICATION SURVEILLANCE REQUIREMENTS FOR SIZEWELL "B" POWER STATION

W.B. SARGEANT
Nuclear Electric plc,
Knutsford, Cheshire,
United Kingdom

Abstract

The paper describes the adaptation of Standard Technical Specifications to the licensing requirements of the United Kingdom for the first PWR to be built by Nuclear Electric plc (formerly a part of Central Electricity Generating Board). The application of probabilistic methods in the design and safety analysis is described, and the decisions to be taken on the scope, structure and interdependence of the technical specifications for Sizewell "B" Power Station are assessed.

Introduction

Sizewell "B" NPS is currently under construction for Nuclear Electric plc, the nuclear electrical generating utility of England and Wales which was formerly part of the Central Electricity Generating Board. It is the first pressurised water reactor to be ordered by the utility, and the need to integrate it into a system of licensing and operating, previously only applied to gas cooled reactors, has posed a number of problems. Some of those concerned with the application of Technical Specifications are illustrated.

In selecting the PWR design for its future programme of nuclear reactors, the very significant benefit of adopting an established, widely used technology was well recognised. It follows that these benefits will be enhanced during the operation of the station if it can be operated in a manner consistent with the majority of international practices. In particular our use of the established experience feedback networks has illustrated the potential benefit of using the Technical Specification structure as the basis of documentation to meet the equivalent UK Operating licence conditions.

Sizewell "B" is a largely replicate design based on the SNUPPS plant, of which Callaway and Wolf Creek are also examples, but the development of Sizewell "B" Technical Specifications from the standard Westinghouse version (NUREG 0452) has to take the following aspects into account:

- the effect of imposing the US system on the UK regulatory structure
- the fundamental differences between the US and UK safety cases
- international developments such as the Tech Spec Improvement Programme.

Operating Licence Conditions

The Nuclear site licence issued by the Nuclear Installations Inspectorate on behalf of the Health and Safety Executive specifies the conditions required for operation of the nuclear facility.

In particular the licensee is required to produce an adequate safety case and to identify the conditions and limits necessary in the interests of safety. Such conditions and limits are known as **Operating Rules** and all operations must be carried out in compliance with such Operating Rules.

An additional condition requires that all operations which may affect safety are carried out in accordance with written **Operating Instructions** to ensure that any Operating Rules are implemented.

The licensee is also required by the conditions of the licence to make and implement adequate arrangements for the regular and systematic **examination, inspection, maintenance** and **testing** of all plant which may affect safety.

Nuclear Electric implements the requirements of these conditions on the gas-cooled reactors by provision of a suite of documents comprising

Operating Rules

Identified Operating Instructions

Maintenance Schedule

The first two in combination encompass the functions and plant systems covered in Sections 2 & 3 of the Technical Specifications, and the third covers the surveillance aspects of Section 4.

Design Safety Guidelines and Criteria

Nuclear Electric specifies the safety criteria against which nuclear power stations should be designed so that they can be constructed and operated on sites near urban areas. The criteria are design targets and not operational limits. The application of the criteria requires the use of numerical probability analysis in safety assessments where appropriate, to ensure that a systematic approach is followed and that a balanced design is achieved in terms of safety performance.

The safety criteria take into account the Safety Assessment Principles of the Nuclear Installations Inspectorate, the UK regulatory organisation, which are applied during the safety assessments of application for a licence to construct and to operate a nuclear power station. The fundamental criteria are based on the radiation doses to the public and to the station staff in normal operation and on the predicted frequency of doses to the public and station staff resulting from accidental releases and exposures. Additionally, engineering criteria specify system reliabilities, in particular for the protection systems, and the approach to be adopted in fault and hazard assessment.

For the PWR project these design safety criteria have been amplified into Design Safety Guidelines. The topics covered are shown in Table 1. Of particular relevance to the application of Technical Specifications to the operation of Sizewell is the need to conform to both reliability targets for

essential systems and to radiological limits for accidental release of radioactivity. Particular guidance is given to the treatment of maintenance and testing in the reliability analyses.

TABLE 1. DESIGN SAFETY GUIDELINE TOPICS

Standards and Quality Assurance
In-Service Inspection, Testing and Monitoring
External Hazards
The Prevention of and Protection against Internal Hazards
Trip, Shutdown and Essential Systems
Reactor Safety System
Specification for Reactor Safety System
Reactor Shutdown Requirements
Reliability Guidelines for Post Trip Cooling and other Essential Systems
Safety Related Electrical Equipment
Emergency Control
Containment
Access to Containment
Design Targets for Doses and Dose Rates
Control of Contamination in Accessible Areas
Radioactive Waste Management
Criticality Safety Requirements and Recommendations for the Design of the Fuel Route
Radiological limits for Accidental Release of Radioactivity to the Atmosphere
Control Instrumentation and Alarm Systems

Reliability Targets

The reliability targets are set in relation to acceptable societal risk of death or accident. The design targets are framed as:

1 The predicted accident frequency for doses of 1 ERL (e.g. 10 rem whole body dose) should not exceed 10^{-4} per reactor year. Accidents resulting in lower doses are acceptable at higher frequencies.

2 For any single accident which could give rise to a large uncontrolled release of radioactivity to the environment resulting from some or all of the protective systems and barriers being breached or failed, then the overall design should ensure that the accident frequency is less than 10^{-7} per reactor year. This is to be interpreted as meaning that the product of initiating fault frequency and the probability to control the accident should be less than 10^{-7} per reactor year.

3 The total frequency of all accidents leading to uncontrolled releases, as in 2 above, should be less than 10^{-6} per reactor year.

In general the target for all accidents is the most severe and can be expressed as:

Total probability of an uncontrolled release $< 10^{-6}$ per annum.

To assess compliance with this target one has to work from an initiating fault schedule and assess the fault sequences which result from the predicted effectiveness of protection, shutdown and cooling. By summing all such sequences for all initiating events one can arrive at an overall probability of an uncontrolled release.

From these probabilistic targets, individual system reliability requirements have been derived.

Maintenance and Testing

Specific guidance is given in Nuclear Electric Design Safety Guidelines on the treatment of maintenance and testing in reliability analyses.

> Ideally the reliability requirements should be met at all times even when plant is out on maintenance, planned or unplanned, or is undergoing testing. However, since the basic criterion quoted above is probabilistic then maintenance and testing can also be treated in a probabilistic manner when demonstrating that the basic criterion is met. Nevertheless, when plant is out on maintenance or is undergoing testing it is desirable that the actual system unreliability at that particular point in time is sensibly limited. It would be undesirable for the cooling system unreliability at any point in time to be worsened by more than one decade when the permitted unreliability lies between 10^{-4} and 10^{-5}, or by two decades when the permitted unreliability is 10^{-6} or less. For cases where the permitted unreliability lies between 10^{-3} and 10^{-4} the point unreliability should never be increased above 10^{-3}.

The Sizewell "B" safety case has developed towards assessing overall station risk, rather than addressing system reliabilities specifically, and at present consideration is being given to a strategy for addressing both point in time station risk and system reliability targets.

Options and Operator Support

In assessing the strategy to be adopted for licensing and operating Sizewell "B" the treatment of maintenance and testing of the plant systems cannot be considered without also considering the need for operator support. To keep

the statement of the permissible plant outages simple and unambiguous it is preferable to restrict the limitations to individual systems. If the point risk is to routinely assessed, a station based interactive computing facility with a model of the safety case and plant status is required.

An alternative proposal being considered is to run the probabilistic safety assessment for combinations of plant availabilities, and the sensitivity of the safety case to specific system reliabilities. This has the advantage of identifying which systems have the greatest significance to safety and will contribute to the decisions on which systems and functions should be included in the Technical Specifications.

Such an assessment would generate a matrix of acceptable plant outage combinations, which could be either held in tabular form within the Technical Specifications volume, or would be straightforward to include in a computerised system for Technical Specification management.

Conclusions

The need to adopt a system which ensures that station operation complies with the assumptions of the safety case and which has the advantages of consistency with other PWR operators, has resulted in the assessment of alternative strategies operated within Nuclear Electric and by other Utilities as discussed above.

CONTROL OF POWER DEPENDENT SAFETY MARGINS

R. HÄUSERMANN
Kernkraftwerk Leibstadt AG,
Leibstadt, Switzerland

Abstract

The Leibstadt Plant KKL, situated on the river Rhein in Switzerland, is a BWR-6, Mark III, GE-Plant with a BBC turbogenerator set with a net electrical output of 990 MW. In December 1973, the work contract was signed and in December 1984 KKL started the commercial operation.

The construction period was influenced by the TMI-incident in 1979. The incident prompted a very tedious design review by the authorities, vendor, and KKL. The PRA-studies were part of the design review.

---

1. Introduction

The experience with first generation nuclear power plants in Switzerland (Beznau I and II in 1969 and 1971, Mühleberg 1972) with regard to the plant Technical Specification TS was valuable for us.

The plant system design for KKL differs significantly from the first generation Swiss nuclear power stations. The groundrule, a symptom oriented technical specification, is common to all Swiss plants. The KKL technical specification (TSL) was checked and approved by the Swiss Nuclear Authority, HSK.

In 1980 work was started on a level 1 PRA, with the objective to find the significant weak spots which potentially contribute to the possibility of core melt. Another goal was to find also event sequences resulting in severe accidents beyond design. The ATWS (Anticipated Transient Without SCRAM) was the most critical event. KKL decided thereafter to backfit the reactor protection SCRAM system with an ARI (Alternate Rod Insertion) system. The results are shown in Table 1.

In 1987 the level 2 PRA study was started. The results formed a basis to define actions for some plant modifications and to get some reference cases to be considered in the emergency procedures. The latter ones include the accident management procedures which shall be used to mitigate the consequences of an accident. The study resulted in the definition of the source terms in the containment. It was decided to install an ignitor system to burn the hydrogen in the containment in a safe manner.

The hydrogen is produced as a result of the Zr-Water reaction when the core is uncovered. The COSA (COntainment SAfeguard) system which permitted to depressurise the containment for some accident sequences, is now under rewiew. Particularly the depressurisation- and filter-capacity.

TABLE 1

LEIBSTADT CORE DAMAGE FREQUENCY RELATED TO FUNCTION FAILURES FOR ORIGINAL RPS ANALYSIS

Function Failure	Core Damage Frequency For Each Initiator Group		Total Core Damage Frequency	Fraction of Total Core Damage Frequency
	LOCA	Transient		
Reactor Subcriticality	7.25E-8	4.03E-6	4.10E-6	69.5%
Emergency Coolant Injection	2.63E-8	1.60E-6	1.63E-6	27.6%
Decay Heat Removal	4.62E-8	1.26E-7	1.72E-7	2.9%
Subtotals	1.45E-7	5.76E-6	5.90E-6	

LEIBSTADT CORE DAMAGE FREQUENCY RELATED TO FUNCTION FAILURES FOR REVISED RPS ANALYSIS INCORPORATING ARI

Function Failure	Core Damage Frequency For Each Initiator Group		Total Core Damage Frequency	Fraction of Total Core Damage Frequency
	LOCA	Transient		
Reactor Subcriticality	4.35E-8	1.60E-6	1.64E-6	47.6%
Emergency Coolant Injection	2.63E-8	1.60E-6	1.63E-6	47.4%
Decay Heat Removal	4.62E-8	1.26E-7	1.72E-7	5.0%
Subtotals	1.16E-7	3.33E-6	3.44E-6	

In 1988 a PRA study for the SEHR (Special Emergency Heat Removal system) was performed. The system is fully bunkered and operates automatically. Once initialised no access is possible for a given time.
No interactions from the main control room are possible. Maintenance or intervention locally is also not possible. Therefore the PRA analysis for that system was done in such detail to include the reliability of critical electrical components.

In parallel to the studies based on PRA methods, KKL continued to develope deterministic methods to detect systematically deficiences well ahead of time when serious consequences could be expected; thus reducing the probability that an event could progress to a core melt situation with high radioactive release. The inspection, periodic testing and the on-condition based maintenance-strategies are part of the deterministic approach. In one instance - based on a PRA-study - the maintenance strategy was considerably improved. The interconnection to the TSL, being part of the plant management, is outlined in Figure 1. The results of the PSA-studies were included into the appropriate procedures. The TSL acts as a safety filter and determines the permissable plant status and outage time in case of unavailable systems or components.

2. Strategy to control safety margins

Dependent on status (number of redundancies) of the nuclear safety systems with regard to Figure 2, the plant must be brought into the proper power range in accordance with the TSL. Power range and outage time allowance, to make an intervention, are fixed in the TSL. The action to control the margins is administratively initiated. Each reduction of the safty margin result in a LCO (Limited Condition of Operation). A LCO describes the status of the deviation and the measures which have to be taken- the so called "Surveillance requirements"- for the duration of the LCO.

In Figure 6 a schematic overview is given, how it is controlled that the safety margins do not fall below the minimum required number of safty systems.

Goals have been set at the plant for the maximum allowable planned and unplanned LCO and are controlled in accordance with the TSL. In most of the cases sufficient time was available to fix the deficiency such that a power reduction could be avoided.

For comparison a similar graph for the power production systems, see Figure 3, is shown. The plant will make an automatic power reduction if system nonavailabilities occur. The degree of power reduction depends on the plant design. The controlling factor is the amount of redundant installations and the protection strategy for the components. The power reduction may go so far that a challenge to the nuclear safety systems results; thus terminating the power transient. Restart of the plant will commence after finding and eliminating the root cause. This action is also controlled by the TSL.

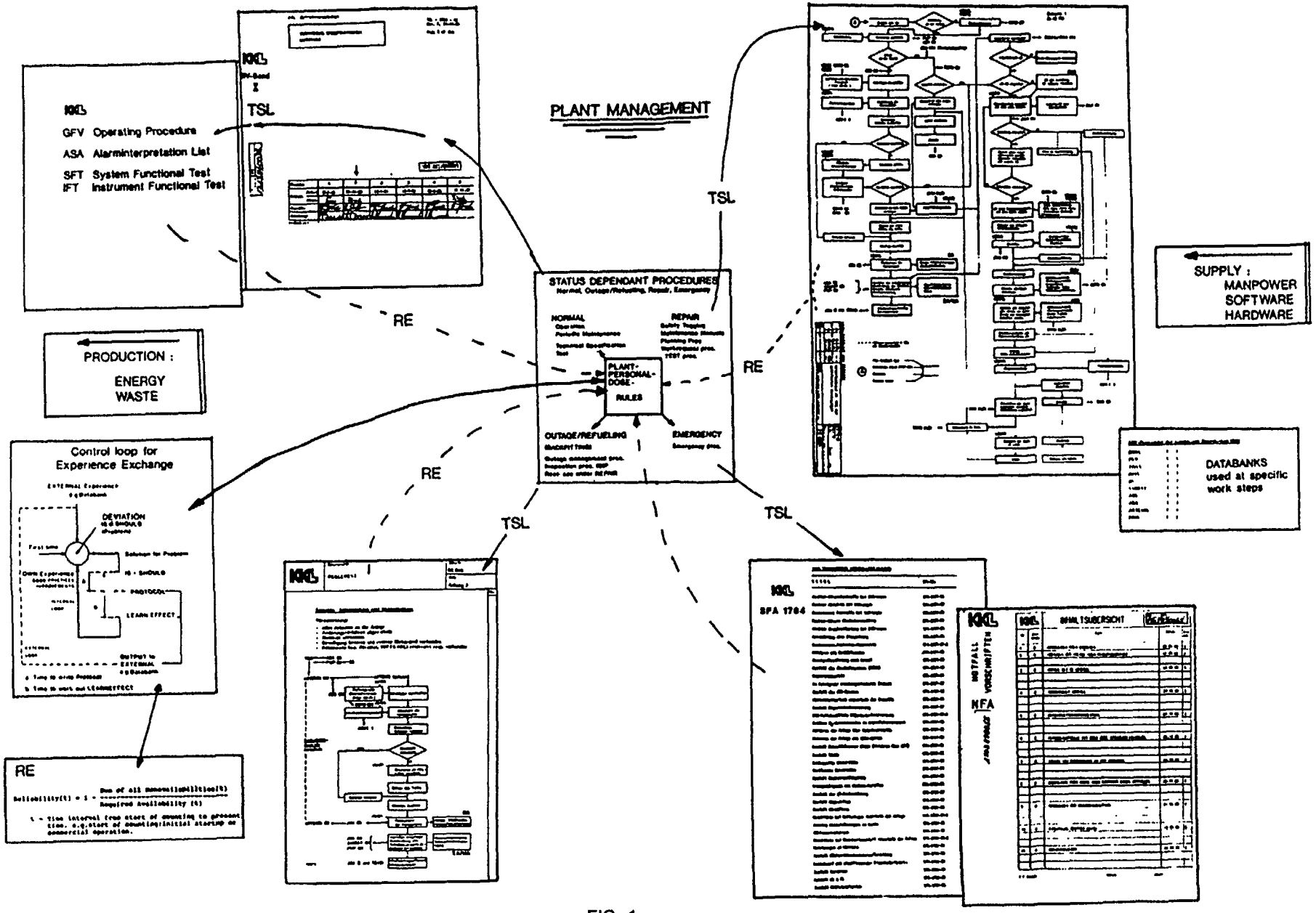

GFV Operating Procedure
ASA Alarminterpretation List
SFT System Functional Test
IFT Instrument Functional Test
TSL
RE
PLANT MANAGEMENT
STATUS DEPENDANT PROCEDURES
NORMAL
REPAIR
PLANT-PERSONAL-DOSE-RULES
OUTAGE/REFUELING
EMERGENCY
PRODUCTION :
ENERGY
WASTE
SUPPLY :
MANPOWER
SOFTWARE
HARDWARE
DATABANKS
used at specific
work steps
Control loop for
Experience Exchange
DEVIATION
LEARN EFFECT
RE

FIG. 1.

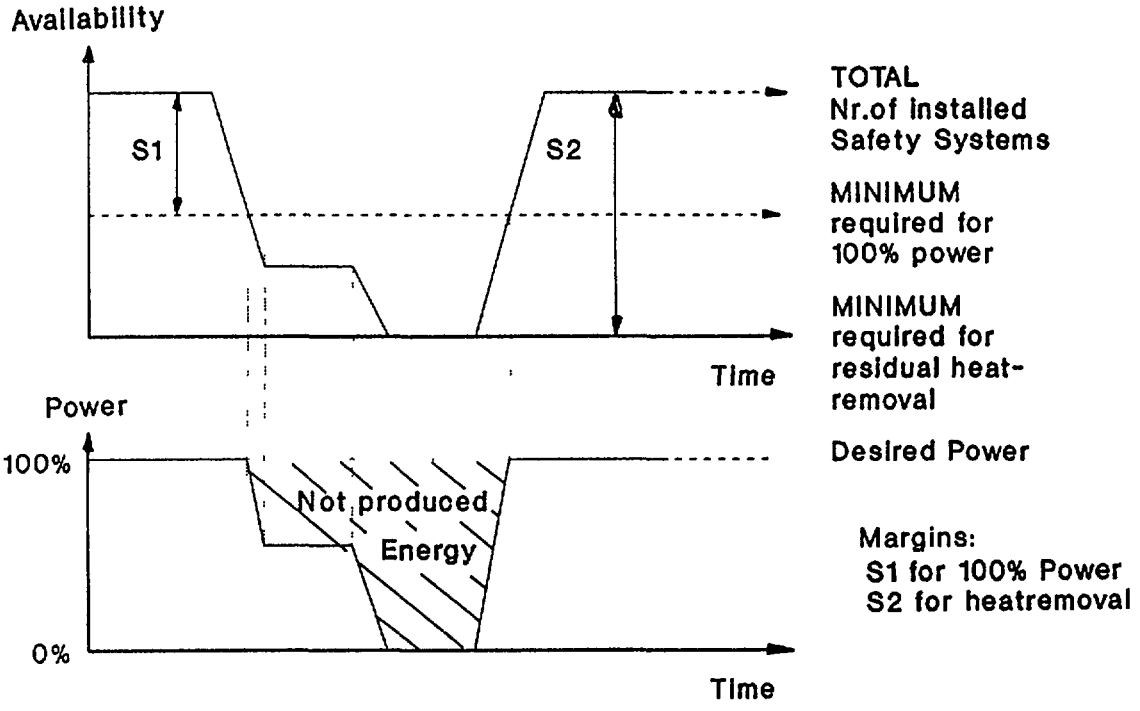


FIG. 2. Safety systems relevant for residual heat removal.

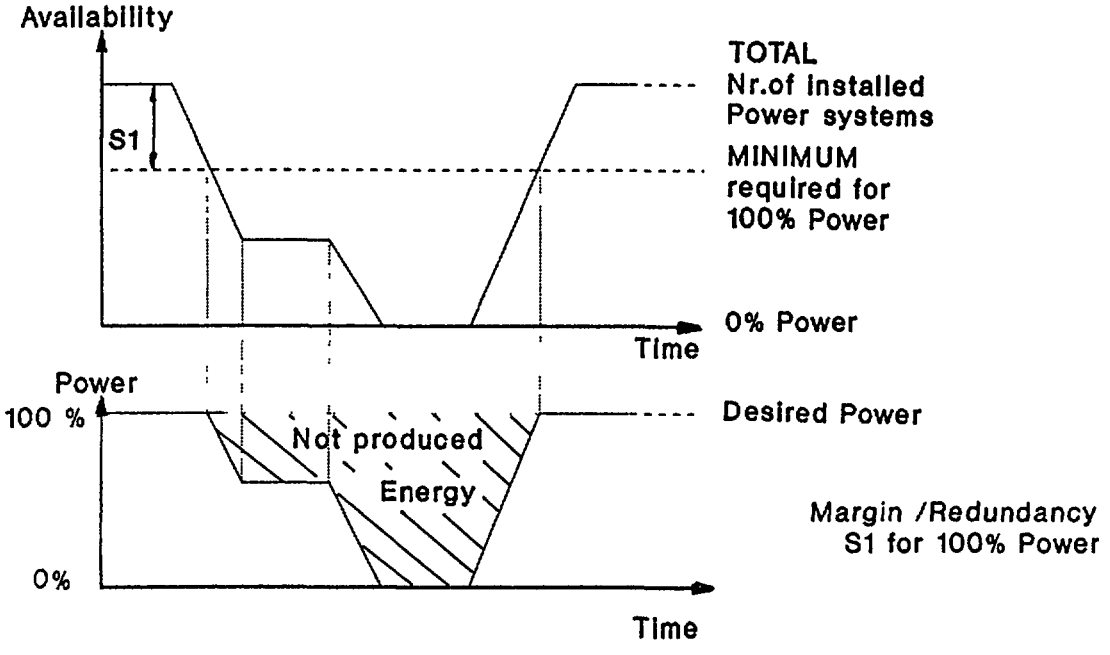


FIG. 3. Power systems relevant for power production.

3. Methods to keep in line with strategy

The crew at the plant is well qualified to perform their functions in operation and maintenance.

The management structure is such that the legislative intent is correctly transfered to the personnel which executes the work at the plant.

The personnel is instructed to report any perceived deviation from the normal plant status. Root cause analysis starts in some cases prior to reaching any alarm setpoints, pointing to possible degraded components. A prerequisite is: Good trend recording, immediate analysis and technical interpretation and actions taken to avoid an unwanted automatic unavailability.

Work at the plant is then performed after verification that the working crew can do it in a safe and qualitative manner.

Perform maintenance in accordance with:

- predictive maintenance practices
- based on condition of plant components (fatigue, corrosion, erosion etc)
- take also small visible and nonvisible internal leaks in the system very seriously
- periodic maintenance practices thus minimising unplanned repairs and other interventions.

4. Quality improvement, learning from experience

After the introduction of a quality improvement program and appropriate quality controls, a systematic continious learning process is necessary. The method of such a system was presented previously in Reference 1. The basis is to learn from own events (experience) and events from others in a feedback process (see Figure 4).

In this process is included the TSL. As was outlined above, for important decisions the PRA-methods are used where an intuitive solution can not be quantitively assessed. The EXTERNAL Experience (see Figure 4) may also be helpfull in such cases. That experience may also be assessed with PRA-methods, before it is applied at the plant.

In Figure 5 an extract of Reference 1 is shown. The curves show events weighted by the severness of nonavailability versus the number of such events. Out of the yearly shift of such a curve the overall change and /or improvement can be judged. Note that this curve is related to functional nonavailabilities. The non functional equippment was brought back in such a status as to warrant functional preparedness. The first phase of success-full operation up to the intervention time is assessed. The second phase is chosen smaller if the first intervention was an unplanned one; thus reducing the possibility of another unwanted unplanned second maintenance intervention. Another important fact can be deduced from Figure 5. The largest amount of work done deals with the so called "less important" events in term of

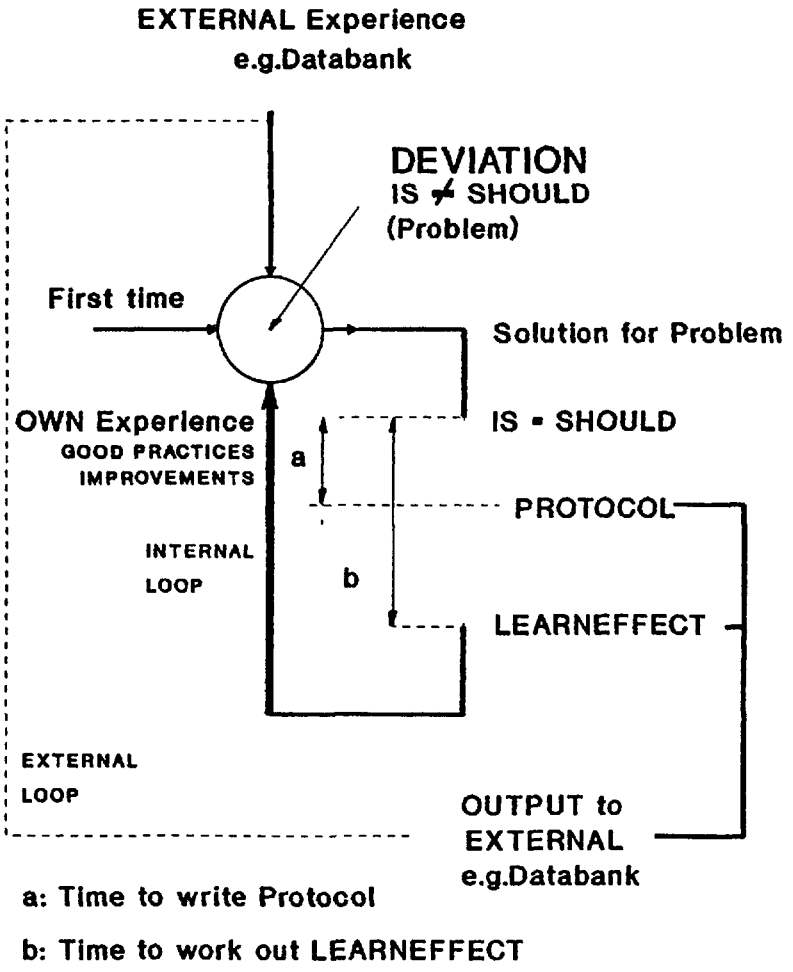


FIG. 4. Control loop for experience exchange.

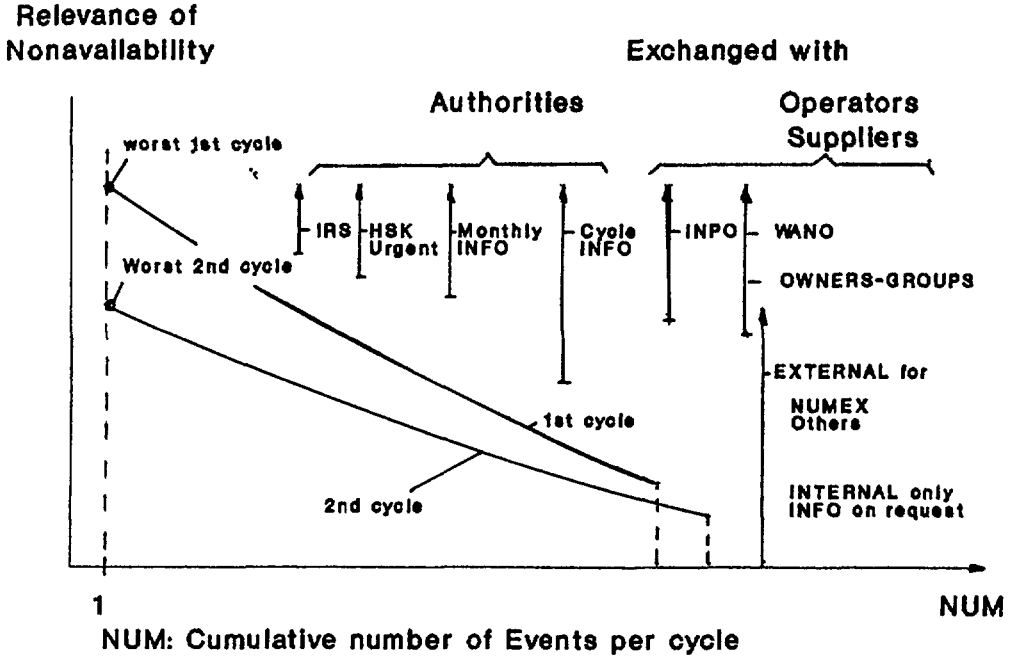


FIG. 5. Relevance of events measured by non-availability.

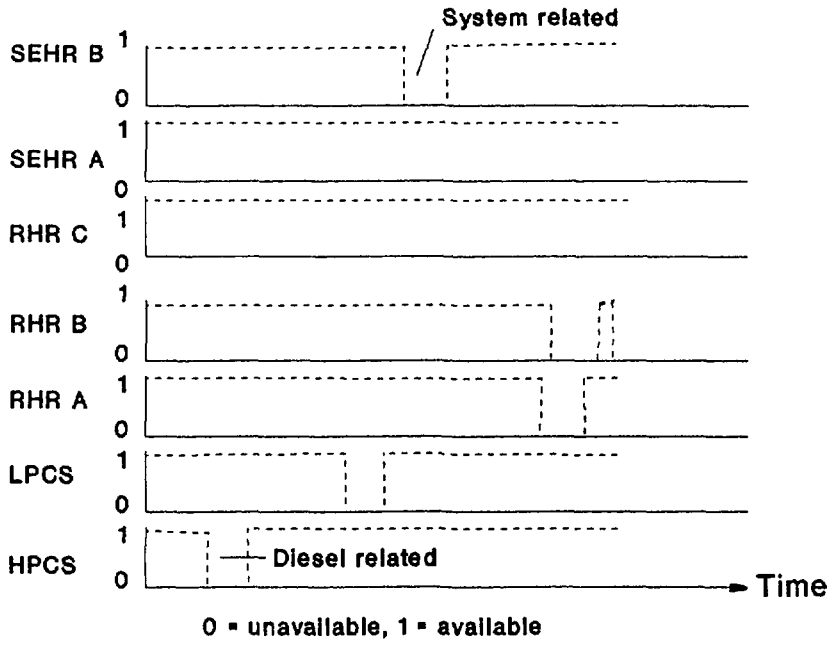


FIG. 6. LCO control — ECCS systems.

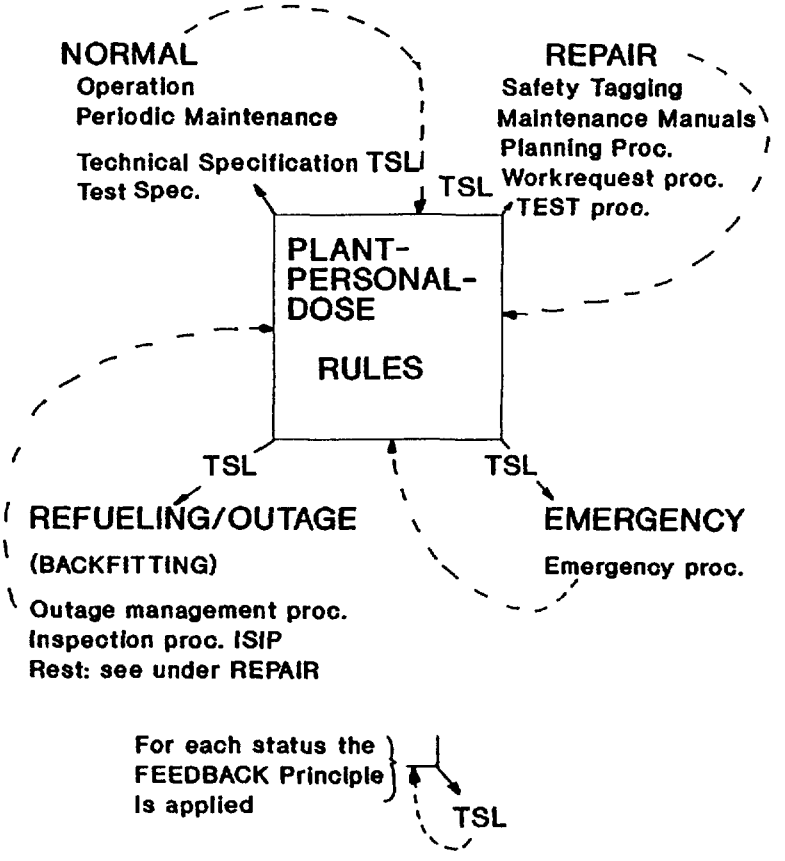


FIG. 7. Status dependent procedures: normal, refueling, repair, emergency.

relevance. However these activities determine to a large extent the absence of the real challenges to safety systems. Preventive maintenance means to prevent real safety system challenges thereby actively participating in lowering the probability to initiate a core melt.

Note: In the proper handling of the details is hidden the big chance to avoid the negative "spectacular" events. To operate a power station away from near misses, i.e. with large safety margins is the best warranty for safe and reliable operation. It is therfore logical to invest in a good tool to check the safety margins.

5. Conclusion

It can be concluded that an active and determined plant management combined with a continious learning effort and substituted by a perodic review of the plant experience with PRA-methods, is a good safety strategy. It is recommended to perform a periodic reevaluation of the original PRA- studies with actual plant specific performance data to spot the possible changes in weak points.(see Figures 1 and 7) .

6. Outlook

KKL has decided to improve the PRA tools and will introduce a LIVING-PRA model at the site. This will support the decision making process for operation and maintenance. Particularly in the area of periodic test frequency and the preventive maintenance. The influence of the human factor in emergency and maintenance situations will be simulated and assessed.

Reference

1.) "Computerunterstützter Erfahrungsaustausch und Ereignis-Datenbanken". Paper Nr. 3.9 presented by R. Häusermann, dipl. Ing. ETH, Kernkraftwerk Leibstadt AG. Titel of Conference: SVA Vertiefungskurs "Computereinsatz im Kernkraftwerk" SVA, Postfach 5032, CH-3001 Bern.

RISK-BASED EVALUATION OF TECHNICAL SPECIFICATIONS FOR A DECAY HEAT REMOVAL SYSTEM OF AN LMFBR PLANT

K. HIOKI, Y. KANI
Oarai Engineering Center,
Power Reactor and Nuclear Fuel Development Corporation,
Oarai, Ibaraki-ken,
Japan

Abstract

PNC has been performing Probabilistic Safety Assessment on the prototype fast breeder reactor Monju since 1982. The objective is to construct a probabilistic model for the Monju plant so that the overall safety assessment can be performed.

This paper presents a method of applying probabilistic technique to the development of the Technical Specifications for the Decay Heat Removal System (DHRS) of an Liquid Metal Fast Breeder Reactor (LMFBR) taking into consideration both the outage risk and shutdown risk.

The DHRS is usually redundant and stands by while the reactor is in power operation. Therefore partial failure of DHRS can be repaired without shutting down the reactor. However, the reliability of DHRS is lowered due to the repair outage. And the probability of occurrence of initiating events that require a plant shutdown and DHRS operation increases as the repair is continued.

On the other hand, if the reactor is shut down manually after detecting the failure, the operation of DHRS whose reliability is deteriorated is needed. From this point of view, a manual shut down can be considered as one of initiating events.

Most of the Technical Specifications have been developed based on deterministic methods or engineering judgments. However, for a new type of reactor such as LMFBR they should be determined based not only on the experiences of LWRs but on a new concept of risk because of the difference of plant design and characteristics.

The basic concept of the method is to minimize the total risk or to keep it less than a preset limit. The method can be used to help plant operator decide if the plant should be shut down or not and, if the operation should be continued, help him determine the allowable outage time (AOT) and the test interval of remaining intact loops.

We expect that this method will be combined with the 'living PSA' and construct an on-the-site system which calculates the plant risk level in the real time mode and gives the AOT and test intervals which are best for the plant safety.

---

1. INTRODUCTION

Power Reactor and Nuclear Fuel Development Corporation (PNC) has been performing Probabilistic Safety Assessment on the prototype fast breeder reactor Monju since 1982. The objective is to construct a probabilistic model for the Monju plant so that the overall safety assessment can be performed. As a part of this effort, operational procedures of the reactor are evaluated based on a risk concept.

This paper presents a method of applying probabilistic technique to the development of the Technical Specifications for the Decay Heat Removal System (DHRS) of a Liquid Metal Fast Breeder Reactor (LMFBR) taking into consideration both the outage risk and shutdown risk.

The DHRS is usually redundant and is on stand-by while the reactor is in power operation. Therefore partial failure of DHRS can be repaired without shutting down the reactor. However, the reliability of DHRS is lowered due to the repair outage. And the probability of occurrence of the initiating events that require a plant shutdown and operation of the DHRS with lowered reliability increases as the repair is continued.

On the other hand, if the reactor is shut down manually after detecting the failure, the operation of DHRS whose reliability is deteriorated is needed. From this point of view, a manual shutdown can be considered as one of initiating events and it is not always the best to shut down the plant.

Most of the Technical Specifications have been developed based on deterministic methods or engineering judgments. However, for a new type of reactor such as LMFBR they should be determined based not only on the experiences of LWRs but on a new concept of risk because of the difference of plant design and characteristics.

The basic concept of the method is to minimize the total risk or to keep it less than a preset limit. The method can be used to decide if the plant should be shut down or not. If the operation should be continued the method calculates the test interval of remaining intact loops and the outage time which satisfy the condition.

2. METHOD

2.1 LCO rules examination procedure

A flow chart of examining Limiting Conditions of Operation (LCO) when a part of redundant safety system is failed is shown in Figure 1.

First, the reference risk should be set. It can be either the risk under normal plant operation or the risk of manual plant shutdown with or without a part of DHRS failed. These risks can be calculated via event tree / fault tree analysis.

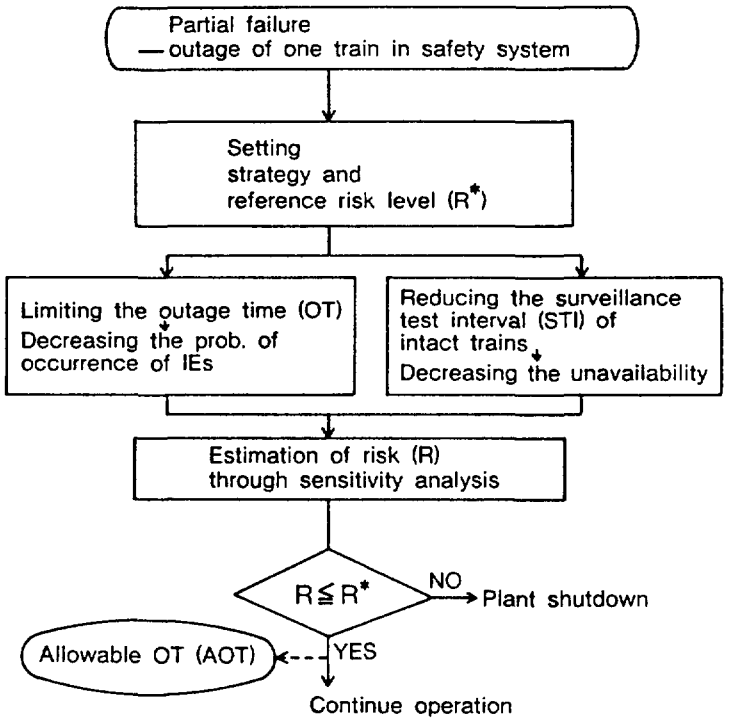


Figure 1 Flow Chart of LCO Rules Examination

Second, the risk levels when a part of DHRS is failed are calculated using fault trees for various test intervals of the remaining intact loops.

Then the present risk is compared with the reference risk and it is determined if the plant should be shut down or not. If the plant operation should be continued, the test interval of the remaining intact loops and the outage time which satisfy the condition is calculated.

2.2 Definition of Risk and Risk Level

As this study is limited to a level-1 PSA, the risk (R) is defined here as the core damage probability in a certain period of time, say one reactor year. On the other hand, the risk level (r) is defined as the present risk per unit time which changes continuously according to the plant situation.

When the plant is under normal operation, the risk level is at r^0 which is not zero. If a component or a subsystem is failed, the failure probability of the system increases and the risk level increases to r^1. And if the failed component is repaired, the risk level returns to r^0 again as shown in Figure 2.

The allowable outage time (AOT) of each component or subsystem is stipulated in the Technical Specifications and if the failed component cannot be repaired within the AOT, the plant must be manually shut down. A manual shutdown requires the actuation of DHRS and it leads to increase in the risk level which is temporary but considerably large. The change of risk level in such a case is shown in Figure 3.

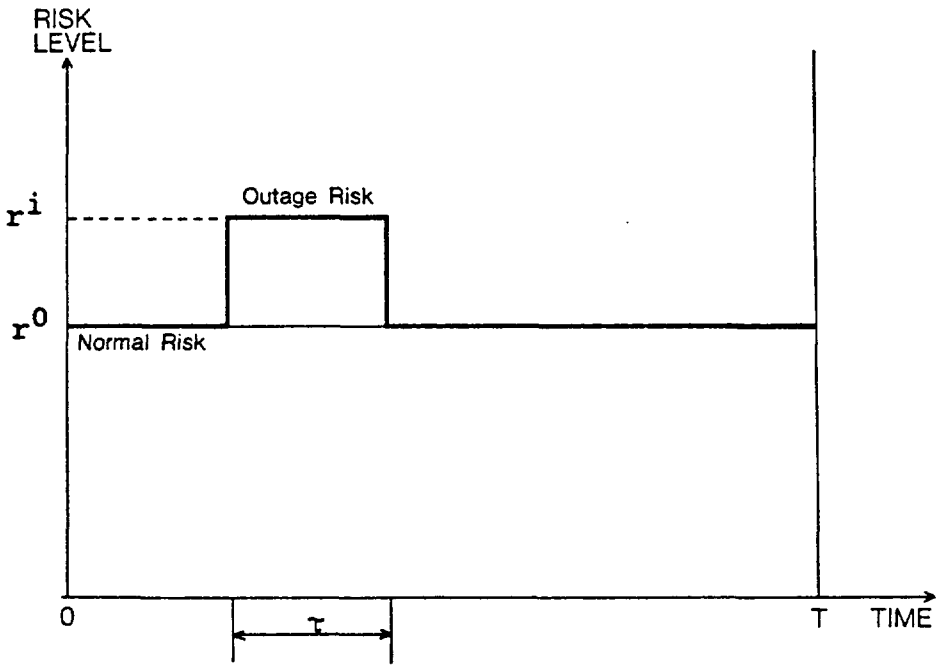


Figure 2 Time History of Risk Level

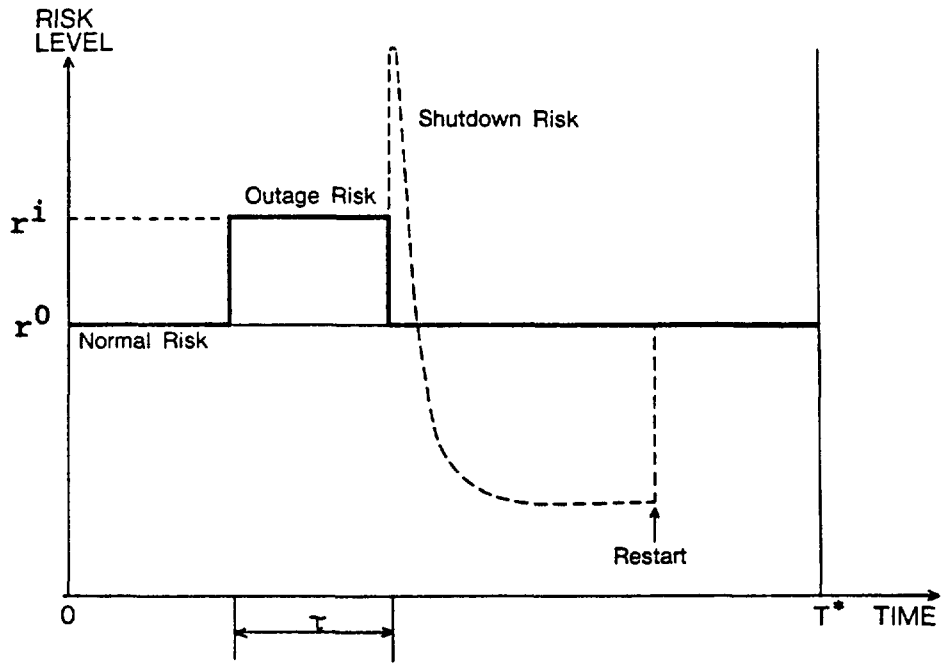


Figure 3 Time History of Risk Level

2.3 Method of limiting risk

We propose several methods to calculate and limit the risk.

Method (1)

Limit the average of additional risk due to a failure of component below a certain fraction of the risk of normal plant operation. This can be represented by the equation below;

$$(r^i - r^0) * \tau / T < \alpha * r^0 \qquad \text{eq. (1)}$$

where r^i: the risk level with a component i failed [/hr],
r^0: the risk level during normal plant operation [/hr],
τ : outage time of a component [hr],
T : a certain time period [hr],
α : the ratio of acceptable risk to the normal risk.

Method (2)

Limit or minimize the sum of the outage risk and the shutdown risk. The risk is expressed as the equation below;

$$R(\tau) = r^i * \tau + \exp(-\tau/\tau_r) * U^i \qquad \text{eq. (2)}$$

where $R(\tau)$: the conditional risk when the outage time is τ hour,
r^i: the risk level with a component i failed [/hr],
τ : outage time of a component [hr],
τ_r: the mean time to repair failed component [hr],
U^i: failure probability of the system with component i failed.

The first term of the right-hand side of eq. (2) represents the risk due to component outage. The second term represents the risk due to manual shutdown where $\exp(-\tau/\tau_r)$ is the probability that the failed component cannot be repaired within τ hour based on the exponential recovery model and plant is manually shut down.

The following three methods can be considered based on the risk defined in eq. (2).

Method (2-1)

Min. $R(\tau)$

Minimize the risk.

Method (2-2)

$R(\tau) < 1.0 * U^i$

Limit the risk below that of immediate plant shutdown after detecting the anomaly. 1.0 means that the plant is manually shut down.

Method (2-3)

$R(\tau) < 1.0 * U^0$

Limit the risk below that of manual shutdown under normal operation. 1.0 means that the plant is manually shut down.

Method (3)

This method minimizes or limits the increment of risk. The risk is expressed as the equation below;

$$\Delta R(\tau) = (r^i - r^0) * \tau + \exp(-\tau/\tau_r) * U^i \qquad \text{eq. (3)}$$

The following three methods can be considered based on the risk defined in eq. (3).

Method (3-1)

Min. $\Delta R(\tau)$

Minimize the risk increment.

Method (3-2)

$\Delta R(\tau) < 1.0 * U^i$

Limit the risk increment below that of immediate plant shutdown after detecting the anomaly. 1.0 means that the plant is manually shut down.

Method (3-3)

$\Delta R(\tau) < \alpha * r^0 * T$

Limit the risk increment below a certain fraction of normal operation risk.

3. APPLICATION

The application of above methods to a DHRS is shown below. As shown in Figure 4, the DHRS of the reference plant consists of three independent loops. DHRS stands by while the reactor is in operation and starts up when the reactor is shut down. Each loop has enough capacity to remove decay heat either by forced or natural circulation. Therefore, when a loop is found inoperable through the periodical test, the reactor needs not be shut down and the failed loop can be repaired. In this application, the loop B is assumed to be failed.

The risk level when all the loops are intact is;

$$r^0 = f_0 * U_{ABC} + f_1 * U_{AC} \qquad \text{eq. (4)}$$

where f_0 : occurrence frequency of initiating event which does not affect the DHRS [/hr],
f_1 : occurrence frequency of initiating event which cause one DHRS loop inoperable [/hr],
U_{ABC}: failure probability of DHRS loops A, B, and C,
U_{AC} : failure probability of DHRS loops A and C.

The risk level when loop B is inoperable and the remaining loops are tested every T_t hours is;

$$r^i(T_t) = f_0 * U_{AC}(T_t) + f_1 * U_A(T_t) \qquad \text{eq. (5)}$$

where $U_{AC}(T_t)$: failure probability of DHRS loops A and C when tested every T_t hours,
$U_A(T_t)$: failure probability of DHRS loop A when tested every T_t hours,

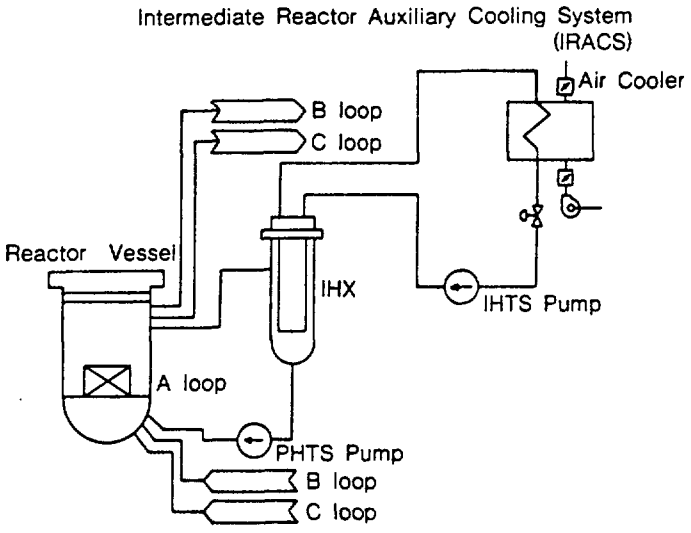


Figure 4 Schematic Diagram of DHRS

Figure 5 shows the failure probability of DHRS for various test intervals when one or two loops of DHRS are failed. The shorter the test interval is, the smaller the failure probability becomes.

The risk when the outage time is τ hours is;

$$R(\tau) = r^{i}(T_t) * \tau + \exp(-\tau/\tau_r) * U_{AC} \qquad \text{eq. (6)}$$

where T_t: test interval [hr],
τ : outage time of a component [hr],
τ_r: the mean time to repair failed component [hr].

The outage time when one loop of DHRS is failed were calculated using the above methods for various test intervals based on the frequency of initiating events and failure probability of DHRS. Figure 6 shows the results. The shorter the test interval of the remaining intact loops, the longer the outage time becomes, but the results depend on the method and the parameter.

Figure 7 shows the risk change with the outage time, when the test interval is 24 hours. Risk is normalized with the manual shutdown risk under normal operation as unity. While the outage time is relatively short, the risk due to manual shutdown is dominant. As the outage time becomes longer, the probability that the component is repaired increases and the probability of reactor shutdown decreases, thus the risk decreases. As the outage continues, the shutdown risk becomes negligible, the outage risk becomes dominant, and finally the risk becomes larger than that of manual shutdown under normal operation.

Figure 8 shows the risk increment change which were calculated using Method (3-3) when the test interval is 24 hours. Risk is normalized with normal plant operation risk

as unity. In the case that the mean time to repair of the failed component is 24 hours, the risk decreases while the outage is less than 100 hours, becomes minimum when the outage is around 100 hours, then increases. When the ratio of acceptable risk level is five percent, the condition is satisfied while the outage is between 60 and 200 hours. In the case that the mean time to repair of the failed component is 168 hours, there is no outage time that satisfies the 5 and 10 percent conditions, but the risk becomes minimum when the outage is around 430 hours.

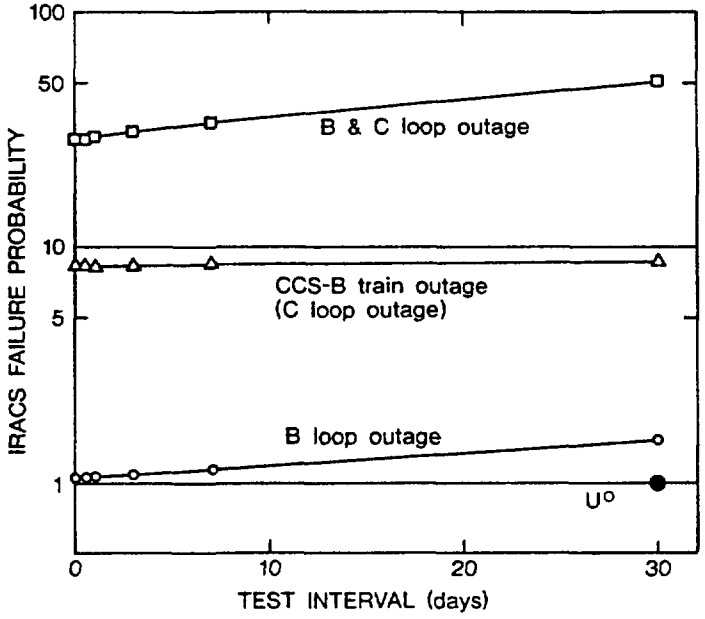


Figure 5 Failure Probability of IRACS

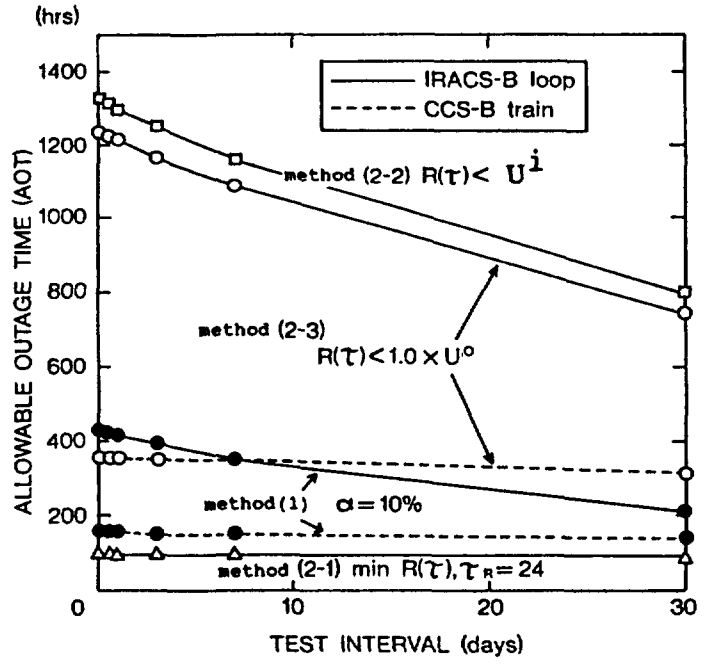


Figure 6 Safety Map for IRACS

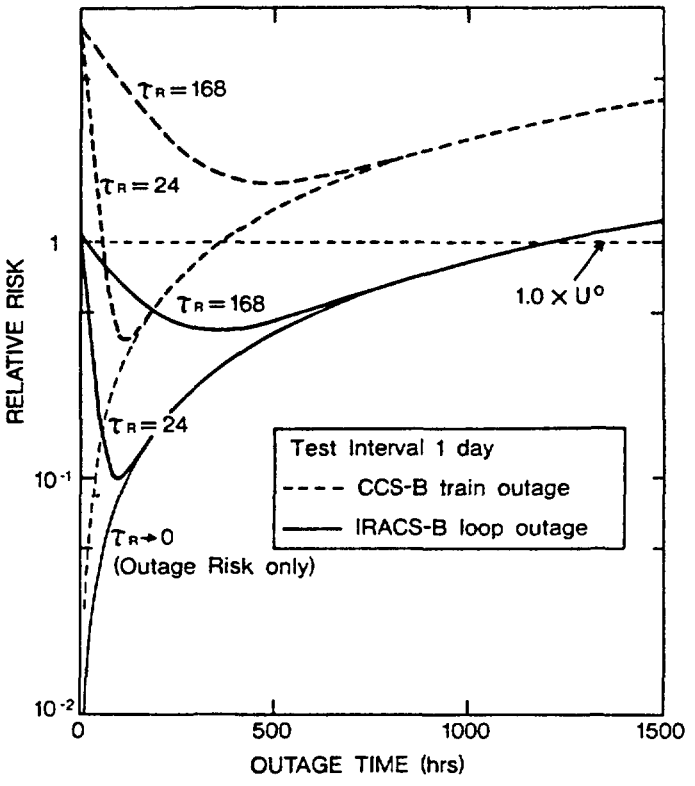


Figure 7 Risk Change with Outage Time

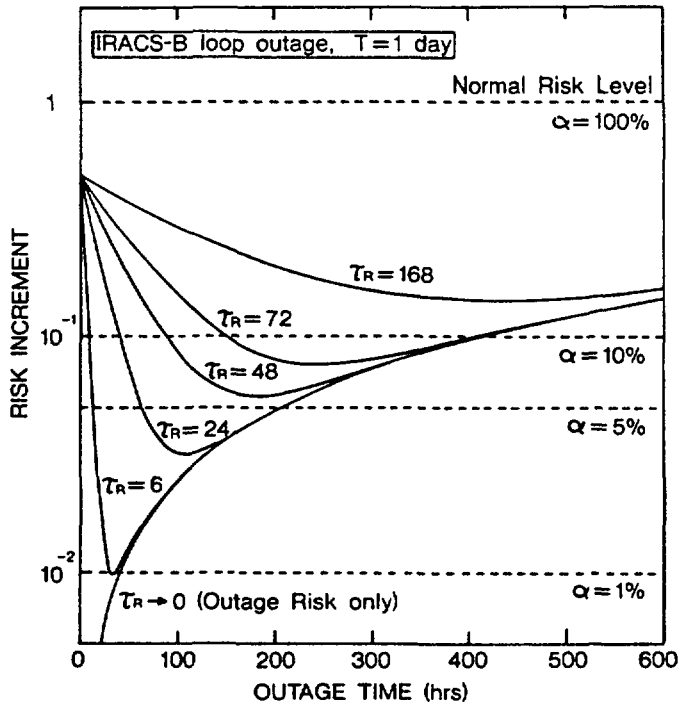


Figure 8 Risk Increment Change with Outage Time

4. PROPOSED METHOD FOR TECHNICAL SPECIFICATIONS EVALUATION

Using the Method (3), following method is proposed to evaluate the Technical Specifications.

(1) Obtain the values for f_0, f_1, U_A, U_{AB}, U_{ABC} through systems analysis,
(2) Decide the acceptable risk level with α and T,
(3) Identify the failed component or system and estimate the mean time to repair,
(4) Calculate the normal risk level r^0 and the risk increment (r^1-r^0),
(5) Draw a chart like Figure 8 for various test intervals,
(6) Decide the range of outage time using Method (3-3),
(7) If no outage time satisfy the acceptable risk follow method (3-1). i.e. continue repair of the failed component until the additional risk becomes the minimum.

5. CONCLUSION

A method of applying probabilistic method for the evaluation of Technical Specifications is proposed. The method considers the risk due to manual shutdown as well as the risk due to the outage, and limit the risk increment below a certain fraction of the reference level.

The method was applied to a DHRS of an LMFBR and Technical Specifications were evaluated.

We plan to apply the method to other systems while evaluating the reference risk level and the acceptable risk level based on the examples of LWRs and other PSAs.

We expect that this method will be combined with the 'living PSA' and construct an on-the-site system which calculates the plant risk level in the real time mode and gives the outage time and test intervals which are best for the plant safety.

REFERENCES

Sato. K., Tobioka, T., Abe. K. and Aizawa, K., "Current Status on PSA-related Activities in Japan," PSA '89 International Topical Meeting Probability, Reliability, and Safety Assessment, April 2-7, 1989, Pittsburgh, Pennsylvania, U. S. A.

Piirto, A., Mankamo, T. and Laakso, K.J., "Development of Technical Specifications Using Probabilistic Methods," NEA/CSNI-UNIPEDE Specialists Meeting on Improving Technical Specifications for Nuclear Power Plants, September 7-11, 1987, Madrid, Spain.

Kani, Y. et al., "Application of Probabilistic Techniques to Technical Specifications of an LMFBR Plant," PSA '89 International Topical Meeting Probability, Reliability, and Safety Assessment, April 2-7, 1989, Pittsburgh, Pennsylvania, U. S. A.

USE OF PSA TO EVALUATE OPERATING STRATEGY COMPLIANCE WITH OPERATING POLICIES AND PRINCIPLES REQUIREMENTS

B.N. DICK, P.N. LAWRENCE
Ontario Hydro,
Toronto, Ontario,
Canada

Abstract

Within the Canadian regulatory environment, the Operating Policies and Principles (OP&Ps) define the operational safety philosophy and the limits and conditions for safe operation of our nuclear generating stations. As is the case with Technical Specifications, these limits and conditions are, for the most part, based on deterministic safety analysis and engineering judgement. However, unlike the Technical Specifications, the OP&Ps are intended to specify a minimum number of key constraints, and to specify them in very broad, general terms.

A program to perform level 3 Probabilistic Risk Assessments (PRAs) at all of Ontario Hydro's nuclear generating stations is being undertaken by the corporation's design organization. At present, the PRA for one station, Darlington-A Nuclear Generating Station, has been completed with work underway, or planned, for the remaining nuclear generating stations.

This paper describes several examples to illustrate how the Darlington PRA has been used to evaluate proposed operating strategy compliance with the requirements embodied in the broad, conceptual limits defined in the OP&Ps.

The paper concludes with a discussion of planned and potential future developments, including the more extensive use of PRAs in the day-to-day operation of Darlington Nuclear Generating Station.

INTRODUCTION

A Level 3 PSA was performed during the design phase of the Darlington "A" nuclear generating station (DNGS, 4 x 880MWe CANDU). The PSA, the first of its kind for an Ontario Hydro (OH) generating station, formed the basis of the station's operational reliability program.

This paper describes how the PSA, and tools developed from the PSA, are used to ensure that plant operating strategies are consistent with the plant's safety philosophy. This philosophy is specified in a document called the Operating Policies and Principles (OP&Ps).

The PSA approach to the assurance of public safety will become increasingly important to OH; Level 3 PSAs will be completed for OH's four older nuclear generating stations over the next 5 years. As experience with PSAs increases and acceptance of the approach improves, it is possible that the OP&Ps will be refocused, taking benefit from the insights of the PSA. A brief discussion of potential future application of the PSA to the OP&Ps is included.

OPERATING POLICIES AND PRINCIPLES

Within the Canadian regulatory environment, OP&Ps are prepared by the plant operator for each of its nuclear generating stations. The purposes of the OP&Ps are to:

1. define the operational safety philosophy for the station;

2. specify limits and conditions for safe station operation, including limits of authority; and

3. act as an interface between OH and the Canadian regulator, the Atomic Energy Control Board (AECB).

The OP&P document has three broad sections:

1. a section covering administrative issues;

2. the main body of the document covering the operating philosophy for each large grouping of safety-related systems (see, for example, Table 4), and

3. an appendix detailing the minimum acceptable performance standards for systems and components, derived from the plant's safety analysis.

Each OP&P is comprised of a principle and, if necessary, the policies (rules) which must be followed if the intent of the principle is to be met. For example, in Table 4, OP&P 68.1 covers shutdown system availability. The contained safety-related principle is that system availability must be maximized, clauses a to d provide rules which must be followed to meet this principle.

The OP&Ps, like Technical Specifications, have historically been developed on the basis of deterministic safety analysis and engineering judgement. Unlike Technical Specifications, however, the OP&Ps specify a minimum number of conceptual and numerical constraints, providing a framework for the preparation of detailed operating procedures. The level of public risk resulting from station operation is maintained at an acceptably low level by ensuring that all operational activities are consistent with this framework.

This approach to assuring public safety evolved from the recognition that all possible plant conditions and transients could not be anticipated, and that to encumber operating staff with well meaning but inappropriate operating restrictions would be counterproductive. The level of detail in the OP&Ps is:

1. sufficient that when an unanticipated event occurs, the Shift Supervisor is able to choose the optimum operating strategy, yet

2. the OP&Ps remain a manageable set of constraints.

A manageable set of constraints, together with training and experience, provides the optimum combination to allow operating staff to respond to unanticipated transients.

DNGS RELIABILITY PROGRAM

Basis of the Program

The licensing approach for the DNGS included two risk-based components: a dose-frequency limit for individual accident sequences (Table 1) and, for selected safety-related systems, a deterministic availability limit (Table 2). This

approach resulted in the definition of availability limits, either explicit or implicit, for a number of poised safety-related systems.

Table 1

DOSE-FREQUENCY LIMITS FOR DNGSA

Frequency	Individual Dose	
	Whole Body	Thyroid
>10E-2	50 mRem	500 mRem
10E-3 to 10E-2	500 mRem	5 Rem
10E-4 to 10E-3	3 Rem	30 Rem
10E-5 to 10E-4	10 Rem	100 Rem
<10E-5	25 Rem	250 Rem

Table 2

DETERMINISTIC AVAILABILITY LIMITS

System	Limit
Shutdown System 1	10E-3
Shutdown System 2	10E-3
Emergency Coolant Injection	10E-3
Containment System	10E-3

The PSA for DNGS, called the Darlington Probabilistic Safety Evaluation (DPSE) (2), was produced in support of the above licensing approach. Thus, the DPSE had to be capable of providing failure probabilities for individual systems in order to demonstrate compliance with licensing limits.

In applying the DPSE to station operation, it was decided not to use the full integrated PSA but rather a system based approach developed from the PSA. If each of the systems were controlled to according to programs developed from the PSA, the overall intent of the PSA, and the station's licensing approach, would be met. Factors in the choice of the system based approach included:

1. the program for each system could be strongly linked to its safety-related significance, the more significant the system the more extensive the reliability program;

2. the system based approach was consistent with the organization of the station based support group;

3. system based models would be simpler to use and interpret;

4. the need to demonstrate compliance with system based unavailability limits.

Application of the Program

Systems at DNGS are divided into two types: process and poised (Table 3). Process systems are those active systems involved in the normal maintenance of fuel cooling and in the generation of electricity. The poised systems, however, are those intended to mitigate the consequences of process upsets, eg. a loss of regulation or a loss of heat transport coolant. The poised systems are further subdivided into: the Special Safety System (SSS), the Major Mitigating Systems (MMS) and the other poised systems (Table 3).

Table 3

SYSTEM TYPES AT DNGSA

Type	Category	Examples
Process		Heat Transport System Moderator System Reactor Regulating System End Shield Cooling System Boiler Feedwater System Steam System Turbine-Generator and Auxiliaries Electrical Distribution System Fuelling System
Poised	Special Safety*	Shutdown System 1 Shutdown System 2 Emergency Coolant Injection Containment System
	Major Mitigating*	Standby Class 3 Power** Emergency Power System** Auxiliary Boiler Feed System# Emergency Service Water System# Boiler Emergency Cooling System# Shutdown Cooling System
	Others	Heat Transport Pressure Relief Turbine Tripping System D2O Recovery System Annulus Gas System Boiler Steam Relief System

* Complete Set
** Standby Electrical Systems
\# Standby Boiler Feed Supplies

Table 4

OP&Ps for the DNGS Shutdown Systems

68.1 Shutdown System Availability (see Appendix B)

The shutdown systems shall be operated and maintained to maximize availability. In order to comply with this principle:

(a) Neither shutdown system shall intentionally be removed from service unless the reactor is in a guaranteed shutdown state.

Removal of either shutdown system from service shall require the prior approval of the Station Manager on case-by-case basis.

The AECB shall be advised prior to removal of both shutdown systems from service where the guaranteed drain state is not being used.

(b) The shutdown systems shall be tested according to programs which demonstrate individual shutdown system unavailabilities, each independent of the other, of less than 10**-3 yrs/yr (as per OP&P 03.5).

(c) Where maintenance is necessary, it shall be done according to policies and limits outlined in OP&P 03.1, OP&P 68.2 and OP&P 68.4.

(d) Any trip function which is found to be impaired must be placed in a safe state or the reactor shall be shutdown in a controlled manner.

68.2 Shutdown System Impairment (see Appendix B)

If either shutdown system is confirmed to be outside the reactivity depth, rate of insertion or accident coverage limits claimed in the Safety Report, the reactor shall be put in the guaranteed shutdown state in an orderly manner and shall remain... shutdown until repairs are completed.

68.3 Shutdown System Modifications

Modifications to the shutdown systems shall only be made according to policies outlined in OP&P 01.6.

68.4 Trip Setpoints (see Appendix B)

For all operating conditions, shutdown system trip setpoints shall be adjusted to maintain the trip coverage as claimed in the Safety Report. Manual adjustment of trip setpoints shall only be done following procedures approved by the Station Manager.

68.5 Resetting of Reactor Trips

Completed reactor trips shall only be reset following specific Shift Supervisor authorization. Such authorization shall be given only after verifying that the condition which caused the reactor trip no longer exists.

The operational reliability program at DNGS is focused on the poised systems and, in particular, the SSSs and MMSs. This emphasis reflects:

1. the nature of poised system failure, ie. not readily detectable;
2. the safety related significance of the system;
3. licensing constraints, particularly for the SSSs;
4. the complexity of the systems; and
5. the likelihood of the systems operating in abnormal configurations.

For each of the SSSs and MMSs an unavailability model was derived from the DPSE; unavailability being the probability that a system will fail to respond to a process upset. These models were reviewed by system responsible engineers to identify modelling assumption which were likely to prove operationally onerous. These potential difficulties were reviewed by non-station based reliability experts and appropriate modifications were made to either the models or the affected programs.

CURRENT APPLICATION OF PSA TO DEMONSTRATE OP&P COMPLIANCE

The requirement in the OP&Ps to maximize safety-related system availability provides an immediate use for the unavailability models derived from the PSA. These models are used to:

1. monitor long term system performance;

2. control system configuration, eg. test deferrals or extended maintenance outages;

3. assess the implications of proposed system design changes, and

4. develop and rationalize system testing programs.

Details of the above applications are provided in Reference 3.

If safety-related system performance is to be controlled using unavailability, it is important that an up-to-date record of the performance of contributing components be maintained. A meaningful record of component performance requires, in turn, a precise definition of component "failure"; the appendix of the OP&Ps provide this definition. In cases where the appendix does not provide sufficient detail to determine whether the component would have satisfied the requirements of the plant safety analysis, data is passed to safety analysts for detailed review.

It is important to note that the unavailability models do not only provide a numerical tool but also a wealth of qualitative data. In assessing the implications of a design change or a revised operating procedure, it is often not necessary to resort to a requantification of system unavailability; a review of the fault tree logic alone can often eliminate proposed changes. This powerful aspect of the PSA/fault tree approach is too frequently ignored.

It must be emphasized that the OP&Ps do not explicitly specify how the contained safety-related principle must be achieved, eg. an unavailability target implies the need for a testing program but the OP&Ps do not specify what must be tested and at what frequency. It is the responsibility of the station support staff to develop the appropriate programs and to be able to justify these programs in light of the OP&Ps.

POTENTIAL APPLICATION OF PSA TO THE OP&Ps

OH has only recently begun to make active use of the PSA approach. The following are potential uses of the PSA currently under examination.

Currently the OP&Ps are, for the most part, based on deterministic safety analysis and engineering judgement. The PSA approach provides the potential to either confirm the deterministic rules or to rationalize the OP&Ps so that they

are clearly focused on the major contributors to public risk. For example, the OP&Ps may provide a tool for answering the following potential questions:

1. are the restrictions placed on a system by the OP&Ps consistent with the safety-related significance of the system ?

2. given that a system is outside of the bounds specified in the OP&Ps, is the response specified in the OP&Ps, usually a timed plant shutdown, consistent with minimizing public risk ?

3. are the system unavailability targets consistent with the safety-related importance of a system ?, or should they be tightened or relaxed ?

Answers to the above questions could not only lead to a refocusing of the OP&Ps but could also provide valuable information on the relative importance on safety-related systems, functions and components.

OH has recently begun exploring the possibility of using risk-based safety goals and value impact analysis for assessing proposed design or operational changes. The PSA approach provides the potential for ensuring that a cost effective solution, consistent with the requirement to minimize public risk, is chosen. This solution may be radically different from a solution based solely on deterministic rules and engineering judgement.

SUMMARY

OH has completed a PSA for one of its nuclear generating stations. This PSA, and tools developed from it, are being used to ensure that operating strategies are consistent with the safe operating envelope defined in the OP&Ps. As experience with the PSA approach increases it is likely that its insights will increasingly be incorporated into the OP&Ps. The benefits of this wider application will include operational programs and decisions more clearly focused on the major contributors to public risk and improved operational flexibility.

REFERENCES

1. D-SI-1.18, Darlington Nuclear Generating Station Operating Policies and Principles, Ontario Hydro.

2. Darlington Probabilistic Safety Evaluation - Main Report, Ontario Hydro, December, 1987.

3. P.N.Lawrence and S.Petrella, PSA Based Elements of the Reactor Safety Operational Reliability Program at Ontario Hydro, 2nd TUV Workshop on Living PSA Application, Hamburg, May 7, 1990.

OPERATIONAL DECISION ALTERNATIVES IN FAILURE SITUATIONS OF STANDBY SAFETY SYSTEMS

T. MANKAMO
Avaplan Oy,
Espoo

M. KOSONEN
Teollisuuden Voima Oy,
Olkiluoto

Finland

Abstract

When a failure is detected in safety systems during plant operation, the risk level may increase much above the baseline, specially in rare multiple failure situations. In such cases the operators face different operational alternatives, eg. testing the remaining parts of safety systems, and/or decision on plant shut down or some backup arrangements. A series of applications at the Finnish nuclear power plants prove that the probabilistic risk and decision analyses can provide support for the systematic comparison of these alternatives.

At the TVO plant (BWR), the probabilistic analysis has shown that in failure situations of the residual heat removal systems, the shutdown constitutes a higher risk than continued operation over usual repair times of less than one day. Based on the results, appropriate modifications to the technical specifications and operating instructions are under way concerning repairs of multiple train failures in residual heat removal systems during power operation.

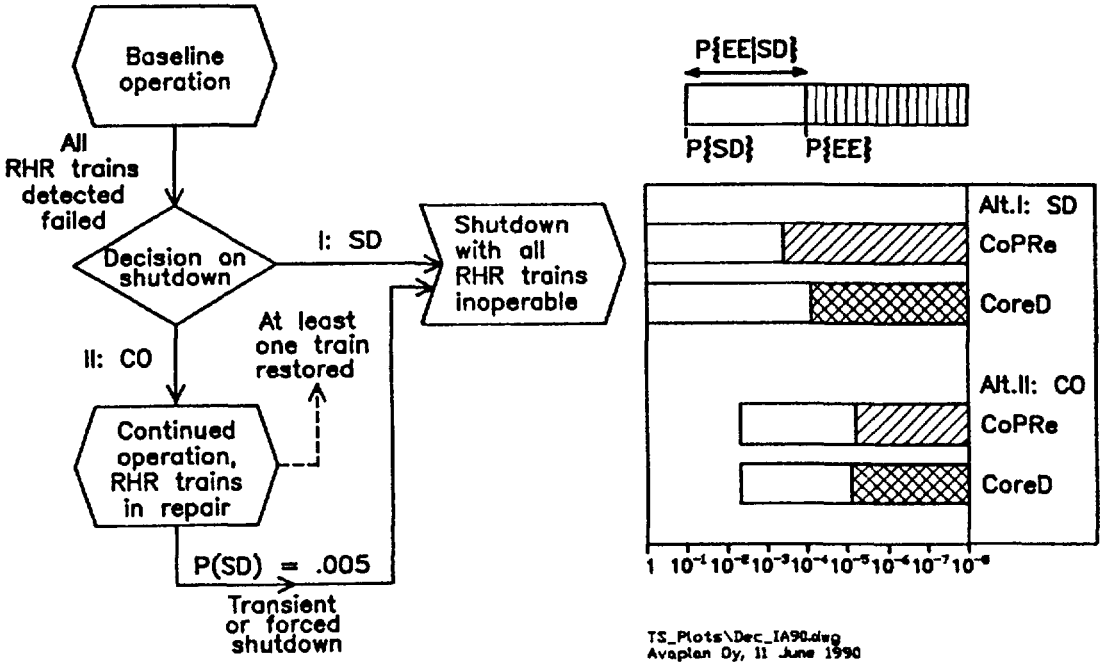
---

1 INTRODUCTION

In a nuclear power plant, the influence of a failure detected during power operation depends on the systems and safety functions affected. For the 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 primary to find out the operational alternative of minimum risk until the normal plant state is restored.

1.1 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.1, and will be discussed in more detail below. There are further alternatives such as



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 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 [3]. Likelihood of the plant shutdown with the associated demand on RHR function, and the expected risk of undesired end events are presented on the right hand side for the operational alternatives.

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

- 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 even when no plant shutdown requirement is actual? This question is specially relevant when the staggered testing scheme is used.

The benefits and risks of various alternatives may not be readily deemed. The probabilistic methods can provide valuable aid in the problem resolution, as shown by the recent applications at the Finnish nuclear power plants. The applications range from the consideration of preventive maintenance (PM) during power operation and surveillance test intervals (STI) to allowed outage times (AOT) for safety systems [1-4].

1.2 Method development

The successful treatment of the subject has called for the development of new methodological ideas in regard how to model and quantify expected risk of decision alternatives - and how to take the uncertainties into account in order to verify the confidence in conclusions. The main advances are concerned with [5-7]

- modeling of phased mission by using extended event sequence diagram
- consideration of recovery paths
- implementation of time-dependent component models based on shared cause model of common cause failures (CCF).

For the processing of event sequences and specific type 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.

In this paper, the emphasis will be on the description of the reasoning process and experiences of how to utilize probabilistic methods in safety related decision making and planning of operating instructions. A more general and thorough treatment of the subject area is presented in the final report of the joint Finnish-Swedish project "Optimization of tecnical specifications by use of probabilistic methods", NKA/RAS-450, which was conducted during 1985-89 as a part of the research program of NKA (Nordic Liaison Committee for Atomic Energy) [8]. The application at the TVO plant described here, served also as a case study for consideration of LCO issue within the NKA/RAS-450 project.

2 CONTINUED PLANT OPERATION VERSUS SHUTDOWN

The increased risk level, known by the operator in a failure situation, is illustrated schematically in Fig.2. The operator faces alternative paths to proceed. The main decision to be made then is (compare also to Fig.1), whether to

1) continue plant operation over the repair time of the fault or
2) shut down the plant, or proceed to some other operational state where the faulted component's inoperability has a smaller influence.

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

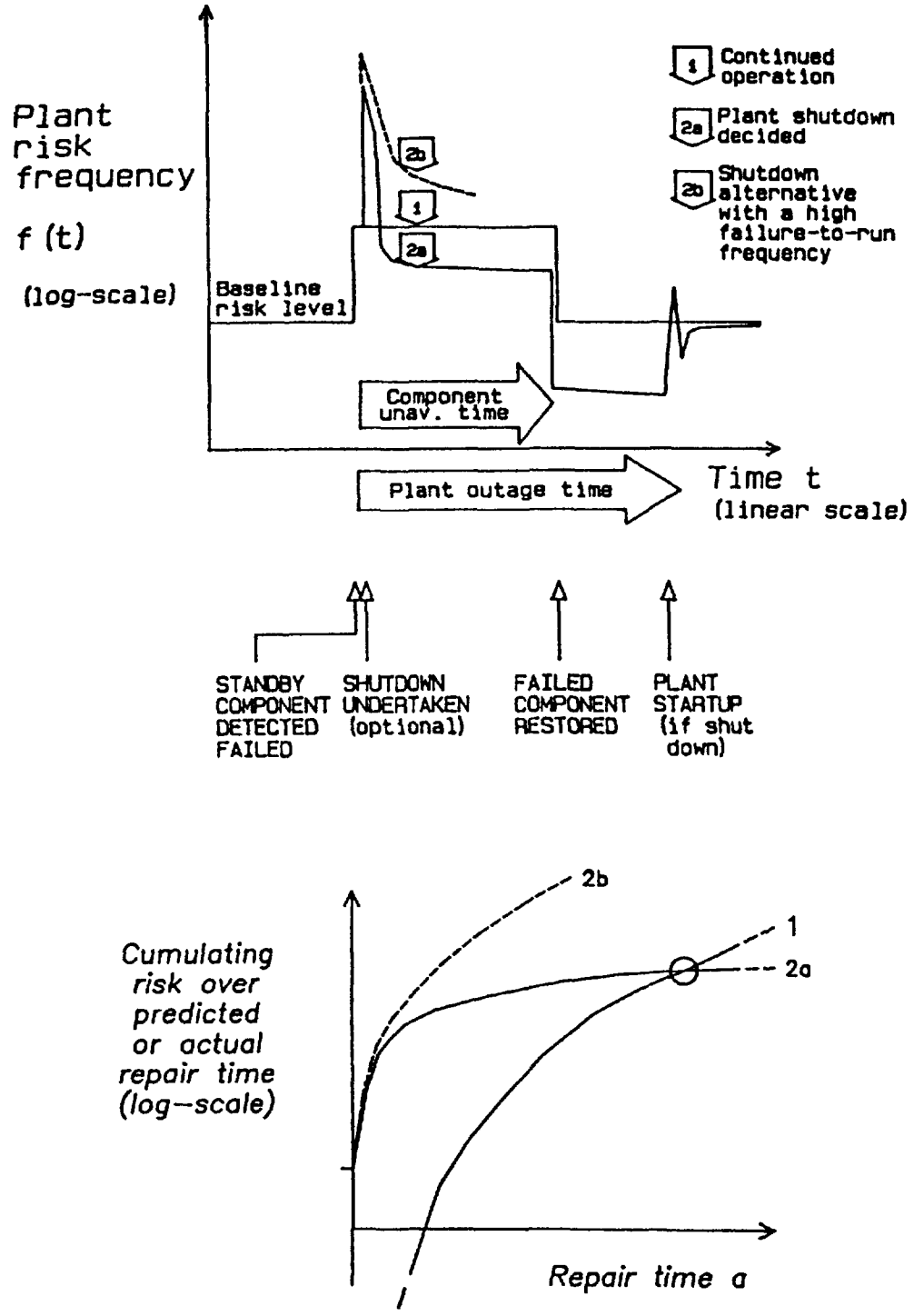


Figure 2. Conditional risk frequency in failure situation of a standby safety system with comparison between the operational decision of plant shutdown versus continued operation. The corresponding cumulative risks over prevailing failure state are presented in the lower part [5].

- 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 grid, etc.)

In Fig.2, Curve 1 represents the case of continued power operation over the repair time. The risk associated to 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.

2.1 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 shortly repairable 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.2. The crossing point of Curves 1 and 2a represents the shortest repair, which, if exceeded, justifies 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.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 some 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.1, where the

- whole bars represent the likelihood of entering shutdown 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

The first entity, likehood of entering shutdown, is 100% for the decided shutdown, but relatively small in 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 favoring continued operation as a safer alternative over usual repair times.

2.2 Influence of preset AOT

Above, 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.

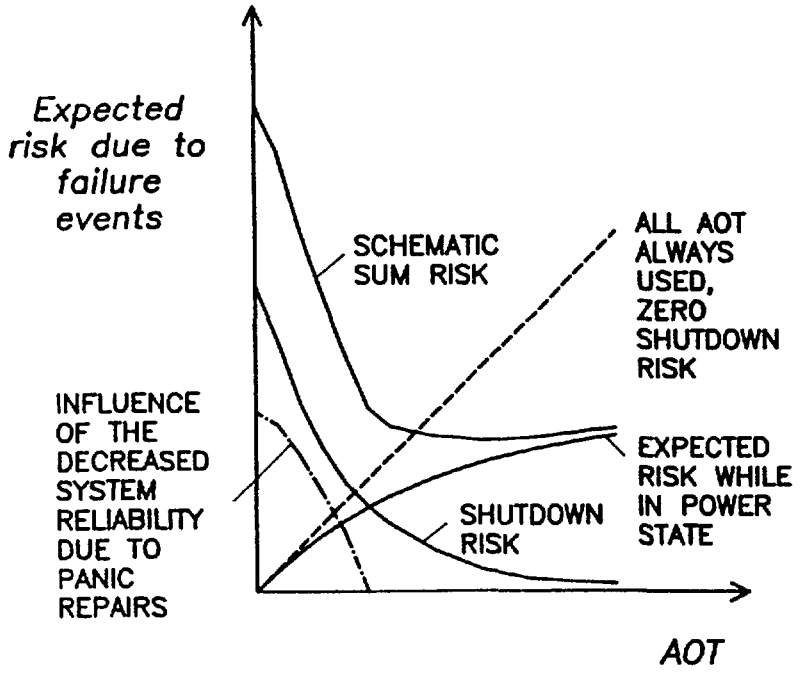


Figure 3 Schematic presentation of, how a preset AOT influences expected lifetime risk.

The experiences show that if AOT is longer than the mean repair time, so 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 short AOT may result as a side effect in situations where faults are attempted to be repaired hastely 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 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 [9-10], there is unrealistically assumed that given any AOT, it all will be used in every repair. This results in erroneous correlation between the expected risk and AOT as illustrated in Fig.3: the stated assumption together with the omittance of shutdown risks, means that the total risk increases linearly as the function of AOT (dashed curve in Fig.3).

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. The AOT criteria are discussed in more detail in [8], in many respects paralleling the scheme of Ref.[11].

3 TS PROBLEM RESOLUTION STRATEGY

The treatment of 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 contrary to the consideration of acceptable risk increase over continued operation in the LCO state and the eventual trade-off between test interval changes, as has been typical in other applications [9-11].

In the resolution strategy structure proposed in [9], the many kind of constraints, which limit the possible resolution alternatives, are not considered as explicitely 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.4, where the contraints influence right at the beginning on the selection of resolution alternatives. This guarantees that practicable alternatives are selected for deeper investigation.

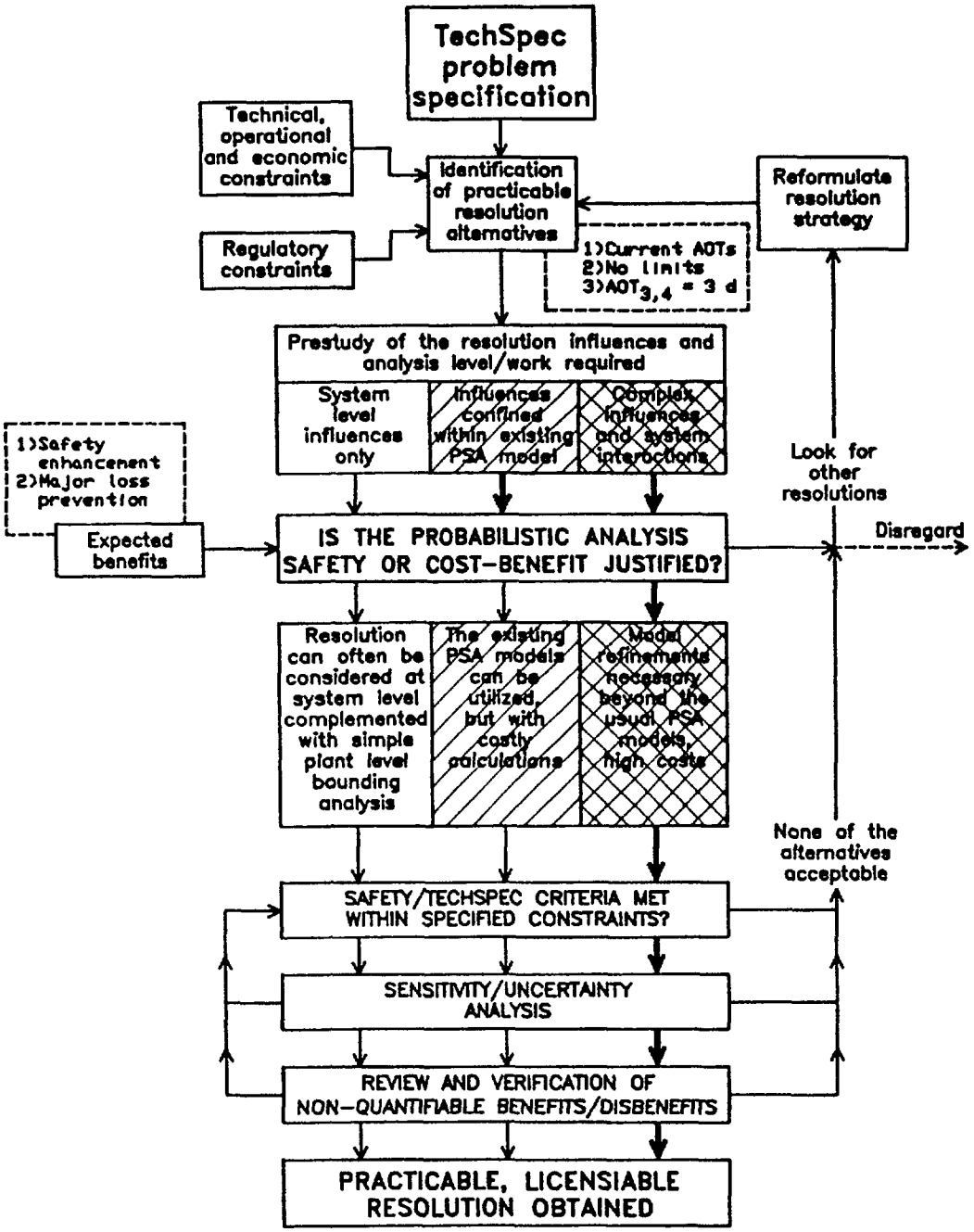


Figure 4 TS problem resolution strategy in the analysis of the AOT issue in the TVO/RHR system case [12].

Another important difference is the inclusion of the prestudy stage, because that is usually needed in order to clearly define the problem and to predict the analysis work required and expected benefits, prior to start or not an actual, bigger analysis effort.

Also the confinement of the analysis at the lowest (least resources consuming) level is structured in another way. The emphasis should whenever possible be placed on the search of

- "smallest risk alternative within the constraints"

compared to

- "acceptable risk increase".

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

4 TVO CASE

4.1 Plant/RHR systems description

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. Safety-related systems are divided into four redundant and from each other separated parts (4 x 50 or 4 x 100 per cent subsystems).

The systems that can be used for residual heat removal RHR function are schematically presented in Fig. 5. There are three diverse paths (321-721-721, 322-721-712 and 321-331-763-714) available for removing heat in reactor shutdown state from the primary system to the sea, which is the ultimate heat sink. Turbine condenser could also be used for heat removal in some cases. These paths have a specific order of operational preference, which means important functional dependences to be taken into account in the modelling and quantification of event sequences.

4.2 Case study layout

The background to the study was the general interest to compare LCO shut down with continued operation in RHR system failure states. The resolution flow followed is presented in Fig.4. Because RHR function is needed in shutdown state, the current LCOs were considered nonlogical, as they did not allow repair during continued plant operation, in the cases of three or all four trains failed. The

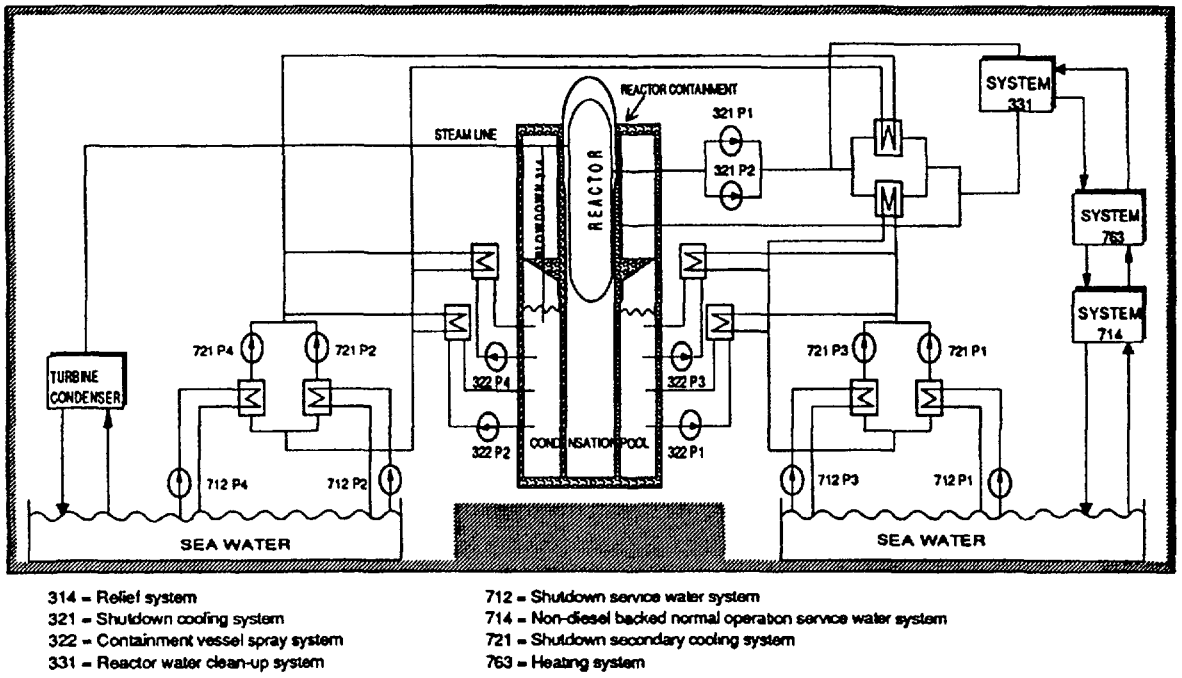


Figure 5 Residual Heat Removal systems at the TVO plant (BWR).

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 cases.

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.

During the early stages of the study, no plant PRA was available. Furthermore, because more advanced methods need to be applied beyound what 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 benefitting from the PRA.

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

4.3 Risk/end events

The analysis end states are divided into two categories. The first one is a failure of the RHR and the second one is a failure to supply water to the reactor. Undesired end events considered, representative for the influence of multiple RHR failures on the plant risk are:

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

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

The loss of the ordinary RHR function failure does not mean a reactor core melt, if the feedwater is operable and the core is covered with water. The residual heat is removed from condensation pool by boiling and releasing steam from containment via pressure relief lines, which are built for severe accident sequences. A failure to retain water level high enough in reactor leads to reactor core melt and thus also to radioactive release.

These two end states are handled separately, when making comparisons between plant shutdown and continued operation alternatives.

4.4 Main results

The main result is the fact that in case of failures in 721/712-systems the continued operation over usual repair times is preferable to shut down. This is especially obvious when having a triple or quadruple failure.

When making decision about the lenght of AOT one should take into account both the break point in the cumulative risk over predicted repair time and the expected risks per event or/and per lifetime. The break points are presented for CoPre and for CoreD end states in lower parts of Figs. 6-7.

4.5 Proposed AOTs/operating instructions

The following conclusions can be made:

1) In case of single failure the risk frequency increase is small and also the expected risk is small. The current 30 days AOT is deemed suitable.

2) In case of douple failure the risk frequency increase is moderate, but the expected risk over mean repair time of less than one day for continued operation is still lower than shutdown alternative. The current 3 days AOT is deemed suitable.

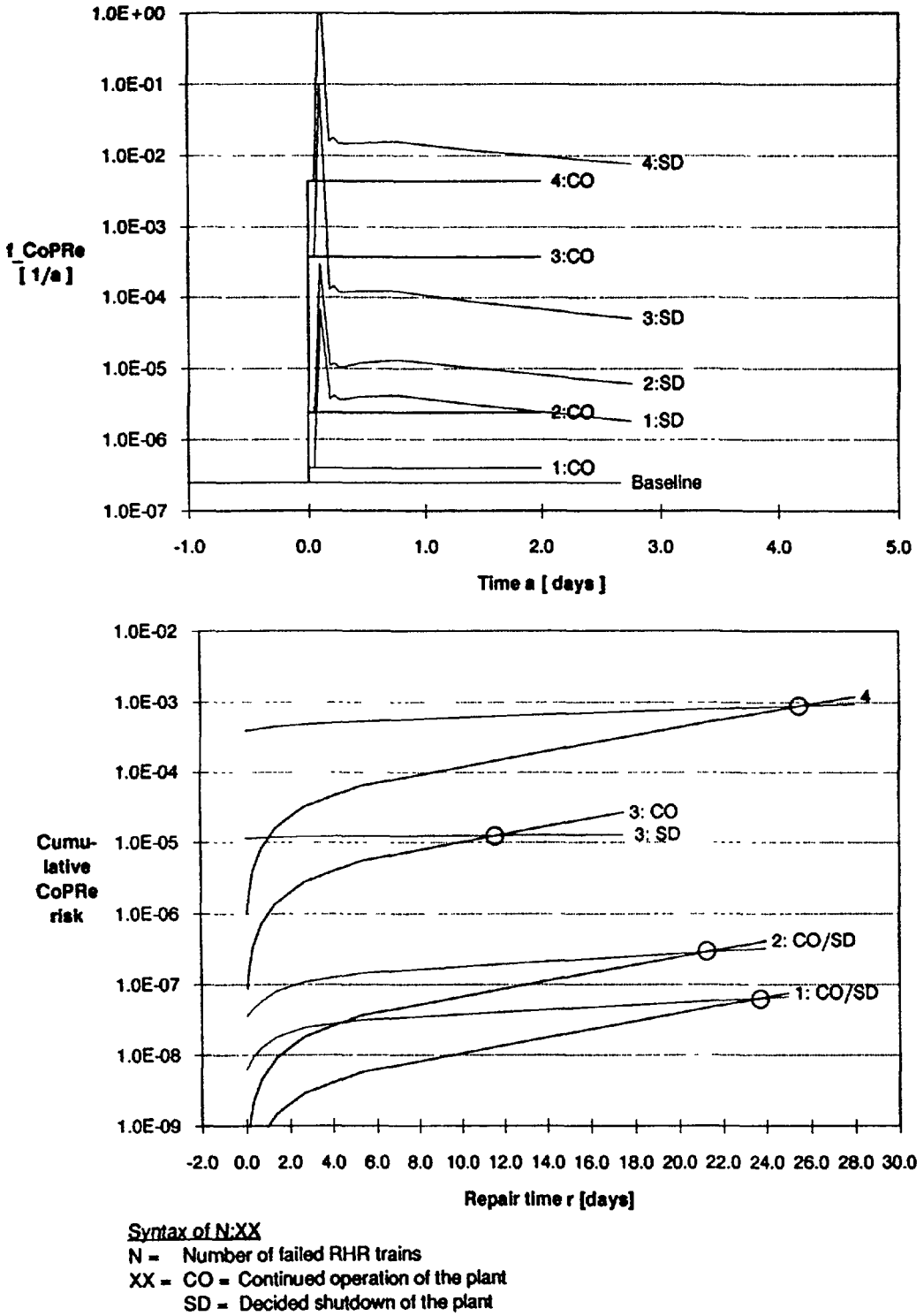


Figure 6 Risk frequency and cumulative risk over predicted repair time for the containment pressure relief due to loss of RHR in the TVO/RHRS case [3].

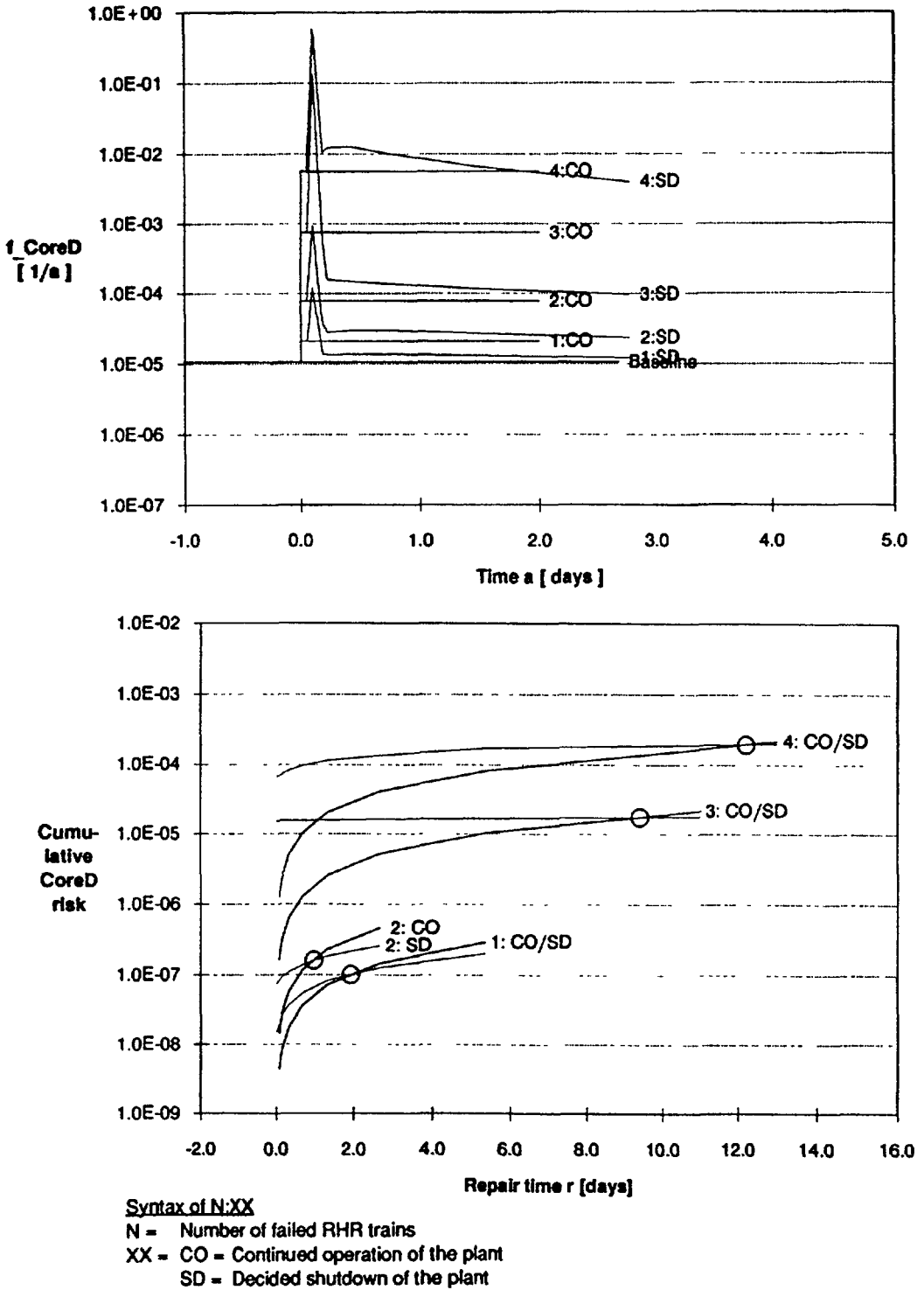


Figure 7 Risk frequency and cumulative risk over predicted repair time for the coredamage event due to loss of core cooling in the TVO/RHRS case [3].

3) In case of triple or quadruple failure the immediate shutdown constitutes significantly higher risk than continued operation over mean repair times.

Because the advantage of the continued operation for usual repair times in triple and quadruple failure situations is so obvious, the requirement in current technical specifications to shut down the reactor in 24 hours will be changed to allow maximum 3 days AOT.

Because the detailled specification of the new AOT rule is quite difficult, we have used an instructions diagram to aid in the implementation. The instructions diagram presented in Fig. 8 gives you guidance how to proceed in case of 2 or more failures are detected in RHR trains during power operation. In such a case, the plant is in the state of 3 days Limited Condition of Operation (LCO). There is two ways to get out that state:

1) All but one of the failures are repaired, then the 30 days LCO is entered or
2) No more repairs are possible during the remaining AOT and the plant shall be shut down.

If the repairs have not been completed during the first day of the 3 days AOT, the remaining 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.

5 SUMMARY

The relationship between the continued plant 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 generalized.

The risk analysis methods have proved to be applicable and useful in comparison of operational decision alternatives. The complexityof phenimena to be studied implies, however, that both good analytical scills and understanding of plant operations and design are necesssary for successful treatment of the subject. Uncertainties need to be carefully considered in order to verify the conclusions.

Based on the results, appropriate modifications to the technical specifications and operating instructions are under way. The repair time limit of three days, currently allowed only in double failure situations, will be extended to failure situations of three or all four redundant trains in the residual heat removal systems considered.

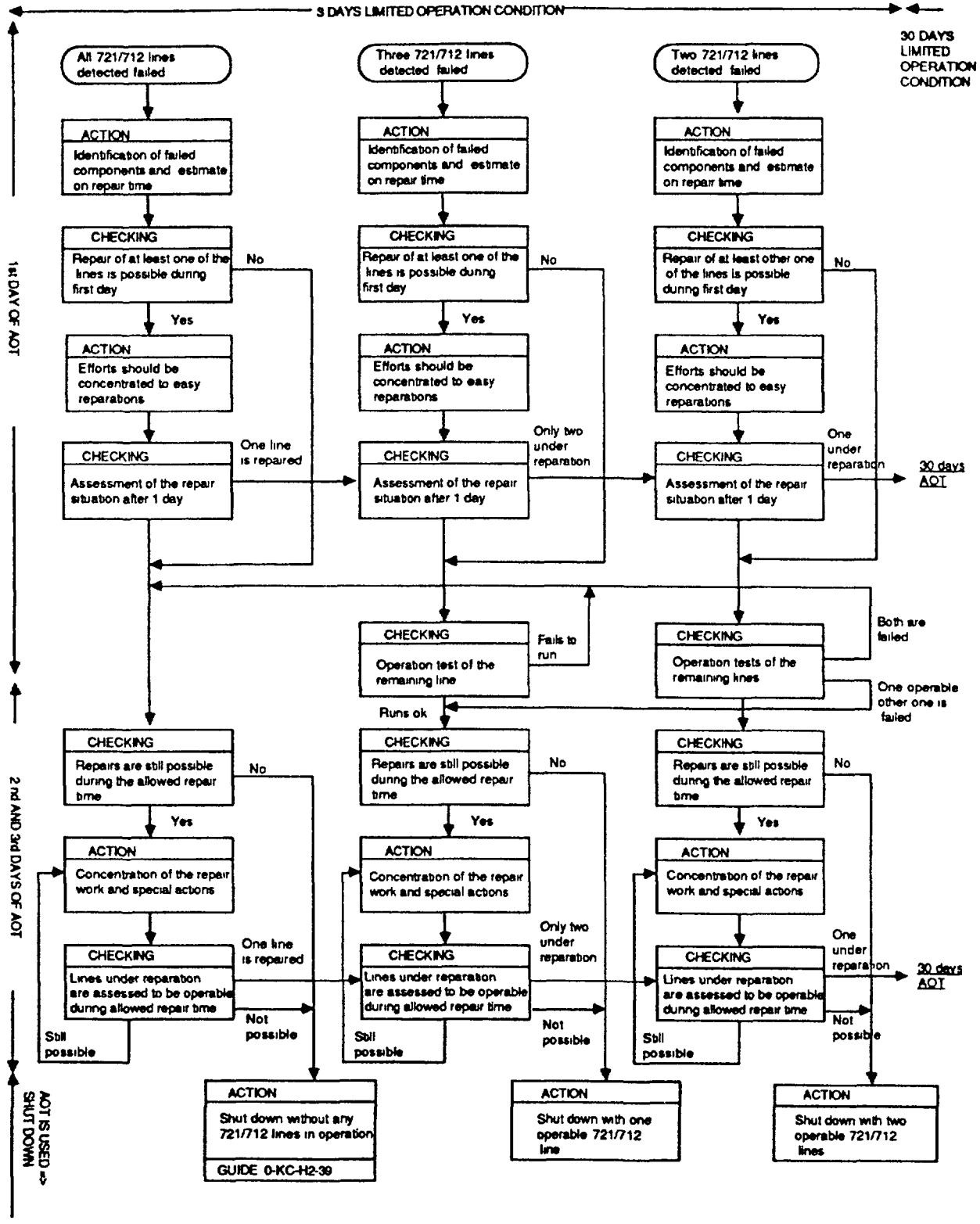


Figure 8 Instructions diagram which is proposed to aid operators in multiple failure situations.

REFERENCES

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

2. 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.

3. 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.

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

5. 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.

6. 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.

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

8. Final report of NKA/RAS-450, Optimization of technical specifications by use of probabilistic methods - a Nordic perspective. Ed. by Laakso, K.J, Technical Research Centre of Finland, May 1990.

9. 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.

10. 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.

11. Vesely W. & Samantha P.K., Risk Criteria Considerations in Evaluating Risks from Technical Specification Modifications. Technical Report, BNL & SAIC, Draft, January 1989.

12. Mankamo, T., Engqvist, A. & Kosonen, M., Resolution strategy of TechSpec problems. 12 June 1989.

EVALUATION OF VVER 440 TECHNICAL SPECIFICATIONS USING PSA

Z. KOVÁCS
Research Institute of Fuel and Energy Complex,
Bratislava, Czechoslovakia

Abstract

In the paper two case examples are chosen to demonstrate revision of VVER 440 technical specifications regarding surveillance frequencies and out-of-service times.

Two V-213 type units have the same Reactor Protection Systems (RPS), but different test intervals for measuring channels, namely:

a) each channel has to be demonstrated operable once each month;
b) each channel has to be demonstrated operable once every two months.

In case of the second case example, AOT risk measures at the system level were calculated for the components of High Pressure Core Cooling System (V230 type reactor).

1. Introduction

Two nuclear power plants, located in Jaslovské Bohunice and Dukovany, are in operation in Czechoslovakia. The plants are equiped with VVER-440 reactors. The Jaslovské Bohunice NPP consists of two V 230 and two V 213 type units, the Dukovany NPP consists of four identical V 213 type units. The later units (V 213) have modernized control and safety systems.

Technical Specifications (TS) define limits and operating conditions to the operation of nuclear power plant. TS give the test intervals, test duration time and in case of faults allowed outage times for repair and maintenance of safety systems. During tests and allowed outage times, the power operation is allowed to continue, but if the test duration or repair time will be exceeded, for the increase of the risk the operational conditions have to be changed to a safer condition. Usually this means a cold shutdown of the power plant. In some cases the plant may request an extension of allowed outage time from authorities responsible for nuclear safety. Reduction in the number of shutdowns results in increased plant availability and hence economic benefits.

TS of VVER 440 type reactors have been based on deterministic analyses presented in Final Safety Analysis Report and on engineering judgement. The probabilistic methods provide a systematic approach which can be used to evaluate the additional risk during the test and the presence of component fault in safety related systems. In case of a fault it allowes compare the benefits and the transient risk of continued power plant operation. Probabilistic assessment combined with operating experience data can in this way be used as a valuable aid in decision making and also in revision of technical specifications based on deterministic analyses.

In the present article two case examples are chosen for demonstrating VVER 440 technical specifications revision regarding surveillance frequencies and out-of-service times.

2. Case Example 1 - Revision of the test interval for the reactor protection system (VVER 440-V 213)

The reactor protection system (RPS) acts to prevent reactor conditions from exceeding safe limits or to reduce severe consequences of occured major disturbances. It has four different levels (RPS-I-IV) such as fast and slow trip. RPS-I has the highest level interaction by initiating simultaneous drop of all control rods with gravitational speed of 20-30 cm/s. Safety signals are groupped as: nuclear signals (deduced signals based on ex--core measurements) and technological ones (non-nuclear signals of any part of unit).

RPS-I includes measuring channels, logic trains and terminal train. Measuring channels are used for sensing and conditioning of various nuclear and non nuclear parameters. If a conditioned parameter exceeds its limit boundary a safety signal is generated for the connected logic train. A 2-out-of-3 logic train receives safety signals from 3 measuring channels, performs logic operation and activates the terminal train. There are two sets of measuring channels and logic trains for each parameter (2x2-out--of-3). Functional diagram of RPS measuring channels, logic trains and terminal train is in Figure 1-2.

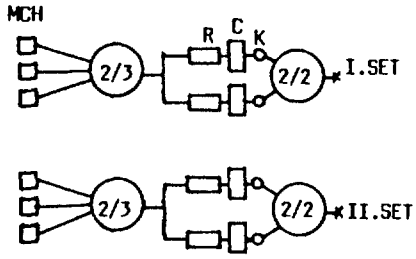


FIG. 1. Measuring channels and logic trains of RPS-I.

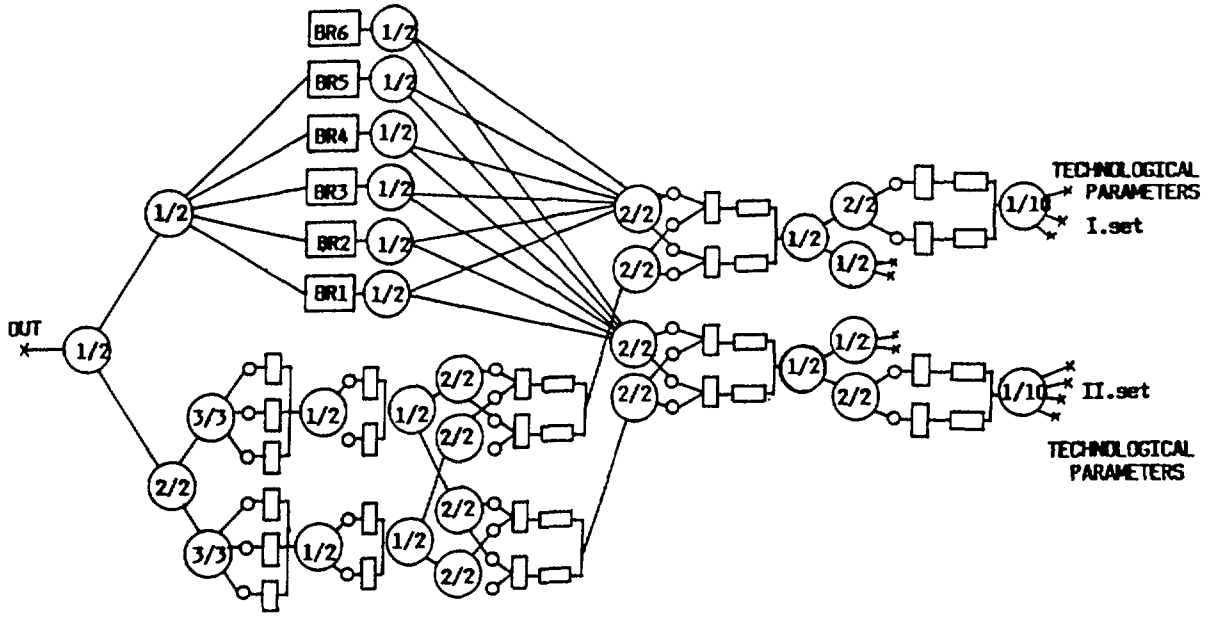


FIG. 2. Terminal train of V 213 RPS-I system; R: resistor, C: relay coil; K: relay contacts; BR: control block of driving mechanism; MLC: measuring and logic channels.

For RPS-I the following limits are given in the current TS of 3. unit of Jaslovské Bohunice NPP:

- Each RPS-I channel have to be demonstrated operable once each month. The two sets are tested separatly: one set each two weeks. (Physical interlocks are provided to prevent two RPS-I sets from being bypassed at one time)
- In the event that one of the three channels of the same logic train is inoperable, reactor operation may continue for up to 72 hours. While the channel is in repair the RPS-I will be reduced to 1-out-of-2 coincidence.
- In the event that two of the three channels of the same logic train are inoperable, the given set have to be done into the test mode, where can be bypassed max. 8 hours.

- The monthly check of a set can affect the RPS availability max. for 8 hours.
- The logic trains and terminal train have to be demonstrated operable twice each year during power operation.

The 1. unit of Dukovany NPP has the same RPS-I. The only difference is in test interval of channels:

- Each RPS-I channel has to be demonstrated operable once each two months (the 1. set in odd month and the 2. set in even month).

Other limits are the same as in case of 3. unit of Jaslovské Bohunice NPP. The task is to assess consequences of difference in TS.

A fault tree methodology was used to estimate the avarage unavailability of both RPS-I. The results in both cases are the same: 6.9E-5. Reactor protection system unavailability for different test intervals of channels is in Figure 3. It is observed in Figure 3 that the unavailability of the RPS-I up to 3 months test interval of channels is constant. The increase in unavailability occurs after 3 months. Calculations resulted that the highest contribution to the RPS-I unavailability is from terminal train. Contribution from measuring channels appears only in case of their testing after 3 months.

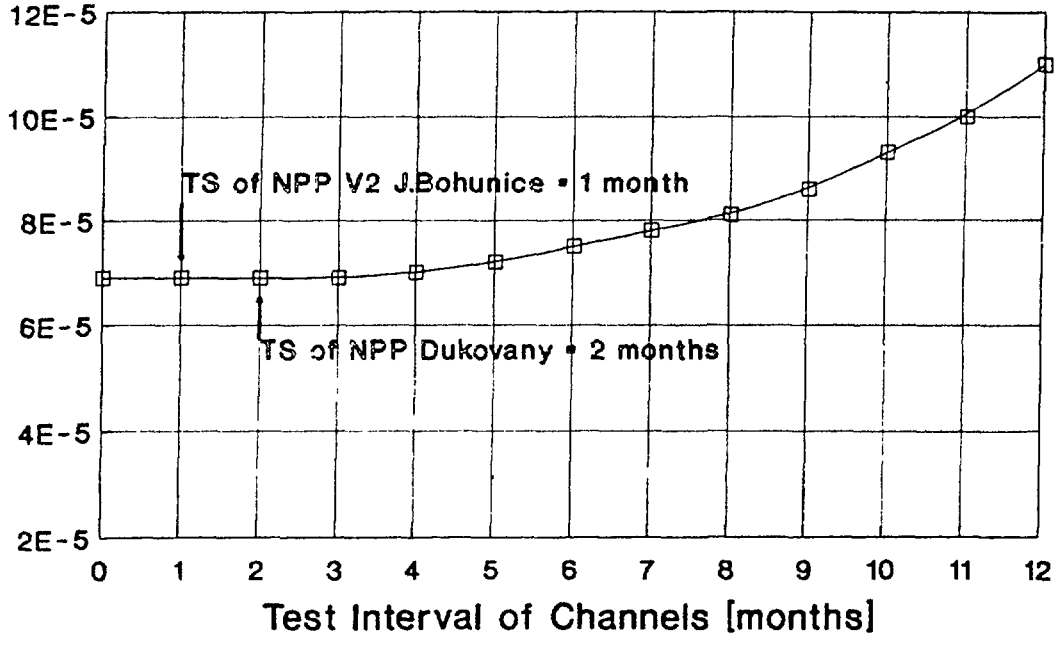


FIG. 3. Reactor protection system unavailability for different test intervals of channels.

The terminal train contains minimal cut sets with two components. These cut sets highly increase the unavailability of trip signals produced in measuring channels and logic trains.

These results show us, that the test interval of RPS-I in case of 1. unit of Dukovany NPP is more convenient than in case of Jaslovské Bohunice NPP. Therefore a suggestion was given to change the RPS-I test interval in the TS of the 3. unit of Jaslovské Bohunice NPP from 1 month to 2 months.

Less testing can lead to reduction of human errors during test, the shift supervisor and control room operator will have to spend less time in authorizing, overseeing and participating in the performance of the test, hence having more time to spend in monitoring other plant functions pertaining to normal plant operations.

3. Case Example 2 - Revision of Allowed Outage Time (AOT) for High Pressure Safety System of the 1. unit of J. Bohunice NPP

The high pressure safety system is provided for emergency core cooling during a loss of coolant accident when the primary reactor coolant system pressure remains high. A simplified schematic of the system is shown on Figure 4. In the system six pumps are shared between two technological groups.
Technical specifications require:

- Two out of three HP pumps shall be maintained operable and a pump can be inoperable for 72 hours from both technological groups.

The TS do not allow the maintenance of MOV HD10A1 and HD20A1 during power operation. The task is to calculate the influence of MOV outage on the operating risk of the unit.

The system level calculations were performed for the components in the HP safety system. The emergency core cooling success criteria was determined by thermohydraulical calculations.
The criteria up to 200 mm LOCA break size is met if a HP pumps injectswater into the primary circuit. (The design basis accident is 100 mm LOCA break size).

At the system level of analysis, the baseline unavailability and increased unavailability due to the outage are calculated. The baseline calculations are similar to that performed in PSAs.

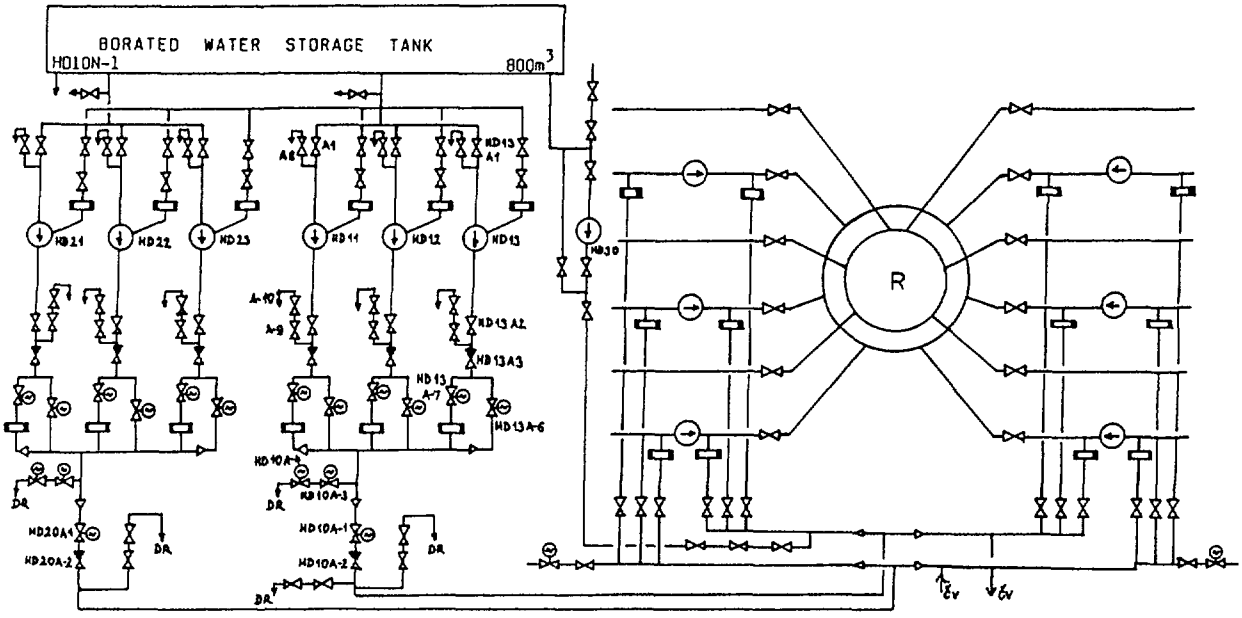


FIG. 4. High pressure safety system.

The increased unavailability is the conditional unavailability during the outage. The conditional unavailability is calculated considering the system reconfiguration during the outage (unavailability of the downed component is 1).

The operating risk of a plant due to an AOT is the risk associated with the component being down and unavailable during an accident. This risk is sometimes called the conditional AOT risk. The cummulative AOT risk is the risk associated with the projected downtime of the component over some period of time.

The AOT Risk Measure at the system level is:

$$\frac{Q^+}{Q} \cdot \frac{d}{T} \leq \beta \quad \text{, where}$$

Q - Baseline system unavailability
Q^+- Increased system unavailability (conditional)
d - Allowed outage time
T - Reference time period
β - Control value on the risk from a given downtime.

The system level calculations performed for the components in the HP Safety system is presented in Table 1 and Figure 5. The differences are primarily due to the differences in the importances of the components for the system. The highest contribution

to the system unavailability is from check valves (HD10A2 and HD20A2) and MOV (HD10A1,HD20A1). This is reflected by the higher values of the AOT risk measures for these components.

Table 1.

AOT Risk Measures at the System level
for Single Component Outage in HP System
(Q=4.0E-2, T=7000 h)

Component under maintenance	Q^+/Q	$\frac{Q^+}{Q} \cdot \frac{1}{T}$ d
HP pumps HD 11-13; HD 21-23	1.23	1.8E-4.d
CHECK VALVES HD 10A2, HD 20A2	5.37	7.7E-4.d
MOV HD 10A1, HD 20A1	5.45	7.8E-4.d
MANUAL VALVES	1.21	1.7E-4.d
CHECK VALVES HD 11-13A2 HD 21-23A2	1.22	1.7E-4.d
MOV HD 11-13A6,7 HD 21-23A6,7	1.02	1.4E-4.d

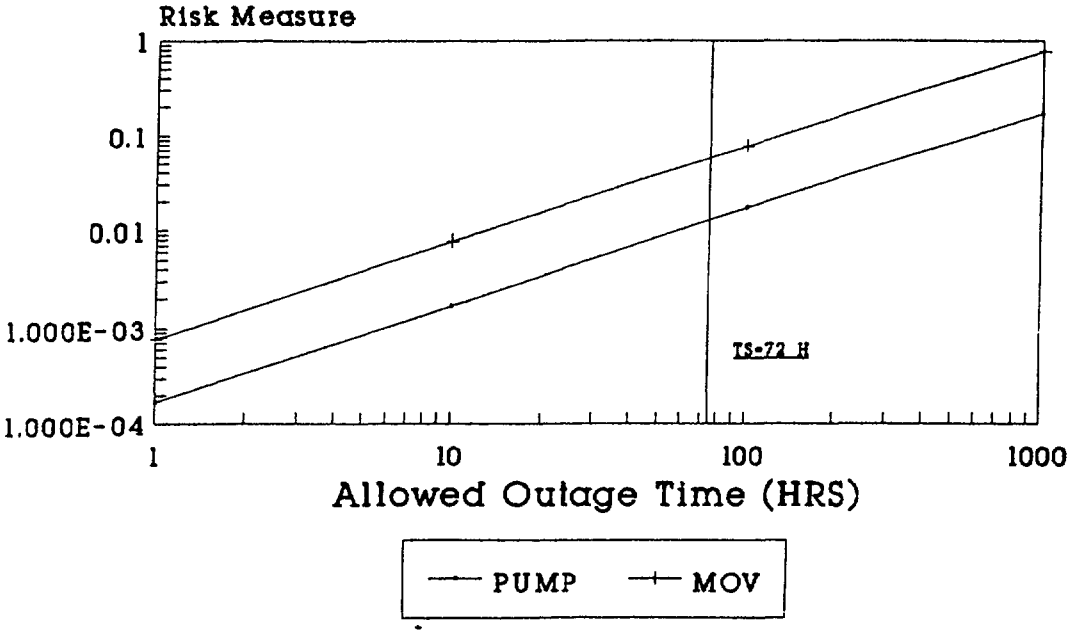


FIG. 5. AOT system level measure for components in HP safety system.

The higher value of the risk measures can be used to identify the reliability assurance activities for these components, checking of other critical components may be required to assure that they are available before repair is begun.

The conclusion from the analysis is, that the success criteria of the system and the AOT risk measure for MOV HD10A1,HD20A1 (0,06) allow their maintenance during power operation (a MOV can be under maintenance). The suggested AOT is 72 h, but the average repair time is only 32 h.

References

1. A. Piirto, T. Mankamo and K. J. Laakso: Development of technical specifications using probabilistic methods, CSNI/UNIPEDE Specialist Meeting, Madrid, Spain 7.-11. 9. 1987
2. P. Baybutt: Case studies on technical specification revision, Battelle Columbus Laboratories, 1. Workshop on Advances in Reliability Analysis and PSA, Hungary 1985
3. H. Nováková: Reliability Analysis of HP safety system of the 1. unit of J. Bohunice NPP. Report VÚPEK, 823-01-02-4/1, 1990 (in Slovak language)
4. J. Mišak: Thermohydraulical analyses for VVER 440 (V 230) units, Report VUJE, 239/1988. (in Slovak language)
5. V. Sopira and Z. Kovács: Reliability Analysis of RPS-I (VVER 440-V 213), Report VÚPEK, 823-01-02-4/2, 1990 (in Slovak language).

RISK BASED OPERATING CONFIGURATION MANAGEMENT

E.R. SCHMIDT, P.J. FULFORD
NUS Corporation,
Gaithersburg, Maryland,
United States of America

Abstract

This paper discusses the development of methods and software as well as experience with the utilization of a PRA for configuration management related activities such as:

1. Planning maintenance activities.

2. Checking, confirming, and justifying allowable outage times and, in the long-term, possibly replacing the license technical specifications.

3. Providing information for development of accident management activities.

The impact of components being out of service for test and maintenance is to increase the core damage frequency (CDF) over that with all components nominally available. This new CDF represents the "instantaneous" CDF for the current configuration.

A number of difficulties arise in providing a technically valid assessment of the current configuration risk in short turn-around times. These include:

- Completeness of modeling
- Conservative treatment of unlikely (non-important) scenarios.
- Ease of updating model for design changes.
- Model size.

Two basic approaches are available to provide the configuration dependent assessment of CDF:

1. Modifying, and then re-solving the event tree/fault tree models to reflect the actual configuration.

2. Modifying and requantifying a core damage Boolean equation to reflect the actual configuration.

A computer program designed around the second approach has been developed. This program, NURISK, allows systems, trains, or components to be taken out of service or restored to service by specification of system, component type or specific component identifying number. Initiator frequency can also be changed to account for such things as switchyard maintenance or RPS testing.

For the new configuration, the core damage equation is minimalized to eliminate non-minimal cutsets and a new CDF calculated. The change in CDF is then used to indicate an allowable outage time. The user can specify the actual outage time and store in a log, the history and cumulative increase in probability of core damage due to test and maintenance activities. Importance measures are calculated and displayed to indicate what can be done to reduce CDF as well as what would cause a further increase in risk. Finally, the core damage scenarios that make up the current status CDF can be displayed.

An Electric utility in the U.S. has begun to use the PRA on its two-unit BWR station as part of its operations and maintenance practices. Maintenance outages of systems and components that are important to safety, as determined by the PRA, are scheduled based on safety considerations. Facility policy, based upon NURISK insights, is to not remove more than one safety-significant component at a time, i.e., related component outages. Additionally, the total planned maintenance outage time for each component is controlled by guidelines established using NURISK. The guidelines limit the total contribution of maintenance outages to core damage frequency to the amount attributed to maintenance in the PRA. Additionally, a limit on the allowable instantaneous risk of core damage frequency is established. The instantaneous core damage frequency is calculated by NURISK. Examples and typical results of the use of the PRA will be presented and discussed.

INTRODUCTION

This paper discusses the development of methods and software as well as experience with the utilization of a PRA for configuration management related activities such as:

1. Planning maintenance activities.

2. Checking, confirming, and justifying allowable outage times and, in the long-term, possibly replacing the license technical specifications.

3. Providing information for development of accident management activities.

Subjects to be addressed include:

- o Risk measures, limits, and other useful information
- o Making information available to plant personnel
- o The NURISK software
- o Utility applications

RISK MEASURES, LIMITS, AND OTHER INFORMATION

The impact of components being out of service for test and maintenance is to increase the core damage frequency (CDF) and consequently the risk over that with all components nominally available. The usual PRA results, such as dominant core damage sequences and the importance of various unavailabilities are based on the annual average unavailabilities due to failures as well as test and maintenance (T&M). The average unavailability is not a true reflection of plant status, at any given point in time,

particularly, with regard to T&M where a system or train is either in T&M or it is not. Risk results based on annual average unavailability are not a good indicator of what is important to risk for actual plant configurations, particularly where multiple components are out of service. A more valid and useful measure is the "instantaneous" CDF for the current configuration. This instantaneous CDF is the CDF if this configuration existed for the entire year. Given that the annual average initiator frequency and component failure rates are applicable at the present time then the instantaneous CDF represents the CDF while in this configuration or CDF_i.

Two types of limits on this would appear to be appropriate. The first would be an absolute limit on the instantaneous value of CDF while the second is a limit on the probability of core damage. The latter translates to an allowable time in the specified configuration (or an allowable outage time, AOT). That is,

CDF_i x AOT = Probability of CD over the AOT

Besides limits on instantaneous CDF, a limit on cumulative impact on CDF over some time period, such as a year, is also appropriate particularly for planning purposes. This is an extension of the current technical specification approach which limits the duration of an outage but not the frequency.

In establishing any one of these limits or goals the limit could be either on the total CDF or on the change in CDF above the no maintenance baseline. While overall goals such as the safety goal policy and the implementing subsidiary guidelines represent total values, a change from the baseline seems more appropriate for judging adequacy of operations. Use of delta's also minimizes the dependence on absolute values of CDF. In any event, at large values of CDF or delta CDF, the two methods approach each other.

Table 1 represents a suggested table of AOT's. This table is based on a maximum increase in probability of core damage for any single configuration of 10^{-6}. This value of 10^{-6} is based on considerations of safety goals and an estimate of the core damage probability due to a forced shutdown because of exceeding the AOT. In reality, the later is a function of plant configuration and increases as the instantaneous CDF increases. This would then yield large AOT's for the larger CDF_i's if it is assumed that the plant should be shutdown only if the increase in risk due to continued operation exceeds that due to the shutdown. This area needs further research.

Table 1

ALLOWABLE OUTAGE TIMES

Change in CDF	AOT
Greater than 10^{-3}	Not Allowed
10^{-3} to 3 x 10^{-4}	8 Hours
3 x 10^{-4} to 10^{-4}	1 Day
10^{-4} to 3 x 10^{-5}	3 Days
3 x 10^{-5} to 10^{-5}	10 Days
10^{-5} to 10^{-6}	30 Days
Less than 10^{-6}	No Limit

Given the establishment of criteria or goals which limit risk (or its surrogate, core damage frequency), the risk of the actual plant configuration must now be compared to the criteria and the results presented for action/information. If AOT's are being established, then there could be a direct calculation of AOT and this presented without any reference to PRA terminology. For purposes of minimizing risk and effective planning, assessing the impact on AOT of other configuration changes such as restoring components to service or testing or starting a standby system should also be possible. A tracking system which provides the cumulative impact on risk could be a significant value in monitoring the effectiveness of outage planning. For accident management, knowledge of the dominant core damage sequences in the actual plant configuration is important.

MAKING INFORMATION AVAILABLE TO PLANT PERSONNEL

To be useful, the kind of information described above must be readily available to the plant personnel. While tables of system, train, or component importance (such as the risk achievement worth) are possible for single items out of service they are not practically possible for multiple outages. A fast response computer model is therefore needed.

A number of difficulties arise in providing a technically valid assessment of the current configuration risk in short turn-around times. These include:

- Completeness of modeling
- Conservative treatment of unlikely (nominally non-important) scenarios.
- Ease of updating model for design changes.
- Model size.

A modern full scope PRA may include consideration of several thousand basic events, including the detailed evaluation of several hundred accident sequences producing a total of over a hundred thousand cutsets. For a given plant status many fewer cutsets would be expected to dominate the CDF. Changing the status by taking one or more systems out for test and maintenance can change the dominant sequences significantly.

An operational support model encompassing the full scope PRA would be very large to allow proper treatment of plant complexity, provide the necessary information to make decisions and to cover a wide range of plant configurations. Such a large model makes it difficult to achieve the goal of having information quickly available to the plant staff.

Two basic approaches are available to provide the configuration dependent assessment of CDF:

1. Modifying, and then re-solving the event tree/fault tree models to reflect the actual configuration.
2. Modifying and requantifying a core damage Boolean equation to reflect the actual configuration.

The first approach, while solving several problems concerning model accuracy, requires a highly simplified and modularized model that may not be easily obtainable from the original PRA. The second approach allows fast response but must account for limitations imposed on core damage equation size and the resulting effects of truncation. These limitations can be minimized by tailoring the core damage equation to the plant design and operational needs and practices.

The above discussion covers the technical aspects of generating the risk information needed for decisions. An equally important, but more straight-forward aspect, is the format for presenting this information so that it can be used effectively be the recipient. This is a function of the activities for which the information is intended. If it is actual AOT determination, then the input/output format should be tailored to the utility and operator normal practices and nomenclature and should make no use of PRA terms. On the other hand, if it is for accident management, then use of PRA terms might be more appropriate. Input/output screen formats are therefore very user and use specific.

THE NURISK SOFTWARE

A computer program designed around the second approach has been developed. This program, NURISK, allows systems, trains, or components to be taken out of service or restored to service by specification of system, component type or specific component identifying number. Initiator frequency can also be changed to account for such things as switchyard maintenance or RPS testing.

For the new configuration, the core damage equation is minimalized to eliminate non-minimal cutsets and a new CDF calculated. The change in CDF is then used to indicate an allowable outage time. The user can specify the actual outage time and store in a log, the history and cumulative increase in probability of core damage due to test and maintenance activities. Importance measures are calculated and displayed to indicate what can be done to reduce CDF as well as what would cause a further increase in risk. Finally, the core damage scenarios that make up the current status CDF can be displayed. Several typical screens are reproduced in Figures 1 and 2.

The core damage equation utilized to calculate change in CDF can be taken directly from the original PRA, however, as indicated previously, size limitations forces truncation values which may eliminate potentially important cutsets. To avoid this problem, a maintenance core damage equation is developed by identifying the various maintenance activities at the plant and then re-solving the PRA model with these test and maintenance basic event probabilities set equal to unity to ensure they will be above the truncation value. The resulting core damage equation is then combined with the normal core damage equation and the result includes cutsets covering maintenance as well as random failures.

Such an operational support model was developed from the PRA for a large BWR. The basic PRA and NURISK model parameters are shown in Table 2.

```
                CURRENT RISK ASSESSMENT (With Redundant Failures Removed)
=========V 1.2 ==========================================NUS Corp. =========
              Factors changed from basis status =    3
          FREQUENCY OF LOSS OF OFFSITE POWER INITIATING EVENT          x   2.000
          DIESEL GENERATOR. 12 IN MAINTENANCE                              OUT
          RHR SERVICE WATER PUMP LEG A IN TEST AND MAINTENANCE             OUT
                 Number of redundant failures removed  =  115
          Basis Core Damage Frequency      = 5.818E-006
          New Core Damage Frequency        = 5.005E-005
          Delta Core Damage Frequency      = 4.423E-005
              RISK FACTOR                  =  8.603
                 Allowable outage time is 3 days
```

```
                    Log History Now?      (Y/N) >
```

```
                CUMULATIVE RISK ASSESSMENT LOG FILE READOUT
=========V 1.2 ==========================================NUS Corp. =========
 Time    Allowable     Time in          Risk        Risk        Cumulative     Events
 Step  Outage Time  Configuration    Factor     Increment   Risk Increment   Aff'd
    1. 7.2000E+001  2.4000E+001  8.6025E+000  1.7692E-007  1.7692E-007        3
      FREQUENCY OF LOSS OF OFFSITE POWER INITIATING EVENT       :Freq x    2.0000
      DIESEL GENERATOR 12 IN MAINTENANCE                        :Out of Service
      RHR SERVICE WATER PUMP LEG A IN TEST AND MAINTENANCE      :Out of Service
```

```
                Press any key for next time step log
```

FIG. 1.

```
                        PLANT MODEL PARAMETERS
=========V 1.2 ==========================================NUS Corp. =========

          Number of items in plant model      =   44512

          Number of cut sets in plant model   =    6754

          Number of basic events in data      =     412

          Number of basic events utilized     =     412

          BASIS CORE DAMAGE FREQUENCY         = 5.8178E-006
```

```
                    Press any key to return to menu
```

```
                The  Important Scenarios for the Current Status
=========V 1.2 ==========================================NUS Corp. =========
  RANK  PC CONTRIBUTION                  (Risk Factor = 8.603E+000)
    1   80.435    4.026E-005     * SCENARIO *  (4657)
  FAILURE TO RECOVER OSP AT 20HRS/NO RECOVERY AT 10HRS        <NOOSP2010      >
& FREQUENCY OF LOSS OF OFFSITE POWER INITIATING EVENT         <IETE           >
& FAILURE TO RECOVER OSP IN 10 HRS                            <NOOSP10        >
```

```
          PgUp,PgDn,Home      -or-      ESC to return to MENU
```

FIG. 2.

TABLE 2

Model Parameters

Complete PRA	
Basic Events	3,600
Core Damage Sequences	533
Core Damage Cutsets	124,000
Core Damage Frequency (T&M=0)	5.82×10^{-6}/Yr.
NURISK MODEL	
Basic Events	412
Core Damage Cutsets	6,754
Cut-off for cutsets without T&M	5×10^{-11}/Yr
Cut-off for cutsets with T&M Set equal to 1.0	1×10^{-8}/Yr
Core Damage Frequency (T&M =0)	5.36×10^{-6}/Yr

UTILITY APPLICATION

The plant with this PRA has begun to use the PRA as part of its operations and maintenance practices. Maintenance outages of systems and components that are important to safety, as determined by the PRA, are scheduled based on safety considerations. Facility policy, based upon NURISK insights, is to not remove more than one safety-significant component at a time, i.e., related component outages. Additionally, the total planned maintenance outage time for each component is controlled by guidelines established using NURISK. The guidelines limit the total contribution of maintenance outages to core damage frequency to the amount attributed to maintenance in the PRA. Additionally, a limit on the allowable instantaneous risk of core damage frequency is established. The instantaneous core damage frequency is calculated by NURISK.

Figures 3 and 4 show the results of using the guidelines since returning from a refueling outage in May of 1988. The values shown by each system outage on Figure 4 are the instantaneous CDF and in parentheses the outage duration and the percent of annual goal.

An example use of the NURISK generated guidelines in the operational decision-making process occurred due to a binding discharge valve on the A RHR heat exchanger. A decision had to be made whether to repair the valve while continuing to operate both units at full power or to defer the maintenance to a schedule unit outage. To repair the valve required isolating the line from two RHR service water pumps and two emergency service water pumps that share a common discharge line. The instantaneous risk of entering the configuration necessary to repair the valve influenced the decision to delay the repair to the first scheduled unit outage, while assuring the current situation of cracking open the valve was acceptable.

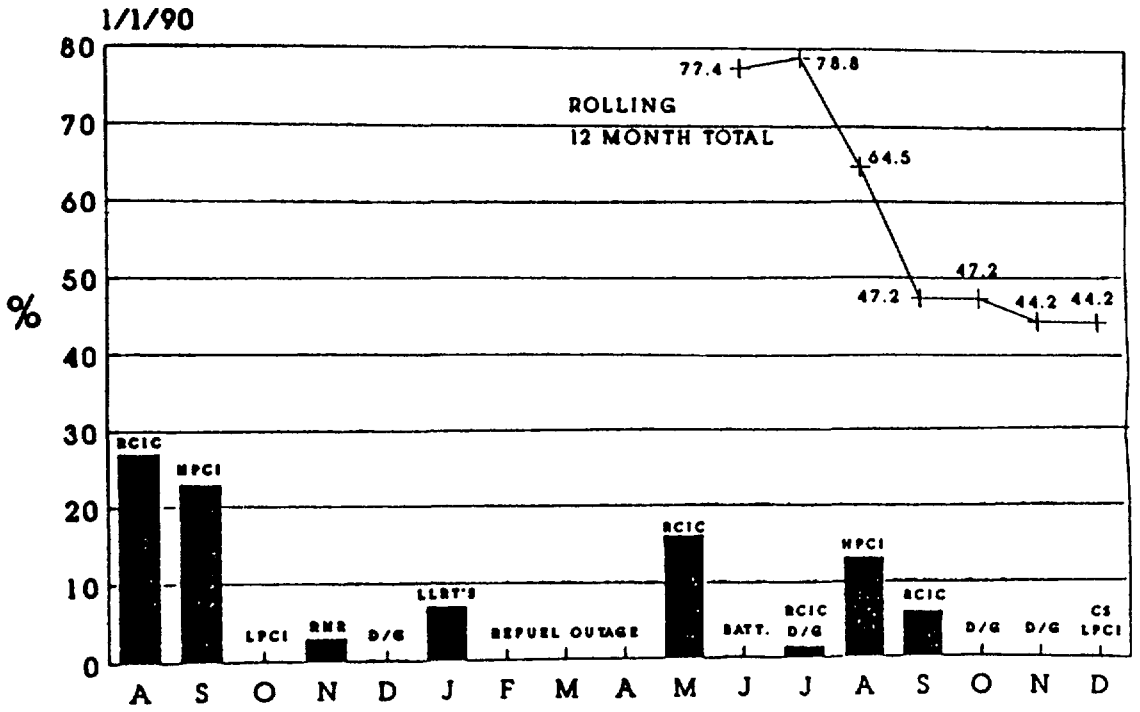


FIG. 3. Percentage of acceptable core damage frequency due to system unavailability.

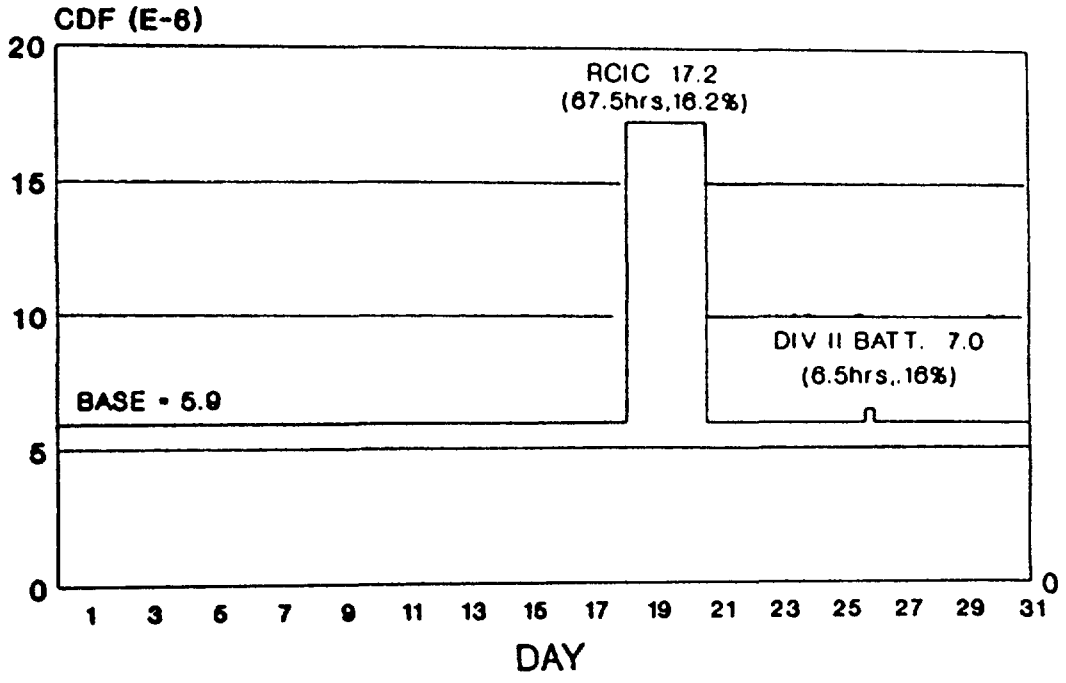


FIG. 4. System unavailabilities (May 1989).

LIST OF PARTICIPANTS

B. Atefi (chairman)	SAIC 1710 Goodridge Drive McLean, Virginia 22101 United States of America
M. Borysiewicz	Institute of Atomic Energy Dept. of Nucl. Safety Analysis 05-400 Otwock-Swierk Poland
P.C. De Gelder	Vincotte Avenue de Roi, 157 B-1060 Brussels Belgium
B. Th. Eendebak	N.V. KEMA Utrechtseweg 310 P.O. Box 9035 Arnhem Netherlands
I.V. Fedik	Zheleznodorozhnaya 24, Podolsk, Moscow Region, 142100 Union of Soviet Socialist Republics
A.E. Galindo	Comision Federal de Electricidad Laguna Verde NPP, Rio Atoyac 97, Piso 11 Col. Cuauhtemoc C.P. 06598 Mexico
M. Gonzales Cuesta	Instituto de Investigaciones Electricas Apartado Postal 475 62000 Cuernavaca, Mor., Mexico
A.C. Hall	Council for Nuclear Safety P.O. box 7106 Hennopsmeer 0046, South Africa
R.E. Häusermann	Kernkraftwerk Leibstadt AG CH-4353 Leibstadt, Switzerland

K. Hioki	O-Arai Engineering Center, Power Reactor and Nuclear Fuel Development Corporation 4002 Narita, O-Arai, Ibaraki-ken, 311-13 Japan
E. Holló	Inst. for Electrical Power Research Zrinyi u.1. H-1051 Budapest Hungary
J. Holy	Nuclear Research Institute 250 68 Rez near Prague, Czechoslovakia
J.M. Hopwood	AECL CANDU Sheridan Park Research Community Mississauga, Ontario, L5K 162 Canada
B.E. Horne	Nuclear Electric plc Barnett Way, Barnwood, Gloucester GL4 7RS United Kingdom
M. Kosonen	Teollisuuden Voima Oy 27160 Olkiluoto, Finland
Z. Kovács	VUPEK Bajkalská 27, 827 52 Bratislava, Czechoslovakia
M.J. Kulig	Central Laboratory for Radiological Protection U1. Konwaliowa 7, 03-194 Warsaw, Poland
K.J. Laakso	Technical Research Centre of Finland, Laboratory of Electrical Engineering and Automation Technology SF-02150 Espoo, Finland
P.N. Lawrence	Ontario Hydro 700 University Avenue, A8-A15 Toronto, Ontario, M5G 1X6, Canada

R.I. Lounsbury	ECL Research Chalk River Nuclear Laboratories Chalk River, Ontario, KOJ IPO, Canada
R. Lobel	Technical Specifications Branch Office of Nuclear Reactor Regulation USNRC, 11E22 Washington, D.C. 20555 United States of America
G.Yu. Loskutov	Research and Development Institute of Power Engineering 101000, Box 788, Moscow, Union of Soviet Socialist Republics
T.V. Mankamo	Avaplan Oy Kuunsade 2 DE SF-02210 Espoo, Finland
S. Martorell	Polytechnic University of Valencia Dpto. Ingeniera Quimica y Nuclear Universidad Politecnica de Valencia P.O. Box 22012 46071 Valencia, Spain
E. Mink	Westinghouse Energy Systems International Rue de Stalle, 73 1180 Brussels, Belgium
P.D. Rawson	Isograph Ltd. 22 Lloyd St. Manchester, M25WL, United Kingdom
A.N. Roumiantsev	I.V. Kurchatov Institute of Atomic Energy 123182, Moscow, D-182 Kurchatov's Square Union of Soviet Socialist Republics

J. Rumpf	Staatliches Amt für Atomsicherheit und Strahlenschutz Waldowallee 117 Berlin 1157 Germany
W.B. Sargeant	Nuclear Electric PWR Project Group Booths Hall Chelford Road Knutsford, Cheshire WA16 8QG United Kingdom
C.H. Shepherd	Nuclear Installations Inspectorate St. Peters House Balliol Road, Bootle Merseyside L20 3LZ United Kingdom
J.P. Sursock	Manager, Safety Performance Program Nuclear Power Division Electric Power Research Institute (EPRI) 3412 Hillview Avenue P.O. Box 10412 Palo Alto, CA 94303 United States of America
K. Theiss	Technischer Ueberwachungsverein Norddeutschland e.V. Postfach 540220 2000 Hamburg 54 Germany
E.P. Tirri	Imatran Voima Oy P.O. Box 112 01601 Vantaa Finland
D. True	ERIN Engineering and Research 2175 California Boulevard, Ste. 625 Walnut Creek, CA 94596 United States of America

G. Verdu Martin	Politechnic University of Valencia Dpto. Ingenieria Quimica y nuclear Universidad Politecnica de Valencia P.O. Box 22012 46071 Valencia Spain
V. Volkov	VNIIAES All-Union Research Institute for Nuclear Power Plant Operation 25, Ferganskaya Ul, 109507 Moscow Union of Soviet Socialist Republics
S.O. Volkovitskij	Science and Engineering Center for Safety in Industry and Nuclear Power (SECSINP) USSR State Committee for Supervision of Safety in Industry and Nuclear Power (SCSSINP) Taganskaya St., 34 109147, Moscow Union of Soviet Socialist Republics
A. Wild	Wild and Boyd Advisors 8 Oberon Street Nepean, Ontario K2H 7X7 Canada

IAEA Participants

S. Hirschberg, Division of Nuclear Safety
L. Lederman, (Scientific Secretary), Division of Nuclear Safety
F. Niehaus, Division of Nuclear Safety
B. Tomic, Division of Nuclear Safety
H. Vallerga, Division of Nuclear Safety

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
CZECHOSLOVAKIA	S.N.T.L., Mikulandska 4, CS-116 86 Prague 1 Alfa, Publishers, Hurbanovo námestie 3, CS-815 89 Bratislava
FRANCE	Office International de Documentation et Librairie, 48, rue Gay-Lussac, F-75240 Paris Cedex 05
HUNGARY	Kultura, Hungarian Foreign Trading Company, P.O. Box 149, H-1389 Budapest 62
INDIA	Oxford Book and Stationery Co., 17, Park Street, Calcutta-700 016 Oxford Book and Stationery Co., Scindia House, New Delhi-110 001
ISRAEL	Heiliger & Co. Ltd. 23 Keren Hayesod Street, Jerusalem 94188
ITALY	Libreria Scientifica, Dott. Lucio de Biasio "aeiou", Via Meravigli 16, I-20123 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-Ruch, Centrala Handlu Zagranicznego, Krakowskie Przedmiescie 7, PL-00-068 Warsaw
ROMANIA	Ilexim, P O. Box 136-137, Bucharest
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
USSR	Mezhdunarodnaya Kniga, Smolenskaya-Sennaya 32-34, Moscow G-200
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