IAEA-TECDOC-751

PSA for the shutdown mode for nuclear power plants

Proceedings of a Technical Committee meeting held in Stockholm, 30 November–3 December 1992

IAEA

June 1994

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

The originating Section of this document in the IAEA was:

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

PSA FOR THE SHUTDOWN MODE FOR NUCLEAR POWER PLANTS

IAEA, VIENNA, 1994
IAEA-TECDOC-751
ISSN 1011–4289

Printed by the IAEA in Austria
June 1994

FOREWORD

Mindful of risks that exist during low power operation and shutdown mode, many NPP operating organizations initiated studies to estimate these risks and to determine the improvements needed. The objectives and scope as well as the methods used in these studies vary significantly. However, most of the studies clearly showed that the risk related to the shutdown state at an NPP is of the same order of magnitude as the risk related to full power operation. The results of these studies also prompted improvements in both procedures and equipment design to reduce the risk in shutdown.

In order to discuss and exchange experience on different aspects of methods associated with estimating risks of shutdown and low power operation, the IAEA held a Technical Committee Meeting on Modelling of Accident Sequences during Shutdown and Low Power Conditions in Stockholm, Sweden, in December 1992. The meeting, which was attended by more than 75 participants from 20 countries, provided a broad discussion forum where all the currently active major shutdown PSA programmes were reviewed. The meeting also addressed the issues related to actual performance of shutdown PSA studies as well as insight gained from the studies.

This document, which was prepared during the TCM, contains the results of extensive discussions which were held in specific working groups. The papers presented at the meeting provide a comprehensive overview of the state of the art of shutdown risk assessment and remedial measures taken to reduce the risk in outages. It is hoped that this document will be very useful to all individuals with interest in increasing safety during outages at NPPs.

EDITORIAL NOTE

In preparing this document for press, staff of the IAEA have made up the pages from the original manuscripts as submitted by the authors. The views expressed do not necessarily reflect those of the governments of the nominating Member States or of the nominating organizations.

Throughout the text names of Member States are retained as they were when the text was compiled.

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

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

The authors are responsible for having obtained the necessary permission for the IAEA to reproduce, translate or use material from sources already protected by copyrights.

CONTENTS

1. INTRODUCTION

The results of several PSA studies on modelling shutdown and low power operation for NPPs showed that, in some cases, risk is comparable with that associated with full power operation. Some of the studies employed a full scope PSA modelling. Others limited their scope and utilized abbreviated methods such as barrier analysis. A variety of developments in the area and strong interest by a number of countries to utilize risk based approaches to improve safety in the shutdown state indicated a need for an international discussion forum on the topic.

The IAEA Technical Committee Meeting on Modelling of Accident Sequences during Shutdown and Low Power Conditions, held from 30 November to 3 December 1992, was attended by 75 participants from 19 countries. A total of 16 papers were presented on the following low power and shutdown (LPS) topics: analytical methods, results of analyses, events, lessons learned, risk management, and administrative and licensing controls.

This report summarizes the discussions held during the meeting. The scope and objective of shutdown risk studies and the methods and insights gained from the studies are discussed. All papers presented at the meeting are included.

2. STATUS OF SHUTDOWN RISK ASSESSMENT

The status of shutdown risk assessment, including its application and related areas, is summarized on the basis of the plenary discussion, opening and closing remarks and comments on individual presentations.

In Sweden the need was recognized for a more complete PSA model, including provisions for uncertainties, for low power and shutdown (LPS) conditions. Sweden's 12 nuclear units have PSAs which were developed with the same code (Risk Spectrum). This results in excellent communication in the PSA area between the licensees and the regulatory body.

Human errors need to be quantified in full power PSAs as well as for shutdown risk assessment. The importance of human errors seems to be higher in shutdown conditions.

Questions on the use of simulators for low power and shutdown conditions stimulated some insights. The committee members considered that computer models could accurately simulate LPS conditions and that these models should be implemented on plant specific operating simulators to train operators. LPS procedures and other administrative controls could and should be tested and refined on the operating simulators. (One country has separate manuals for LPS conditions.) Training on LPS conditions needs to go beyond operators to other plant personnel, especially maintenance personnel. It was also noted that simulator training was a valuable source of human reliability data. Such data could address operator related initiating events as well as operator related exacerbating events. Such errors could be errors of either commission or omission.

The need to train operators in the fundamental technical concepts (thermal-hydraulic, etc.) encountered during LPS conditions was highlighted. The emphasis is that this training has to be performed outside the control room environment.

Another highlight centred on plant management and personnel culture. Management should have an awareness of LPS risk and should emphasize the need to manage this risk to plant personnel. Otherwise, plant personnel could have a false impression that there is little or no risk during LPS conditions. If risk awareness is relaxed the risk could increase (as was confirmed by several incidents). In the same area, personnel, especially on plant shift turnover, should have a questioning attitude. Plant indicators which are designed for power operations may be inadequate for LPS conditions. Therefore, personnel should verify actual plant conditions at changing of shifts. This

verification may require observation outside the control room. One Member State has been using PSA including LPS PSA in its regulatory process for some time. This process resulted in gainful experience.

A number of representatives indicated a desire to implement methods to determine 'real-time' risk and configuration evaluation and management. They discussed the use of computer based tools or hard copy tools until computer based tools could be developed and implemented. The hard copy methods used a 'Master Plant Logic Diagram', a graphical form to represent support and supported systems and components. These tools are LPS safety planning tools.

There was considerable discussion on data collection and application. One comment was that equipment failure rates during power operations were likely to be the same as for LPS conditions. Some representatives stated that they used generic data because plant specific data were not available. A comment was made that some plants actually had plant specific data but were not anxious to report it. A counter argument was that some plants may actually have the data but many others do not. In particular, early data for older plants did not exist. A realistic comment was that many if not most plants need to start to identify and gather required data now in order to have useful LPS data. In a related comment, it was pointed out that the IAEA is currently working to establish guidelines for development and collection of plant specific data for PSA application. Such data would be for both power operation and LPS.

Interesting discussion was centred on the French reactivity addition scenario from injection of a slug of unborated water into the reactor core. The French feel that such a scenario is an important issue and have taken positive steps to reduce its probability of occurrence. The immediate action includes temporary plant modifications to preclude the scenario. Longer term efforts which are under way include developing mockups in order to determine more accurately and measure the physical processes and calculate the results.

3. IMPLEMENTATION OF SHUTDOWN PSA STUDIES

3.1. OBJECTIVES OF LPS PSAs

The following are the typical objectives of LPS PSA:

- to find specific plant vulnerabilities in this mode of operation and assess the risk impact of proposed improvements or changes in the evaluated configurations;
- to assess and provide feedback on outage management and maintenance planning;
- to make recommendations on improvements to accident procedures, maintenance and operating procedures.

3.2. PRECONDITIONS TO START LPS PSAs

- A Level 1 PSA possibly including external events and common cause initiators with system analysis and system fault trees for internal initiators should have been completed;
- A capability for thermohydraulic analysis should be available.

3.3. SCOPE AND METHODOLOGY

One of the most important insights from the LPS PSA analyses performed to date is the expectation that in most cases a plant specific model, analysis and data will be required to capture the essence of the shutdown risk. This is due to the fact that technical specifications for refuelling outage,

and accident procedures and management practices vary widely from otherwise similarly designed plants. Furthermore, analyses or redundancy configurations of safety relevant systems during a refuelling outage have shown that a plant can have as many as 10 to 15 distinct redundancy configurations during a single outage, and as many as 30 to 50 distinct redundancy configurations during outages overall, i.e. when evaluated and compared for all outages. The distinction between these redundant configurations must consider the availability of major water sources, such as the suppression pool, the refuelling water storage tank, or the condensate storage tank. It is therefore easy to see that the attempt to analyse each of these unique configurations could result in a very large LPS PSA. Fortunately, it is usually possible to identify a few controlling configurations by careful qualitative comparison of all the configurations. These controlling configurations should be analysed by separate quantitative models. To determine these controlling configurations, the following aspects should be considered:

(a) plant specific technical specifications, procedures and normal practices for shutdown planning;
(b) time spent in each configuration;
(c) decay heat and other physical considerations;
(d) applicability of generic insights for the type of NPP (PWR, BWR, etc.);
(e) operating experience with specific plants and plants of the same type of plant.

For these reasons, a phased approach for an LPS PSA is indicated, where in a first, qualitative evaluation phase all the unique redundancy configurations are identified and compared to determine the controlling configurations, and to document how each of the other configurations are enveloped from a risk perspective by one of the controlling configurations.

In the second, quantitative phase the risk from the controlling configurations is then determined by a PSA model tailored to each configuration by combining it with the initiating events appropriate for the configuration. This may still be a sizeable effort, but more manageable than if undertaken without screening out the non-controlling configurations.

3.4. MANAGEMENT OF LPS PSAs

Given the plant specific nature of most LPS PSA analyses, the unique compounding effect of multiple redundancy configurations, it is advisable for each LPS PSA project to develop a management plan as its first major task:

- It is recommended to establish a group to discuss and implement the results, otherwise the results may stay in the archives. The group must have the authority to make decisions. It is recommended that plant personnel experienced in plant operations and shutdown planning, etc., be involved.

- The major benefit obtained from the development of such a management plan is that the implementation of the entire project must be thought through and laid out with any unresolved issues identified before other activities can begin. It helps to identify how the available 'in-house' expertise and staff can accomplish the project and whether any external support is needed. This is particularly important, since a LPS PSA requires a significant level of direct support from the plant operation, maintenance and outage planning and management staff.

- It must be realized that the LPS PSA can result in backfitting recommendations. This must fit in with the master management plans.

3.5. TOPICS TO BE DISCUSSED BEFORE THE PROJECT STARTS

(a) Fire and flood

During shutdown, the risk of fire will undoubtedly be greater than during operation since more personnel and more possible fire sources are in play. Aspects of fire protection will, necessarily, be

different. Flood risk and its consequences during shutdown may also be significantly different from that during operation.

(b) Data acquisition

Currently data obtained from full power operation are adapted for use in shutdown PSA. In some cases, data are not directly applicable and in other cases components are used only during shutdown. There is a lack of advice and agreement on the needs for and methods of acquiring data suitable for use in shutdown PSA. In particular, during the shutdown and low power phase, human involvement is much greater and therefore human reliability becomes more important.

(c) Consequence analysis

In addition to nuclear safety, it is felt that a range of other consequences should be considered; for example, events leading to radiation injury, equipment damage, boiling in reactor vessel, extended outages or public concern.

There are several Level 2 and 3 considerations, which may be considered important in addressing shutdown risks. These are:

1. Identify the containment status in redundancy configurations;
2. Include the containment safety systems in the LPS PSA model;
3. Define shutdown plant damage states including failure of containment isolation and other safeguard systems and quantify their frequency;
4. Define shutdown release categories;
5. Quantify the frequency of each shutdown release category;
6. Determine the source terms associated with each shutdown release category;
7. Determine the consequences resulting from each shutdown release category.

Of these seven Level 2 and 3 issues, only item 1 is requested to be included in the scope of LPS PSAs. The need to perform subsequent steps depends on the objectives of the study and the choice of safety criteria or goals (if any).

(d) Periodic testing

During testing, some systems and components may require to be taken out of service for a period and this factor should be allowed for in the PSA. Testing, in its own right, can introduce failures and this aspect may be important enough to be included in the shutdown PSA as well as the full power PSA.

4. SCOPE OF COMPLETED STUDIES

The results of several shutdown PSA (LPS PSA) studies were presented at this meeting. These studies show a substantial variation in the level of detail and scope. They show that currently no agreement exists on the scope of an LPS PSA, and that the differences are a result of the plant specific aspects as well as the intended purpose, ranging from a scoping evaluation to more definitive assessments. Among the studies presented TVO I/II and Paluel appear to present the most complete assessments. The other assessments incorporate assumptions to simplify the analysis that may be justified by future work. Two important LPS PSAs with preliminary results were not represented at the meeting, namely those sponsored by the USNRC for the Surry PWR at Brookhaven National Laboratory and for the Grand Gulf BWR Mark 6 at the Sandia National Laboratory. Even at the screening phase these two studies employ much larger LPS PSA models (180 event trees for Surry and 600 event trees for Grand Gulf) than any of the studies presented at this meeting. An important question to be resolved is whether such large models are necessary to truly represent the shutdown

risk. While one such detailed study for each plant type may be warranted, it is hoped that simpler well designed studies can capture the essential insights and plant specific features of the shutdown risk at individual plants.

There is a consensus that for PWRs, midloop operation presents a shutdown configuration with an important contribution to the shutdown risk. The insights gained from the TVO I/II LPS PSA underscore the importance of a plant specific evaluation. The conclusion that most of the shutdown risk stems from LOCAs below the core elevation is entirely due to plant specific design features which are only found in a few plants. Such insights are likely to be missed in a generic study of a more common design. The French PWRs appear to be the only group with a fully uniform design, operating and shutdown practices to warrant consideration of a generic LPS PSA. Even in this case an effort to identify plant to plant differences, for example in the handling of unscheduled long outages, should be made before a generic LPS PSA is claimed to adequately represent all plants in the group.

In Table I, several aspects of these studies are presented. It can be seen that the great differences among their scopes, initiating events considered, etc., vary from the focused to the full-scope analysis. It must be taken into account that the Forsmark 2 study is not a PSA but it is also included as a comparison with the other studies. The Brunswick study was a pioneer study in the shutdown risk assessment and was mainly focused on the loss of DHR.

In Table I the scope of the studies (with their restrictions, if any); the initiating events considered; the plant response (in the sense of physical calculations); the mission time considered to evaluate the sequences; the assumptions made about the availability of the systems that take part in the sequences; the data used, in the double aspect of hardware failure and human reliability; and, finally, the uncertainty and sensitivity assessments developed are presented.

5. INSIGHTS GAINED FROM SELECTED STUDIES

This section deals with the experience obtained from different low power mode PSA studies. The insights discussed concern only light water reactor plants. The studies and the respective reactors are:

BWR: TVO, Finland;
Forsmark 2, Sweden (qualitative study);
Grand Gulf, USA (NRC reference plant).

PWR: Surry, USA (NRC reference plant);
Paluel, France;
Tihange 3/Doel 2, Belgium;

The insights are presented in the form of the reactor type (BWR, PWR), specific insights and general insights.

5.1. GENERIC FINDINGS APPLICABLE TO ALL LWRs

1. The scope of a study should consider containment status at core damage. Shutdown risk can be defined as fuel damage frequency (FDF) (Level 1 PSA), release magnitude and frequency (Level 2 PSA), or population risk (Level 3 PSA).

2. Frequency of unplanned outages as far as their contribution can be forecast should be considered as a contribution to the different plant operating states (POSs) per year.

3. Transitions between POSs may have to be further studied.

TABLE I. SCOPE OF SELECTED LPS STUDIES

SCOPE	TVO	BRUNSWICK	FORSMARK 2	GRAND GULF
PSA level	Level 1 including external events	(Level 1)	N/A (barrier analysis)	Level 3 (intended) including external events (at the moment)
Restrictions	LOOP excluded	Only loss of RHR	Only predefined events	No restrictions
Initial conditions	Refuelling Q < 8%	-	Refuelling	Q < 15% Any condition
End state	Fuel damage in vessel	Core damage	Fuel damage in vessel	Level 1: Fuel damage in vessel Level 3: Any impact on environment
Initiating events	LOCA above core top LOCA below core top Loss of RHR	Loss of RHR	MCP overhaul CRD overhaul Cold pressurization Refuelling Testing and inspection	Transients LOCAs DHR challenge Special events Hazard events
Plant response	Hand calculations MAAP	-	-	Hand calculations MELCOR
Mission time	20 hours	-	-	-
Assumptions	Technical specifications Working list Automatic actions cut off	-	Technical specifications Working list Automatic actions cut off	-

TABLE I. (cont.)

SCOPE	TVO	BRUNSWICK	FORSMARK 2	GRAND GULF
Systems analysis	Based on full power fault trees Credit for non-safety-related systems	–	–	Fuel power fault trees Changing: Human actions and maintenance unavailability
Data				
Hardware failure	Same as full power (T-book)	–	–	Same as full power (ASEP database)
Human action	Before the accident: screening values As initiating event: screening values, some detailed analysis After initiating event: time reliability curves were assigned	Core damage	Fuel damage in vessel	Level 1: Fuel damage in vessel Level 3: Any impact on environment

4. Outage type strongly influence the shutdown risk.

5. Plant specific outage practices influence the characterization of POSs during low power and shutdown operation.

6. The identification of initiating and other safety relevant events requires a systematic approach, including interviews with the plant personnel, in order to cover the whole range of human performance. The following data sources can be used as a starting point:

- power mode PSA;
- generic initiator list of the reactor type;
- operating experience;
- other plant experience;
- outage programmes;
- technical specifications;
- shutdown procedures;
- accident procedures.

7. Methods such as FMEA and HAZOP should be considered to ensure that all important initiating events have been identified.

8. The scheduled maintenance significantly increases the unavailability of safety systems during shutdown. Non-safety-related systems, such as pool cooling or fire water systems, can be used and their role can be important in a shutdown.

9. Typical adjustments made to PSA fault trees in order to develop fault trees applicable to shutdown conditions were:

- fewer automated system actuations/more manual actuations;
- different system initial state, different failure modes;
- maintenance unavailabilities;
- system success/failure criteria, if necessary;
- different support states.

10. Additional supporting thermal-hydraulic analyses may be needed for more detailed odelling of some accident scenarios and to relax conservative assumptions existing in current models.

11. The dominant contributor to core damage frequency as an initiator or a mitigator of the accidents sequences is operator failure.

12. There is uncertainty in the human error probabilities currently used in PSA. Additional research is needed in the field.

13. Additional procedures for accidents during shutdown conditions, better training and more reliable instrumentation would be beneficial to ensure that utility staff are better able to respond to shutdown accidents. It was recognized that very few procedures are currently available for accidents during shutdown. In most cases, the information on the procedures for power operation can be helpful if applied to shutdown accidents. However, some procedures written with power operation in mind may misguide an operator.

14. The following unique aspects of low power and shutdown operation that affect human reliability analysis (HRA) methods were identified:

- human errors as a significant contributor to initiating event frequency;
- less explicit safety criteria, e.g. coverage of technical specifications and administrative controls;

- incomplete coverage of procedures;
- more dependence on human action;
- in many cases longer operator response time;
- in specific cases extremely short response time;
- insufficient simulator and other training;
- increased and heterogeneous site population;
- certain recovery actions that significantly reduce risk and which should be incorporated into procedures.

15. Technical specifications for shutdown conditions need to be expanded. These should address multiple unavailabilities.

16. Preliminary shutdown PSA results indicate that the off-site releases in the event of core damage during shutdown are comparable to those at full power.

17. For plants with bunkered emergency systems: spurious activation of the bunkered system has to be considered in shutdown PSA.

18. The containment equipment hatch is very important with respect to accident mitigation and large releases.

19. The mission times are extremely accident sequence specific.

5.2. INSIGHTS FOR BWR PLANTS

5.2.1. Generic findings for BWR plants

1. Strict, defined limitations of studies, e.g. power level, primary pressure.

2. Status of the safety and relief valves and the potential for cold overpressure in the filling of reactor at the end of a shutdown sequence.

3. Pool cooling system, fire water system and makeup water system are usually available and can be used to mitigate accident sequences. However, these systems have no safety related requirements.

4. The studies do not normally assume that any water will be supplied from the condenser in shutdown conditions, which may be too conservative an assumption.

5. BWR insights concerning human actions:

- historical data are the first and preferred human reliability data;
- simulator availability in low power states is usually very limited;
- each action requires plant specific evaluation and no generic data should be used.

6. PSA data for power operation are also valid for low power modes unless major differences in operating conditions exist.

7. In TVO and other ABB type reactors the pool chemistry and cooling systems are not safety classified which may also be the situation in other BWRs.

8. In some cases, a simplistic approach was found to be useful in introducing PSA methods, e.g. a barrier analyses.

5.2.2. Specific insights for BWR plants

TVO

Loss of external electrical supply and external events such as fires and floods were excluded from the study. The power levels considered were <8% of nominal. The scope of the study covered mainly the refuelling outages of PSA Level 1.

The main damage state is fuel damage in the vessel and pools. Less severe consequences, e.g. local criticality, cold pressurization of the vessel and major economic loss were also considered. A typical economical loss would be that caused by a crane accident to a unique component for example.

The TVO study distinguished 6 plants operational state depending on the decay heat level and the possibilities of removing it from the core and pools.

TVO used the following sources to identify the initiating events:

- power operation PSA;
- published other low power PSAs;
- NRC list of initiators;
- systematic interviewing techniques;
- incident reports from ABB plants.

Three emergency procedures for the shutdown state existed before the study. They were: large bottom leakage from the main circulation pump penetration; loss of residual heat removal (RHR); and loss of the pool cooling system.

The mission took 20 hours. However, TVO took into account scenarios leading to a core melt up to three days later.

The system scheduled maintenance unavailability, as a significant cause of unavailability, was assessed from the basis of plant technical specifications and scheduled maintenance lists. The unavailabilities were assessed for different plant operational states. Nearly all the automated system actuations were cut off for the refuelling state.

The same data from the Nordic reliability data book (T-book) were used for hardware reliability calculations and power operation.

Thorough qualitative analysis was always the basis of the values used for human actions before an initiating event and as initiating events. However, coarse screening values were used in a systematic way throughout the study. Figures used range between $1 \times 10^{-3} - 1 \times 10^{-2}$. Above these values historical data were utilized. For a couple of very well analysed errors a value of 1×10^{-3} could be used as the error had immediate consequences and was hazardous to workers.

Recovery values range from 0.1 to 0.5, if no specific tests or alarms existed. However, in the case of an initiating event, and were analysed as such, recovery possibilities are extremely sequence related. For recovery from spurious openings of manually operated valves, a more general framework was utilized.

Human errors after an initiating event were considered separately, depending on the action and the time available. Action specific time– reliability curves were drawn based on analysis.

The human reliability study also included special modelling of maintenance task interaction (interaction matrix), barrier diagrams to screen important tasks and chronological phase diagrams for sequences other than those leading to severe core damage.

The TVO study also included an uncertainty and sensitivity phase. A qualitative uncertainty assessment was used at the beginning which focused upon the methods and decisions made in the course of the study. Sensitivity analysis showed again that the results are very sensitive to human reliability estimates. The analysis led to the following actions which significantly reduced the core damage frequency:

- guards were placed at the equipment hatch during the MCP overhaul critical phases;
- the use of piston pumps was prohibited;
- safety valve capping was given up;
- a mechanical cotter pin was installed into an MCP plug.

To reduce the probability of unwanted local criticality, the inspection routines of control rods were changed. Procedural changes and training on the critical events identified will be introduced.

Forsmark 2

A limited study consisted of some predefined events (MCP overhaul, cold pressurization, refuelling, control rod drive overhaul, testing and inspections). Cold shutdown and refuelling states were considered.

The analysis was not a PSA but a barrier analysis prestudy. Fuel damage and less severe damage states, e.g. local criticality, were considered.

The analysis led to the following actions:

- closing of the equipment hatch under the MCP overhaul;
- use of low pressure pumps only in the filling of the vessel;
- installation of a mechanical cotter pin to the MCP plug;
- commencement of procedures and training on the events identified.

Grand Gulf

The study is the NRC reference study with no major restrictions; external events were included. The power level considered is $< 15\%$ of nominal. The study intends to extend to PSA Level 3. The only consequence considered is fuel damage in the vessel. The study includes 7 studied plant operating states.

The initiating events were identified by using the technique created by BNL for the Surry PWR. The MELCOR code was used for thermohydraulic calculations together with some hand calculations. Performance of plant operating staff was included in the study using full power mode procedures as a basis for low power event trees and discussions with personnel.

The system models used were full power fault trees. They were modified to comply with the different conditions of shutdown.

The human reliability data were twofold: the generic initial screening data and final estimations from A.D. Swain's document (NUREG-1278). The hardware data were taken from the updated accident sequence evaluation programme databank.

The analysis is still in progress.

5.3. INSIGHTS FOR PWR PLANTS

5.3.1. Generic findings for PWR plants

1. Dilution accidents should be investigated in all POSs. Boron dilution during midloop operation and 'fast dilution' accidents at hot standby are important risk contributors.

2. Isolation of RCS loops should be avoided during midloop operation as it could be an important contributor to risk.

3. Core damage frequency (CDF) during midloop operations is comparable to power operation CDF.

4. Loss of residual heat removal (RHR) with the RCS in reduced inventory conditions is also a dominant contributor to risk.

5. Once boiling has occurred, the containment may become uninhabitable and the equipment hatch may become difficult to close.

5.3.2. Specific insights for PWR plants

Surry

The study is a Level 3 PSA including internal events, internal fires and floods, and seismic hazards. Currently the Level 1 internal event study is almost complete. Only detailed analysis of midloop operation POS is missing. Point estimates of core damage frequency will soon be available. An uncertainty analysis will follow.

The plant configuration changes continuously in any outage. There are four different types of outages (refuelling, drained maintenance, non-drained maintenance with use of the RHR system, and non-drained maintenance without the RHR system). A shutdown PSA requires the definition of at least three midloop POSs. In these POSs the RCS level is lowered to the mid-plane of the hot leg. The three POSs used in the analysis are:

- midloop operation that takes place early in the refuelling outage (allows fast draining of the RCS loops to permit eddy current testing of the SG tubes);

- midloop operation after refuelling is completed to allow additional maintenance of equipment in the RCS loops;

- midloop operation in which maintenance activity requires midloop conditions. This POS is characterized by the highest decay heat level among the 3 POSs analysed.

The last POS was found to be the most important risk contributor. The characteristics of this POS are high decay heat removal and the relatively short time available for operator action. This result shows that it is preferable to enter midloop conditions when decay heat is relatively low (entering midloop as early as one day after shutdown should be avoided). Before this study was completed, the utility changed its previous outage practice which is expected drastically to reduce the time in midloop configuration.

The MELCOR computer code was used to assess whether or not gravity feed from the RWST could be used to provide longterm cooling (i.e. 24 hr decay heat removal). It was found to be sufficient only when the decay heat is relatively low. However, it can provide a margin of a few hours for restoring other means of decay heat removal when the decay heat is high.

It was found that the use of checklists reduces the impact of component maintenance unavailability. The technical specifications should take account of what happens across different systems in addition to within the systems.

The water level instrumentation used during midloop operation, i.e. standpipe level instrumentation and ultrasonic level instrumentation, have limited applicability during an accident. The standpipe system provides a correct level indication only when there is no pressure buildup in the

system. The ultrasonic level instrumentation only provides a level indication when the level is within the reactor coolant pumps; therefore this level of instrumentation may not be useful during feed-and-bleed operation.

Isolation of the RCS loops contributes to core damage frequency during the midloop operation. This practice makes the SGs unavailable for decay heat removal upon loss of RHR. In a cold shutdown condition the SGs are usually maintained in the wet lay-up condition with the secondary side filled with water. During midloop operation, the availability of the SGs makes reflux cooling a possible method of mitigating a loss of RHR. This may be the only mitigating function available in a station blackout.

The RHR system at Surry has many 'single' failure potentials. This is due to the fact that it is not a safety system (i.e. it does not perform a safety injection function).

The following factors influencing human performance were identified for low power and shutdown operation:

- administrative controls;
- human factors engineering;
- measures to ensure plant staff awareness, e.g. alarms, taggings, etc.;
- operator training;
- workload and stress;
- procedures;
- task verification measures.

The following requirements were identified for an HRA methodology applicable to low power states and shutdown:

- to quantify the frequency of human errors as initiating events;
- to quantify the impact of influencing factors on an error frequency and recovery actions;
- to construct models for an analysis and quantification of diagnostics and knowledge based tasks.

The preliminary results indicate that the off-site releases from core damage during shutdown are comparable to full power release. The risk associated with a specific outage is highly dependent on the outage schedule.

Studies in France

Several topics found to be important have already been manifested in the generic findings in France. There are several insights in the enclosed Electricité de France paper concerning total loss of the RHRs, loss of primary coolant accident and dilution by a plug of water.

There are two cases where a boron dilution can take place: RHR connected and RHR not connected. There is a real contribution to risk while RHR is connected, especially during midloop operation and only in the case of the 'plant dilution accident' if not connected.

As a result of the study concerning the loss of RHRs instrumentation improvements (Vortex detection, US level measurements) were carried out. A safety engineer should be present in the control room during water level changes.

Studies in Belgium

The studies in Belgium manifest the role of bunkered systems. The CDF in shutdown is significant when compared to power operation. The methodology used in the studies in Belgium was quite similar to that of the study in France due to the similarity of the reactor type.

6. APPLICATION OF LPS PSA RESULTS

6.1. SAFETY CULTURE/HUMAN FACTORS

As a result of PSA it is necessary to make sure that everyone involved in shutdown, from top management to the last worker, is aware of the high risk during certain stages of shutdown. Employees/staff should be aware that an error could result in an initiating event with a short reaction time. The results of a shutdown PSA can select the relevant stages for which this assumption is correct.

Human factors are responsible for two different inputs to a low power and shutdown PSA:

- Initiating event (result of a human error).
- Human error during the response of an initiating event.

The frequency of initiating events produced by human errors can be reduced by detailed shutdown planning including maintenance and testing tasks. This should be supported by an administrative control. The PSA can identify at which stage (plant condition) human error is particularly relevant to the risk so that the planning can concentrate on these stages.

One major benefit of a shutdown PSA is the provision of a basis for identification of the period of greatest risk of core damage or other consequences during the outage. Identification of the periods of greatest risk will bring benefits in terms of safety culture providing that personnel at *every level* are informed of this aspect. Identification of the periods of greatest risk will also highlight the need for additional protective measures at certain stages during the outage.

6.2. TRAINING

It has been recognized that most of the current sessions concentrate too much on 'at power' training scenarios, in which the operator is expected to respond to instrument failure. However, outage and low power operation has been recognized as high risk, and until now little emphasis was placed on the plant startup and shutdown simulation.

More training should be focused on certain critical phases or scenarios (midloop operation with low coolant inventory, boron dilution, etc.). An effort should be made to develop training tools that highlight 'critical parameters' (for instance, using displays of estimated time to boil, minimum water level before pump cavitation, etc.).

A good understanding of the potential for core damage during the shutdown and outage operations by all personnel who may be involved in dangerous activities should reduce the risk associated with them. Events such as loss of residual heat removal function, loss of power sources, loss of shutdown margin or coolant inventory should be included in training programmes.

6.3. TECHNICAL SPECIFICATIONS

There is substantial plant to plant variability in outage planning and management, and therefore technical specifications should not be used to define minimum requirements during an outage. However, it must be recognized that such requirements have the potential severely to restrict the ability to conduct the outage efficiently. It is therefore essential to show that a technical specification requirement for shutdown conditions is in line with the safe outage conduct. In spite of the remaining unresolved questions and issues, a completed LPS PSA is the best tool available to date, to support these far reaching decisions for shutdown technical specifications. There is a sense of urgency in completing a substantial number of high quality LPS PSAs that need to be independently peer reviewed to provide the database of insights needed to consider the need for shutdown technical specifications.

Because many of the existing TS focused on power operation, the utilities should improve their TS to include the following:

- off-site and on-site AC power requirements;
- RHR system and support systems requirements.
- required containment integrity for PWRs;
- necessary systems for inventory control;
- for PWRs requirements to protect against fast and slow dilution accidents and loss of RHR (during draining to midloop conditions).

The above limitations should especially apply to critical plant conditions during shutdown such as midloop operational and refuelling operations.

On the basis of future PSA and deterministic analysis, the TS improvements should also address the following:

- closed versus an open RCS;
- heat removal capabilities (SG in PWR, boiling in BWR);
- use of RCS jam seals;
- safety related equipment versus reliable or temporary equipment;
- RHR recirculation capabilities.

6.4. PROCEDURES

There are three main types of procedures:

1. *Continuous use of procedures* (read and check a line at a time, all along an elementary operation), useful to guarantee the PSA analyst that actions are made as required.

2. *Checklists*, to be used before beginning some critical operation. These have to be available, particularly to track the status of the plant (control of configuration of systems and changes), including inventory of redundancies (mandated or available) inventory of coolant, of borated water or boron, etc.

3. *Procedures that support basic and generic information*, available as a quick reference at any moment. They can tell:

- what is good practice;
- how to plan outages;
- how to manage water inventory, cooling means, support systems, etc.

They can include such results of analyses as:

- graphs giving the time to boil in a variety of cases, depending on water level, decay power, temperature of the water, etc.;
- graphs giving the time to close the containment in a variety of cases;
- graphs giving the time to excess dilution.

They can be used to plan the outages.

Procedures 2 and 3 have to be made with an overall view of the plant.

They may be either implementations of the conclusions of the PSA or rules telling the analyst how things are done;

In every case, as for technical specification, there can be feedback in every direction, between the PSA and the procedures (in an iterative process).

The shutdown PSA is expected to demonstrate the importance of an overall testing policy and to provide feedback useful in the development of this policy — for example, a need may be identified to test certain components important for the shutdown phase during operation.

6.5. BACKFITTING

It is important to recognize that there are significant risks during the shutdown period.

In future it is anticipated that plant and system design will consider shutdown PSA. In the meantime, it is expected that shutdown PSA will highlight requirements for backfitting in current systems used during shutdown — in much the same way as full power PSA has led to improvements in safety systems.

6.6. FIRE AND FLOOD

One benefit of implementing a shutdown PSA will be the increased awareness of the risks and consequences of fire and flood. The shutdown PSA will also identify the key sequences where fire and flood in specific locations may damage apparently remote systems. This may lead to beneficial modifications of procedures and instructions.

6.7. SENSITIVITY/UNCERTAINTY/IMPORTANCE (SUI) ANALYSES

SUI analyses are important in implementing the results and models of the LPS PSA to improve plant operations during shutdown and thus reduce risk. These analyses should provide insights of the source of risk, the sensitivity of the results to assumptions and uncertainties, and the importance of the various features in maintaining current plant risk levels. Caution should be taken when making changes in operational activities or programmes since there is the possibility of introducing new vulnerabilities or removing a feature which is important in keeping risk low. Both the risk achievement and risk reduction worth should be considered to prioritize features and human actions with respect to their importance to risk.

Appendix

PAPERS PRESENTED AT THE TECHNICAL COMMITTEE MEETING

ANALYSIS OF ACCIDENT SEQUENCES IN SHUTDOWN STATES FOR THE DOEL 3 AND TIHANGE 2 PSAs

P. FOSSION
Tractebel Energy Engineering

P. DE GELDER
AIB-Vinçotte Nuclear

Brussels, Belgium

Abstract

In the framework of the decennial safety revaluations of the Doel 3 and Tihange 2 nuclear power plants, level 1+ PSAs (including containment response analysis) are being carried out. Both analyses will be finished towards the end of 1992.

From the beginning of these projects it has been decided to include also the shutdown states. This paper describes the scope of the analysis and the methodologies used. It describes e.g. the shutdown states considered in the analysis together with the plant specific data used for establishing the operating profile of the plants, the initiating events taken into account, analyses carried out to determine the system success criteria in these shutdown conditions, the methodology used for the human reliability analysis.

Since the analyses will only be finished at the end of 1992, a detailed evaluation of the results will only be available in spring 1993. However, a description of the major findings already available is given. Especially the problems encountered in performing the analysis (for example on human reliability modelling) and which are specific for an analysis of the shutdown states are highlighted.

1. INTRODUCTION

For the seven nuclear power plants nowadays in operation in Belgium, the Royal Decree of Authorization imposes to perform a safety revaluation every ten years after initial start-up. For the Doel 3 and Tihange 2 plants, which started up in the years 1982-1983, this safety revaluation process, mentioned further on as the decennial revaluation, is now going on. This revaluation is carried out in close cooperation between the utility (Electrabel), the architect-engineer (Tractebel) and AIB-Vinçotte Nuclear (AVN) as regulatory body.

Since Doel 3 and Tihange 2 (900 MWe Framatome PWRs) were designed on a deterministic approach, it was judged useful by the utility, the architect-engineer and AVN to perform a probabilistic safety analysis (PSA) in the framework of the decennial revaluation of these plants. It was agreed to perform a level 1 PSA, with additional analysis of the containment response for characteristic accident sequences but without analysis of the source term (fission product behaviour within containment).

The PSAs are performed [1,2] by Tractebel Energy Engineering (further referenced as Tractebel) and reviewed by AVN.

2. SHUTDOWN AND LOW POWER SAFETY ASSESSMENT

Within the decennial revaluation for Doel 3 and Tihange 2, some subjects dealing with safety during low power and shutdown states, have been incorporated. They consider especially :

- operator aids during these states. Based on external and plant specific experience, the needs and the available means for the operator aids are evaluated;
- loss-of-coolant accidents during non-power states, in relation to analyses performed in the framework of the Westinghouse Owners' Group.

Besides these subjects treating some particular aspects of safety at low-power and shutdown, it was decided at the start of the PSA-projects to include also low-power and shutdown states within the PSA-analyses. This should yield a more global evaluation of the safety during these states.

In the following paragraphs, these analyses carried out in the framework of the PSAs are described in more detail.

3. SCOPE OF THE ANALYSIS

3.1. Low-power and shutdown states covered.

For the PSA, two principal modes of operation of the plants have been distinguished :

- state A : operating conditions during which the operation of the RHRS is not permitted ($p > 30$ bar; $Tm > 180$ °C).
- state B : operating conditions during which the RHRS can assure decay heat removal ($p \leq 30$ bar; $Tm \leq 180$ °C).

Within these two principal modes, further distinction can be made between stationary modes in which the plant can remain for long time intervals and transitional modes, characterized by large variations in (p, T), when going from one stationary mode to another. Since the annual fraction of time spent in the transitional modes is rather low, it was felt that for a first analysis these modes could be left out of the scope. As shown in § 5.1, these transitional modes not considered in the PSA represent only about 0,7% in time.

After elimination of these transitional modes, 4 states are further considered within the PSA :

- state A : from 100% power, over hot shutdown, down to the (P11, P12) - permissives characterized by ($p > 138$ bar, $Tm > 284$ °C). Within the whole domain covered by this state, the ECCS starts automatically if required.

- state B1 : shutdown with RHRS connected; primary pressure between 30 and 23 bar, primary temperature between 120 and 70 °C; primary coolant in single-phase (solid) state.

- state B2 : shutdown with RHRS connected; primary pressure equal to atmospheric pressure, primary temperature between 70 and 10 °C. Since this state has to be reached for interventions on the primary side, it is supposed that during the whole time spent in this state the reactor is on mid-loop operation.

- state B3 : reactor open for refueling with RHRS connected; reactor pit filled with water.

3.2. Initiating events covered.

For establishing the list of initiating events to be covered by the Doel 3 and Tihange 2 PSAs, two main sources were used : generic lists of initiating events taken from literature or other PSAs and an analysis of plant specific aspects (design and operating experience) which could indicate plant specific initiating events.

At least for a first phase of the PSA, it was decided to exclude from the scope of the analysis the external hazards (seismic hazard, aircraft crash,...) and the internal hazards (fire, flooding,...). Hazards such as airplane crash and explosions in the vicinity of the plant were already considered on a probabilistic basis at the design stage of Doel 3 and Tihange 2 , in accordance to USNRC-rulemaking. The analysis of hazards as internal flooding and fire was postponed since they were well covered on a deterministic basis during design (especially by strict physical separation). Also for earthquake it was judged that sufficient margins are incorporated in the seismic design, so that reconsideration of the seismic hazard in the PSAs is not of high priority.

The two sources and the limitations mentioned above, led to the following list of initiating events to be covered for the shutdown states :

- loss-of-coolant-accidents; in state B1 the maximum leak considered has an equivalent diameter of 12" (corresponding to a rupture of the RHRS suction line), while in states B2 and B3 the maximum leak considered has an equivalent diameter of 2" (ruptures of connections during material handling actions).

- transients, as spurious operation of the ECCS, reactivity incidents, loss of cooling systems (component cooling system or service water system) and loss of RHRS.

- loss of electric power (loss of offsite power or loss of electric busbar)

- spurious operation of the "bunkered systems" (installed as protection against external hazards).

- ATWS, (limited to dilution in state B1).

4. METHODS USED FOR THE SHUTDOWN ANALYSIS

The PSA-model is based on the combination of small event trees and large fault trees. Hence, quantification is done by fault tree linking.

For the initiating events dealing with leaks in the primary or secondary circuits (in case of shutdown states, only loss-of-coolant-accidents), the accident sequences are analysed over a mission time of 2 weeks. For the other initiating events, the mission time is limited to maximum 72 hours.

The success criteria of the systems and the time delays for operator intervention are established from plant specific thermohydraulic calculations, or from generic references [3,4,5]. For each initiating event, a dossier containing the characteristics and the major results of the different thermohydraulic-calculations, is established. This dossier is a support document for the event tree construction.

Within the human reliability analysis, two major tasks have to be distinguished : the analysis of pre-accident human errors and the analysis of human errors in the post-accident phase.

The methodology used for the analysis of pre-accident human errors is to a large extend based on the ASEP-methodology [6]. The analysis of post-accident human errors is based on the methodology developed for the French PSAs [7]

5. DATA USED FOR THE SHUTDOWN ANALYSIS

5.1. Initiating event frequencies

To determine the frequency of the initiating events during the shutdown states, the time spent in each of these states should be known. Therefore an analysis of the operating experience of the Doel 3 and Tihange 2 plants has been performed. The results of this analysis, averaged over ten years of experience and over the two plants, is shown in tabel 1. As already mentioned in § 3.1, it can be deduced from table 1 that the transitional modes of operation, not covered by the PSA, represent only 0.7% in time.

TABLE 1

Operating profile of the Doel 3 and Tihange 2 plants

State	Description	Duration (h/y)	Contribution (%)
A	From 100% power to (P11-P12)	7912	90,3
B1	Cold shutdown (pressurized; solid)	123	1,4
B2	Cold shutdown for primary intervention (assimilated to mid-loop operation)	366	4,2
B3	Cold shutdown for refueling (reactor pit filled)	301	3,4
Total		8702	99,3

Most of the initiating event frequencies during the shutdown states were obtained from those during full power, adjusted to reflect the number of hours spent in each particular state. Some frequencies (e.g. total loss of component cooling or service water system) were deduced from calculations based on the reliability analyses of the systems.

5.2 Component reliability data

The reliability data of the components (failure on demand, failure to run) are the same as for the power state.

No specific test and maintenance unavailability data for the shutdown states are available. In some cases, the accident sequence quantification is performed assuming one redundancy out-of-service for preventive maintenance.

6. RESULTS

Since the PSA analyses for Doel 3 and Tihange 2 will only be finished at the end of 1992, no detailed results can be given at this moment.

However, the partial results show already that the core melt frequency during the shutdown states will not be negligible compared to the full power state. The human factor contributes significantly to the core damage frequency in the shutdown states. As a consequence, a specific set of procedures for the shutdown states was developed.

Findings related to the installation itself will only be available after detailed analysis of the results, including the sensitivity analyses.

Doubts have been raised about the applicability of the human reliability methodology (developed for power states) to non-power states. For example, special attention has been devoted to the analysis of the initiating event "inadvertent draining during mid-loop operations". This event necessitates quick reactions of the operator in order to restore the situation before deterioration and it is not evident whether time-reliability curves deduced for operator response to initiating events in power states are applicable to non-power states.

REFERENCES

1. M.I. COLARD, P. FOSSION and M. ROCH, "Methodology and Status of the PSA studies for revision of the Belgian Doel 3 and Tihange 2 NPP", presented at the conference on "Nuclear Safety : The Way Ahead", organised by IBC Technical Services Ltd, Brussels (February 27-28, 1991).

2. M. ROCH, "Status of PSA Studies for Doel 3 and Tihange 2 Nuclear Power Plants", presented at the conference on "PSA/PRA Safety & Risk Assessment", organised by IBC Technical Services Ltd, Londen (December 3-4, 1992).

3. WCAP-11916. "Loss of RHRS Cooling while the RCS is Partially Filled", July 1988.

4. Abnormal Response Guideline ARG-1. "Loss of RHR while Operating at Mid-Loop Conditions"; Validation Report; March 15, 1990.

5. NUREG/CR-5855. "Thermal-Hydraulic Processes during Reduced Inventory Operations with Loss of RHR". April 1992.

6. A.D. SWAIN, "Accident Sequence Evaluation Program - Human Reliability Analysis Procedure", Nureg/CR-4772.

7. EPS-1300. Etude Probabiliste de Sûreté d'une tranche du Centre de Production Nucléaire de Paluel (1300 MWe). Rapport de Synthèse (31 mai 1990).

MODELLING OF SELECTED INITIATORS FOR SHUTDOWN AND LOW CONDITIONS OF VVER 440 REACTORS

I. ČILLÍK*, I. TINKA**, J. KLEPÁČ*

* Nuclear Power Plant Research Institute,
Trnava

** Energoproject,
Prague

Czechoslovakia

Abstract

The shutdown safety of VVER 440 reactors is discussed in relation to reactivity changes which may occur related to the load follow operations. The risk was estimated for the following: withdrawal of a control rod group and control rod ejection. The framework for analysis of other initiating events is given.

INTRODUCTION

During the last period of safety analysis of VVER 440 NPP in CSFR the attention is focused also on the safety analysis of shutdown and low power state of reactor. It is also because of the solution of the maneuverability problem of VVER 440/V 213 units like the consequence of the increasing of electricity production from NPP's to the 50% level. In the past some specific initiators of reactivity changes of VVER 440 were solved in Safety Reports and at least also in PSA Level 1 study for Dukovany NPP.

It is clear, that there is interest to extend this list of shutdown and low power initiators with the intent to establish sufficient operational procedures minimalize these events and to increase the safety of these NPP's.

SHUTDOWN AND LOW POWER STATE REACTIVITY CHANGES INITIATORS SPECIFICATION FOR VVER 440 REACTORS

Within the Safety Reports for Dukovany and Mochovce NPPs were analyzed followed initiators of reactivity changes during shutdown and low power reactor state:

a) inadvertent withdrawal of control rod group
b) control rod ejection

c) inadvertent connection of a cold RCS loop
d) uncontrolled decrease of the boron concentration in the reactor coolant
e) sudden release of boron sediments in reactor core
f) inoperability of control rods:
   - one control rod stuck in the bottom position
   - one control rod stuck in the top position
   - an anticipated insertion of a control rod into the core from a stuck position.

In the frame of this initiators category the attention will be dedicated to initiators ad a) and b) during shutdown and low power state from following reasons:

1. Cool water of 55÷70 °C temperature is storaged in the emergency core cooling system. From the point of view of positive changes of reactivity, the injection of this water to the core is not dangerous because of the 12 g H_3BO_3 per kilogram concentration of solution. This concentration gives sufficient margin of undercritical state of reactor during it's cold state (20 °C). Potential risk due to injection of cold water into core follows from the possible mistake of the connection of cooled loop of primary circuit to the working loops. If temperature difference between cold part of working loop and hot part of connected loop is greater than 15 °C, the opening of the main closing valve is blocked (if they are not closed, the overcooling of the loop is not possible), as well as the start of main circulating pump.
   There was performed calculation of hypothetical case, that whole loop is cooled down to 50 °C. Also in this non realistic state would be possible the core melting only in the case of reactor protection system total failure.

2. During non controlled decreasing of H_3BO_3 concentration in the coolant the positive reactivity increasing occures (the negative reactivity comes near to 0) slower than in the case of the control rod group withdrawal. On the other hand, if all H_3BO_3 were be removed out of core, total positive reactivity introduction would exceeded the negative reactivity of all control rods after reactor scram. The calculation demonstrated, that in the case of the maximal possible velocity of H_3BO_3 concentration decreasing (during regime "great" boron re-

gulation is injected into core reactor clear water without H_3BO_3) the reactor would be critical in the case of right action of scram signal after period of 50÷70 minutes. Than the operator has enough time to realize sufficient measures - to stop the dangerous decreasing of H_3BO_3 concentration in core. Because of slower progress of determined parameters (reactor power, fuel temperature, cladding temperature,...) during H_3BO_3 concentration decreasing in the comparison with inadvertent withdrawal of control rod group, these initiators can be grouped into one analyzed - control rod group inadvertent withdrawal.

3. During the sudden release of boron sediment in core (according to performed calculation) icrease positive reactivity is lower and slower than in the case of control rod ejection. In the case of low power and shutdown state of reactor this process depend on the rate of boron sediment release and the velocity of control rod ejection and the amount and localization of boron sediment in the core. These data have uncertainties and knowledges are on the low level to obtain enough verified input data for neutron-physical and thermal--hydraulic calculations.

4. The last group of initiators (f) was not still analyzed for different operational modes including shutdown and low power conditions. Due to this state it is not possible to provide risk modelling on the sufficient verified level.

RISK ANALYSIS OF SELECTED REACTIVITY CHANGES INITIATORS

Inadvertent withdrawal of control rod group

Only one safety function (SF) which can minimalize the consequences of this initiator is reactor protection system action of first (HO1) and second (HO2) category. Realization of other type of SF, like, for example, residual heat removal, has not any significant effect.

Function event tree is very simple. It has only two sequences - one is correct function of reactor protection system (RPS) without core melting and other without RPS with core melt consequence.

The success criterion is RPS action at the last moment at 35. sec. from the moment, in which start inadvertent movement of control rods group out of core (at 40. sec. maximum fuel temperature reaches the value 2670 °C, which corresponds to spent fuel melting temperature in the case of RPS action). Neutron-physical and thermal-hydraulic calculations were performed by code REPA 1D. Fuel elements are divided into five channels in the code, which have the same axial power distribution, but they differ in relative power.

From the point of view of accident result judgment, channels 4 and 5 are significant, where channel 4 represents the maximum loaded fuel element and channel 5 the hypothetical hot channel, which has added 10 % for uncertainty of power macrodistribution and 10 % for uncertainty of power microdistribution.

The calculations were performed for following initial conditions and assumptions:

- critical reactor, reactor power 13.75 kWe = 0.001% of nominal power
- three control rods groups are in the bottom position; the others in the top position
- reactor coolant flow is 8590 kg/sec
- reactor input coolant temperature is 266 °C
- reactor output coolant pressure is 12.26 MPa
- others parameters were chosen conservativly.

In the case of RPS total failure (without scram) the time course of essential physical parameters is following:

Time (sec)	Parameter value
0 ÷ 25	Neutron power increasing, fuel and coolant temperatures remain on initial values
27.4	Reactivity maximal value - 0.519 %
42.5	Hot channel DNB (channel 5)
52.6	Reactor power equal to 112 % of nominal power
55.2	DNB in channel 4
57.8	Fuel maximum temperature - 2670 °C (spent fuel melting)
61.5	Fuel maximum temperature - 2840 °C (fresh fuel melting) in the channel 5
62.6	DNB in channel 3

66.7 Maximal value of average fuel radial enthalpy - 840 kJ/kg (for allowed degree of fuel element damage) in the channel 5)

75.9 DNB in channel 2

83.7 Maximum fuel temperature in the channel 4 - - 2670 °C

The calculation was interrupted in 88.7 sec, when reactor neutron power reached the value of 12 % of nominal power and further it would increase nearly proportionally (linearly). Scram signals (HO1 and HO2) would be created till 15. sec of the process, scram signal from power increasing till 30. sec of the process.

Control rod ejection

The most unfavorable state from the point of view of control rod ejection is shutdown reactor hot state with one or two control rod groups fully inserted in reactor core (given by their allowed position in critical or nearly critical state). Disfavor of this state is given namely by:

- high level of ejected rod efficiency (criticality on instant neutrons)
- power distribution coefficient high disequality
- ejection short time (0.1 sec), when feedback influence (only Doppler effect affects) is not sufficient to decreases significantly power maximum during process.

In the old Russian documentation there was given ejection rod velocity approximately 0.55 m/sec, to which corresponds the time of rod ejection from core cca 4.5 sec. For this time relations of the operation mode progress would have qualitativly different character if feedback influences of moderator temperature are not taken into account.

For instance it is possible to demonstrate the example when in the case of the efficiency of ejected control rod 1.4 beta and ejection time 0.1 sec the melting temperature (cca 2800 °C) and maximum allowed value of average fuel radial enthalpy (840 kJ/kg) are exceeded in hot channel. If ejection time of control rod is changed from 0.1 sec to 4 sec, the reached power maximum will change from cca 40 (times of nominal value) to cca 0.4, fuel temperature maximum do not exceeded over cca 750 °C in the hot channel and fuel radial enthalpy cca 180 kJ/kg.

The reason, why this analysis is not being carried out with this "realistic" ejection time, are conservative requests which are applied in FRAMATOM, Westinghouse, ABB and Babcock-Wilcox analysis. These companies follow the way of improvement of used code, but there are also other possibilities of improvments in this type of calculations.

In the case of the conservative assumption of control rod ejection time in shutdown reactor hot state is not possible to exclude core melting even in the case of reactor scram.

Due to this situation the function event tree has only one sequence which leads directly to core melt. In this case is not also possible to establish success criteria. This analysis leads to the technical specifications changes:

a) during the reactor work in hot shutdown state minimum four control rod groups have to be in the top position, what ensures higher level of scram efficiency
b) in the case of follow load regime of reactor in the rate from 50 to 100 % of nominal power, the working control rod group (6. group) can not be inserted in to core more deeply then 125 cm over core bottom.

For the a) conditions different calculations were performed, which demonstrated, that in this case it is not possible to exclude core melting during shutdown reactor hot state. This calculations were performed by code REPA 1D, which uses one point kinetics model of core configuration and is for this type of work standardized.

The mentioned calculations were performed under the following assumptions and beginning conditions:

- critical reactor in hot state, power = 13.75 kW (0.001 % of nominal power). Four control rod groups are in the top position, two in the bottom position
- reactor input coolant temperature - 266 °C
- pressure at the core outlet - cca 12.26 MPa
- ejected control rod efficiency is 0.81 % (1.266 beta)
- the most unfavorable reactivity coefficient according to fuel temperature is - 2.9×10^{-5} K^{-1}
- the same according to moderator temperature is 0 K^{-1}
- the shortest life time of instant neutrons
- the most unfavorable value of heat transfer coefficient of fuel-cladding gap (from the point of view of maximum fuel temperature)

- the most unfavorable axial power distribution (from the point of view of fuel temperature)
- control rod ejection time - 0.1 sec.

For the calculation fuel elements were divided in five channels with following initial power rate (just after control rod ejection)

Channel	Relative power
1	1.0
2	2.5
3	4.0
4	7.1
5	8.6

Relative channels are related only to channel 1, which is the average channel to represent the all core. Channel 4 represents the calculation value of the most loaded fuel element, channel 5 is the same, but with 10 % increasing of values because of power macrodistribution uncertainty and 10 % for power microdistribution uncertainty. It means that channel 5 is hypothetical hot channel to which is possible add maximum fuel elements from the six adjoining fuel assemblies around the ejected control rod. It is possible to add maximum 15 % of fuel assemblies from the total assemblies number to the channel 4. These results are from the point of view of further use for core damage evaluation and specification very conservative (real evaluation would be about 50 % lower). Overmore, there is assumption of 1 sec delay of scram signal and of the activation of control rod drivers and so on. Due to these conservative assumptions the power maximum from the point of view of power progress after control rod ejection from core exceeds before reactor protection system is activated.

Then in the channel 5 the value of fresh fuel melt temperature (2840 °C) and maximal value of average radial fuel enthalpy for allowed degree of fuel elements damage (840 kJ/kg) will be exceeded.

For the comparison of efficiency of reactor protection system the same case was calculated as a ATWS. In this case the result was, that the scram has not any influence on the neutron power progress, but it has positive influence on maximum neutron power reached.

In the case of proper work of reactor protection system, the maximum top boundary of fuel elements damage will be following:

1.7 % with fuel melting

15 % with dishermetical cladding.

In the case without scram about 15 % of fuel elements will be melted.

More control rod ejection initiator pass to LOCA with equivalent diameter cca 86.6 mm.

QUANTITATIVE RISK ANALYSIS

In the case of inadvertent withdrawal of control rod group the action of reactor protection system of first and second category (HO1 and HO2) is necessary. The signals for the creation of second category reactor protection system are reactor period less than 10 sec or allowed reactor power exceeding 105 % with the delay cca 10 sec. The signal for the creation of first category reactor protection system is period less than 20 sec or allowed power value over 110 % of nominal value.

Core melting is caused by loss of both scram signals for both types of reactor protection system. If we suppose that from the point of view of technical structure and signal creation the both reactor protection system category are the same, the probability of both scram signals failure will be the same - 1.47×10^{-4}.

In the case of control rod ejection the consequences are the same whether reactor protection system is activated or not.

CONCLUSIONS

On the basis of performed work in this field of reactivity changes initiators modelling during shutdown and low power state of VVER 440 reactor is clear that we need more detailed simulation of the core by three-dimensional code. At present we look for suitable type of three-dimensional code, which will be modified for VVER 440 reactors to obtain more realistic results.

Also in the case of other initiator there is intent to perform shutdown and low power reactor state risk modelling for selected initiators to estimate safety risk of some specific operation nods not only follow load operations of VVER 440/V 213 reactors.

REFERENCES

Tinka I., Kratochvíl J.: Dukovany NPP - Safety analysis of control rod ejection initiator. EGP Prague, 1990.

Tinka I.: Dukovany NPP - Accident Sequence analysis of control rod ejection in shutdown and low power conditions.
EGP Prague, 1990.

Čillík I., Janíček F.: Initiators categorization, technical specification and modelling in follow load operational regimes of VVER 440/V 213 NPP. VÚJE Trnava, 1992.

EXPERIENCE FROM SHUTDOWN EVENT PRA (SEPRA) FOR TVO I/II

R. HIMANEN, J. PESONEN, H. SJÖVALL
Teollisuuden Voima Oy,
Olkiluoto

P. PYY
Technical Research Centre of Finland,
Espoo

Finland

Abstract

The utility TVO is conducting a comprehensive PSA programme for its two 710 MWe BWRs. The programme was initiated in the year 1984, and the level 1 PSA, including internal transients, LOCAs and fires during power operation, was taken into living use in 1992.

In 1990 TVO decided to extend the PSA study to the analysis of refuelling, shutdown and startup. The Shutdown Event PRA (SEPRA) was reported to the authority in September 1992. The study consists of the analysis of leakages and loss of decay heat removal in the planned shutdown conditions. Special studies were performed for the cold pressurisation, for local criticality events, for heavy load transport and for the transients during startup and shutdown.

A remarkable effort was put to identify risks, i.e., to the qualitative analysis. The regular preventive maintenance tasks in the refuelling outages were analysed and the important tasks were selected for further studies. Besides the severe core damage risk TVO was interested in less grave consequences e.g., the economic risks causing significant extension of outages.

The plant specific screening of initiators consisted of a study on the incident history and of interviewing the plant personnel on selected tasks. A number of thermohydraulic calculations were carried out to support the analysis of accident sequences. The operator actions after an initiating event were verified with the operating staff.

The annual core damage risk from the refuelling outage is about an order of magnitude lower as the risk from the power operation. The modifications decreased significantly the core damage frequency. It is foreseen that the SEPRA will form a basis of the procedure enhancement for the low power states.

1. Introduction

Teollisuuden Voima Oy (TVO) owns and operates two 710 MW ABB Atom type BWR units on the west coast of Finland. TVO I was connected to the grid in 1978 and TVO II in 1980.

The utility is conducting a comprehensive PSA programme for its two plants /1/. The programme was initiated in the year 1984, and the level 1 PSA was taken into living use in 1992 /2/ including the internal transients, LOCAs and fires during the power operation. In 1990 TVO decided to extend the PSA study to the analysis of refuelling, shutdown and startup. The reasons for the decision were the need to complete level 1 PSA, international experience on low power state safety /3,4/, but also the good operating experience of both TVO units. They have continuously exceeded 90 per cent annual capacity factor due to short and effective refuelling outages and suffered only a few unplanned shutdowns. The utility wanted to create a realistic view on the risk level during the shutdown, startup and outage conditions.

The short refuelling outage duration is partly explained by uninterrupted activities in three shifts on time critical line. Conducting the refuelling in almost in minimum time requires tight coordination of parallel activities. During the refuelling period numerous subcontractors, work overtime and reduced safety barriers in the plant itself cause additional safety management requirements.

The Shut down Event PRA (SEPRA) was initiated in 1990 and reported to the regulatory body in September 1992. The total manpower of the study was app. 3 manyears. The SEPRA team consisted mainly of TVO's own personnel completed with a human factors assessment expert.

SEPRA consists of operating modes lower than 8 % of nominal power corresponding the hot shutdown. The operating modes are:

1. Cold shutdown	(reactor unpressurized, T < 100 °C)
2. Hot shutdown	(reactor pressurized or T > 100 °C)
3. Startup	(reactor pressure < 70 bar)
4. Hot standby	(reactor pressure 70 bar)
7. Refuelling	

The time duration for these modes has been evaluated as the average value through the years 1986-92, which correspond best the present state. The average refuelling duration is app. 400 hours.

Besides the severe nuclear risks TVO was interested in other risks e.g., significant extension of outages. Six plant damage states were defined:

1) Mechanical fuel damages
2) Local criticality
3) Overheating of concrete constructions
4) Core uncovery
5) Spent fuel uncovery
6) Severe core damage.

Mainly due to limited manpower, the external events and the loss of external electricity supply were restricted outside the study. Also the effort put to the analysis of electrical maintenance tasks as initiating events was concise.

2. SEPRA main tasks

SEPRA was carried out according to a specific project plan and procedure /5/ written by TVO and checked by the Finnish regulatory body (STUK). The main tasks are described in detail in the following:

2.1 Background material collection

The background material collection included international experience from low power mode PSA, documentation from previous TVO's analyses and documents needed in the analysis of different tasks during the refuelling. For example, the material includes TVO's operating, test and maintenance procedures, time tables for refuelling and outage maintenance task lists.

2.2 Assessment of operating experience

The plant specific screening of initiators consisted of a study on the incident history and of interviewing the plant personnel on selected tasks. The incident statistics mainly from Olkiluoto and quasi similar ABB delivered plants were classified according to a draft initiator list. The list was later used in the assessment of initiator frequencies. The operating experience from other BWRs (e.g., from NEA/IRS reports) was found to be less useful due to different designs of the plants.

2.3 Analysis of operational, test and maintenance procedures

The utility's maintenance specialists skimmed through the regular preventive maintenance tasks in the refuelling outages and selected 16 groups of tasks to be further studied by interviewing techniques. A thorough step by step analysis of each task was performed using a structured questioning form called the 'Human Action Deviation Analysis' (HADA). Particular attention was paid to:

- potential confusion of different human tasks as whole
- potential confusion of certain task steps
- ways to detect the human deviations and to recover
- consequences of human actions
- difficulties in the task coordination and in the risk management
- possible measures to reduce the risks.

Another questioning technique called the 'Analysis of Test Influence' (ATI) was developed for the analysis of tests. Apart from the points included in the HADA, the ATI technique emphasises also the overriding of safety device, the restoration process and the completeness dimension of a test. A remarkable effort was put to reveal risks, i.e., to the qualitative analysis. The SEPRA team's view is that this is the only way to guarantee adequate comprehensiveness of the results.

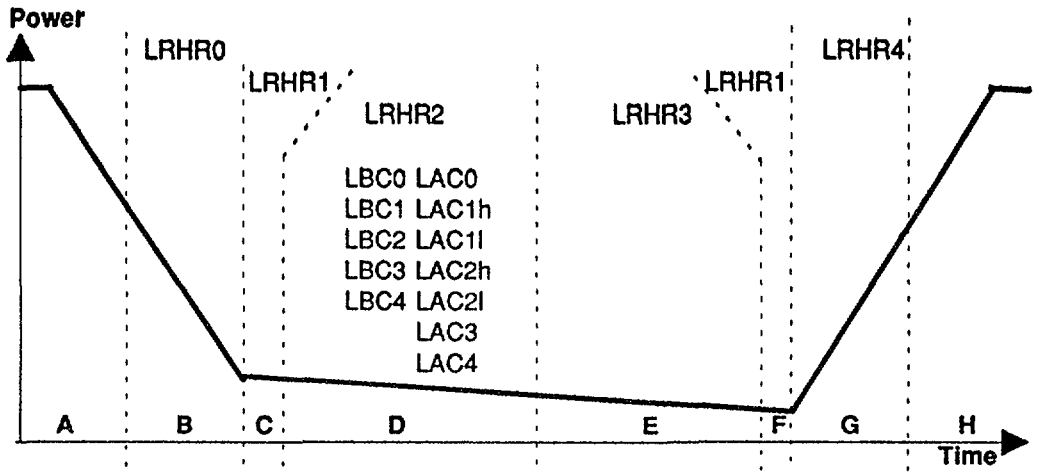
2.4 Determining initiating events, event trees, success criteria and modelling.

The qualitative analysis produced three types of initiators: Leakages Below Core top (LBCs), Leakages Above Core top (LACs) and Loss of Residual Heat Removal (LRHRs). External initiators were not included in the analysis at this stage.

The LACs and LBCs were divided into five classes according to the available compensating water pump capacity. Physical analyses were performed to determine the mass flow of water in different type of leakages. The smallest LAC class corresponds pipe diameter 42 mm and the largest more than 317 mm. For LBC the largest class corresponds leakage through main circulation pump (MCP) axis penetration with diameter 231 mm. Main water sources are the pool water and the core spray system. More information on the classification is given in /9/.

The LRHRs were classified according to the required compensating decay heat removal capacity. Fig.1. illustrates different states of residual heat removal during low power operation and refuelling. A shutdown cooling system and a pool cooling system are available for residual heat removal. The shutdown cooling system is used at the beginning of the refuelling, whereas the pool cooling system has been upgraded by adding an additional heat exchanger line. This enables the pool cooling system operation earlier, app. four days after the shutdown, and the beginning of maintenance of the shutdown cooling system .

The decay heat rate, the configuration of the safety systems and the potential to lose safety systems vary in the course of the refueling outage. Therefore, the low power period was divided into subphases and the safety function success criteria were defined for each of them. The low power incidents allow enough time for manual operations and for thorough planning of recovery actions with only some exceptions: in the case of the largest possible LBC through the MCP penetration the time to close the lower containment personnel access is extremely short.



A and H	=	Phases belonging to the scope of full power PSA
B...G	=	Phases belonging to shut down event PSA (SEPRA)
B	=	Power reduction and reactor shut down
C	=	Pool cooling not possible, opening of reactor lid
D	=	Pool cooling available but the amount of decay heat exceeds its capacity
E	=	Pool cooling available and sufficient for RHR function
F	=	Pool cooling not available, closing of reactor lid
G	=	Startup
LAC	=	Leakage above core
LBC	=	Leakage below core
LRHR	=	Loss of residual heat removal

FIG. 1. Distribution of shutdown initiators in different RHR states.

The SEPRA initiating event frequencies are low when compared with transients in power operation mode. However, the weaker safety barriers cause a narrow safety margin. The LBC initiator frequency range was estimated 1.8 E-6...3.3 E-3 /unit outage and the LAC 1.4 E-4...3.1 E-2 / unit outage. The LRHR initiator event frequencies range is 5.5 E-3 - 1.9 E-1 / unit outage.

Apart from this, special studies were carried out for the unwanted local criticality events, for the overpressurisation of the reactor with steam lines filled with water, for the heavy load transport in the reactor hall and for the transients during short startup and shutdown periods with atmosphere in the containment.

Small event tree/large fault tree technique was used for leakages below and above core and losses of residual heat removal. However, the explicit modelling of, e.g., the sequences leading to unwanted local criticality required different modelling perspective. Task interaction matrix was used to identify coordination errors and to manifest their risk contribution. Its is similar to the confusion matrix approach widely used in human reliability analysis, but the thinking is extended to maintenance tasks. Barrier model illustrates the differences in the safety barriers during different plant operating states. In the refueling outage, the human initiated safety functions is often the only effective barrier while neither containment nor automated functions exist.

Chronological phase diagram can be used to illustrate explicitly latent error sequences and accelerating event courses /6/. Physical parameters and real time scale can be used in the same image to clarify the situation. The diagram was utilised in the analyses of unwanted criticality events, see Fig 2. The method is still under development.

2.5 System analysis and fault tree modelling

The main difficulty encountered in the drafting of event tree models was the lack of written emergency procedures for the refueling period. The fault trees constructed for the power operation were used as the starting point for modelling. However, extensive modifications were required before linking in low power operation event trees, because the initial conditions and the uses of systems are often

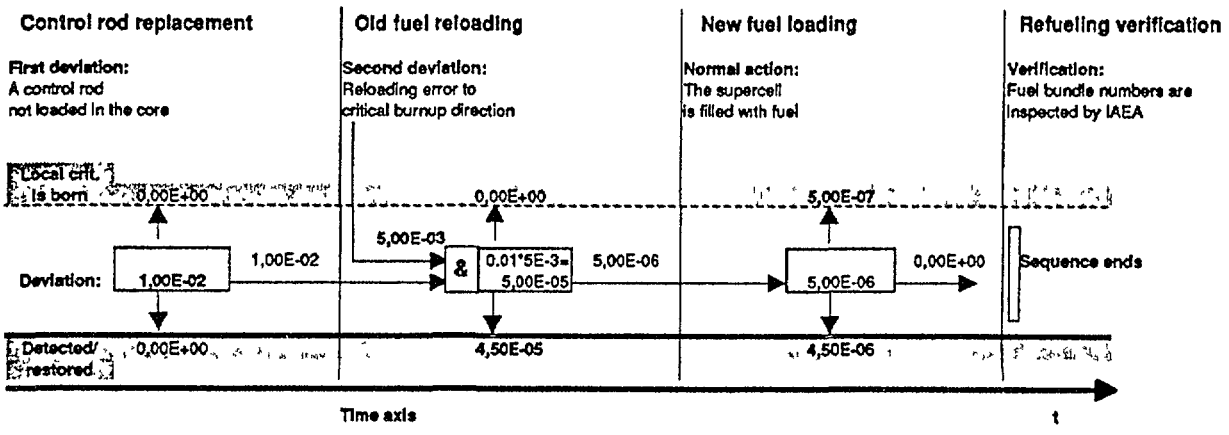


FIG. 2. Chronological phase diagram for a criticality event.

different in shutdown. For example, stand-by systems may be already operating in a RHR state and nearly all the automated actuations are overridden. These observations led to an extensive modification of system models. Also the CCF model of, e.g., 4-train systems with 2 trains prohibited during refueling requires further investigation.

2.6 Reliability data

The human reliability data was based on operating statistics and engineering judgement. Unfortunately, the plant simulator does not give opportunities for large scale utilisation in the refueling state and, thus, cannot be used to generate human reliability probabilities. The SEPRA approch was to use plant specific historical data, when available, and subjective, consistent screening values. The principle was followed when assessing human action probabilities for both initiating events and for recovery actions.

For each quantified human act, a verbal description highlighting the performance shaping factors which mostly affect the quantified case is provided. The background of the used estimate can, thus, be in each case checked and argued. This is an important aspect that should be included in every human error analysis.

Equipment failure rates are based mainly on the same source (T-Book) /7/ as for the power operation. The T-Book contains plant spesific data of TVO NPP.

2.7 Quantitative analysis and its results

Small event tree - large fault tree technique was used to describe and calculate desired sequences. Altogether 15 event trees were constructed, three for leakages below core, seven for leakages above core and five for losses of residual heat removal. The SPSA /8/ code on PC was used for calculations.

The frequency of severe fuel damage during refueling outage is estimated to 3.6 E-6 / unit outage. The contribution of each initiator class is shown in Fig. 3. The leakages below core are dominant initiators. As shown in Fig. 4., their contribution is 68 %. Together with the LACs the loss of coolant inventory has app. 77 % impact. The contribution of the fuel damage in pools is minor as well as the late core melt.

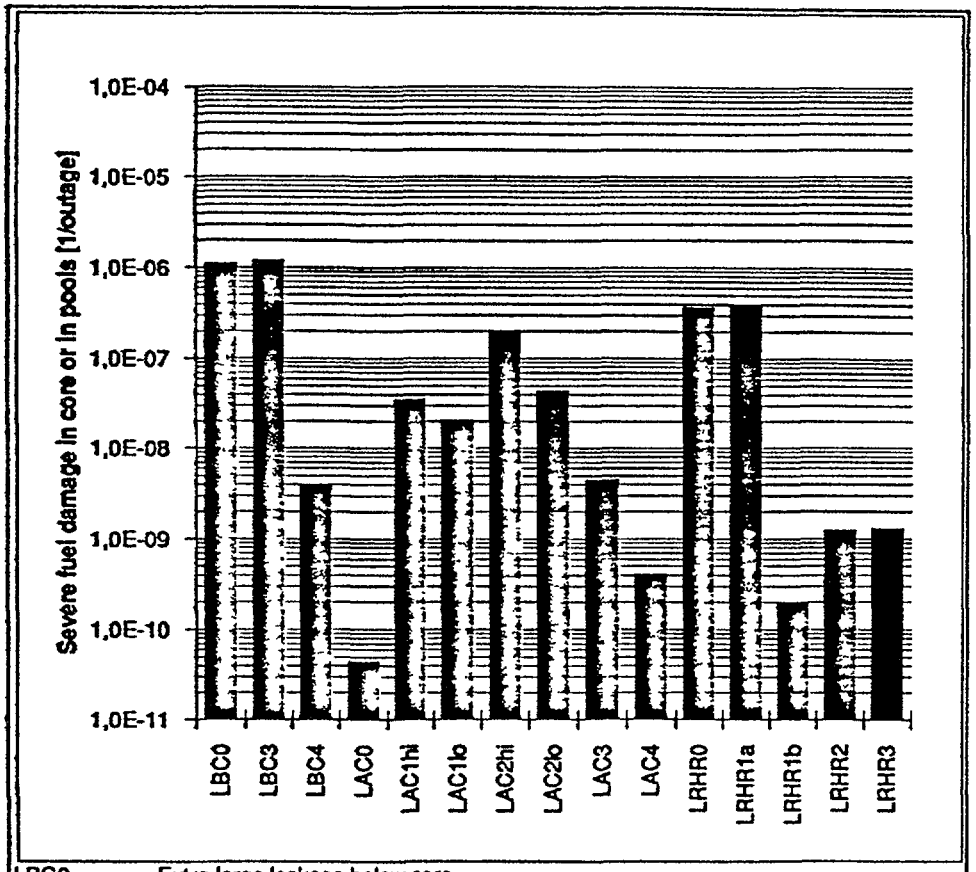
Another interesting aspect is the temporal behaviour of the risk level. The beginning of a refueling outage is important from the risk point of view. As shown in Fig. 5, there is a risk peak during the waterfilling of reactor tank and during the first 3 days of maintenance activities. The former is explained by the potential to overfilling followed by the loss of RHR. The latter consists of several critical maintenance activities below the reactor tank. In addition, the average risk level during the startup and shutdown seems to be 3 times higher than the average risk level in power operation.

The local criticality risk is estimated to 1.8 E-5 /unit outage. The probability of prompt local criticality is more than 2 orders of magnitude smaller. The global criticality for BWR is seen as impossible event. The probability of mechanical

fuel damage is estimated to 6.4 E-2 /unit outage. The probability of a damage of an unique component was evaluated to 1.8 E-2 /unit outage.

2.8 Analyzing the results, modifications, reporting

The refueling outage corresponds about 10 % of the annual core damage risk. The figure is low when compared with other studies, e.g., /3, 4/. One xplanation may be the advanced plant design. The measures taken on the basis of the SEPRA results reduced the risk significantly. Without the measures the contribution of the refueling outage would have been over 50 % of the annual core damage risk. The human deviations dominate the risk with over 90 % contribution. The role of the human actions was confirmed in the sensitivity analysis.



LBC0	Extra large leakage below core
LBC3	Medium small leakage below core
LBC4	Small leakage below core
LAC0	Extra large leakage above core
LAC1hi	Large leakage above core >2.2 m
LAC1lo	Large leakage above core <2.2 m
LAC2hi	Medium large leakage above core >2.2 m
LAC2lo	Medium large leakage above core <2.2 m
LAC3	Medium small leakage above core
LAC4	Small leakage above core
LRHR0	Loss of system 321 reactor lid closed (includes TRW4)
LRHR1a	Loss of system 321, reactor lid closed and steam lines filled with water
LRHR1b	Loss of system 321 in reactor lid opening, pools empty
LRHR2	Loss of system 321, pools filled with water
LRHR3	Loss of system 324, pools filled with water

FIG. 3. The contribution of shut down initiator categories to core damage frequency.

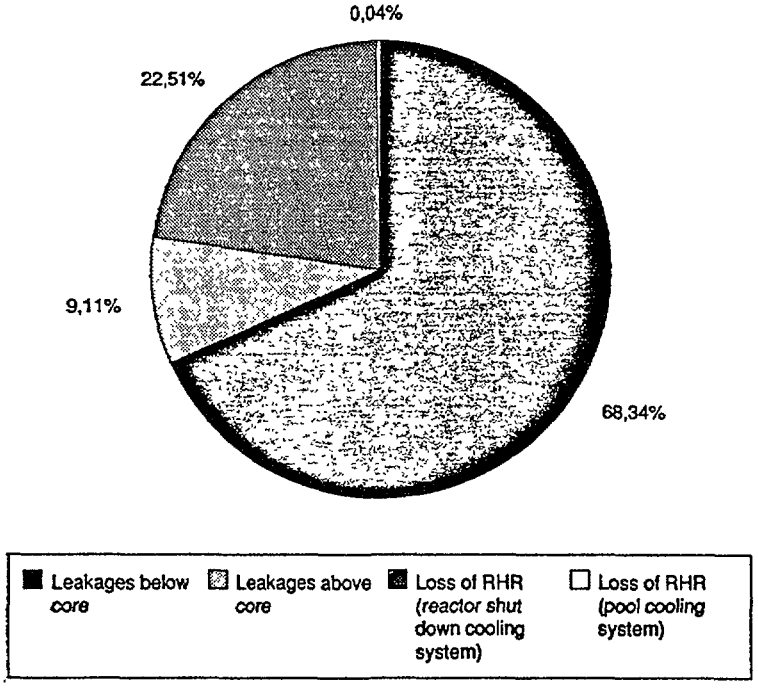


FIG. 4. Contribution of initiator classes to the core damage frequency in refueling outage.

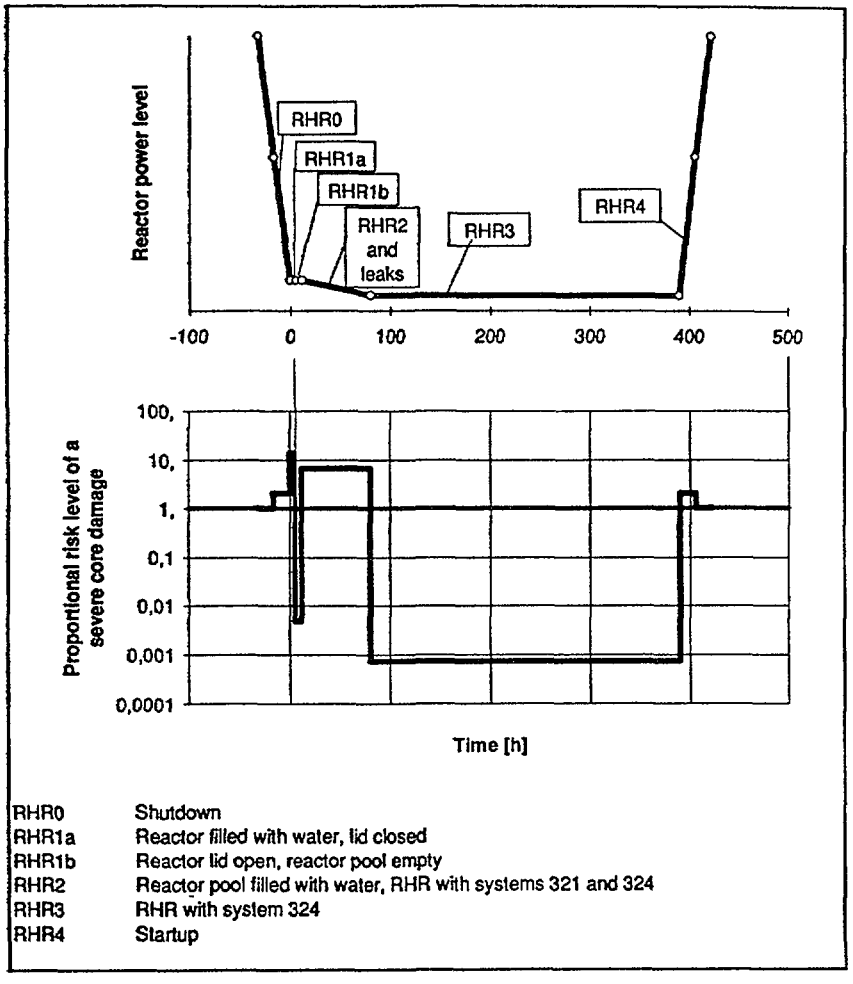


FIG. 5. Temporal behaviour of the core damage risk in the refueling outage.

The dominant risks were decreased in several ways. The preparedness to close the lower personnel access during the main circulation pump overhaul was increased by two specially trained guards. Mechanical cotter pin was installed in the main circulation pump axis penetration plugs to prohibit inadvertent lifting. In order to to prohibit the cold overpressurization the use of auxiliary feed water piston pumps for reactor filling is no more recommended. Pool cooling capacity was increased, capping of S/R-valves was given up and the inspection routine of control rods was modified in parallel with the SEPRA.

3. Conclusions

The Shut down Event PRA (SEPRA) study has contributed to the reassessment of the outage safety level at the TVO NPP. The study demonstrates the position of human actions, which form the largest accident sequence iniator group. Since there are very few automated safety systems for an outage, the human action forms an important part of barriers between an iniator and unwanted consequences.

The results also manifest that the traditional fear of loosing RHR in shutdown is a minor risk when compared to human cause LOCA events. The results of the PRA study have already resulted in actions and they may further lead to procedural changes and completition of the shutdown TechSpecs.

REFERENCES

/1/ Himanen, R., Toivola, A., PRA Program on NPP TVO. PSAM, Los Angeles, February 1991.

/2/ Himanen, R., Vaurio, J., Virolainen, R., Introduction of Living PSA in Finland - cooperation between Utilities and Authorities. 3rd TüV-Workshop on Living PSA Application, Hamburg, May 1992.

/3/ Kiper & al., Seabrook Station Probabilistic Safety Study Shutdown (Modes 4, 5, and 6). New Hampshire Yankee, May 1988.

/4/ Brisbois & al., Probabilistic Safety Assessment of French 900 and 1,300 MWe Nuclear Plants Revue Général Nucléaire, International Edition - Vol. B - December 1990.

/5/ Himanen, R., Project Procedure for SEPRA (in Finnish), Teollisuuden Voima Oy, 1990

/6/ Pyy, P., Human Factors in Scheduled Production Outages, 7th Symposium in Loss Prevention and Safety Promotion in the Process Industries, Taormina, Italy, May 1992.

/7/ T-book. Relibility Data of Components in Nordic Nuclear Power Plants. 3th edition. The ATV Office, 1992. (Available in Swedish and in English).

/8/ I. Niemelä, STUK living PSA code (SPSA), International Symposium of Use of probabilistic Safety Assesment for Operational Safety, PSA'91, Vienna 3-7 June 1991.

/9/ Pesonen, J., Himanen, R., Sjövall, H., Pyy, P. Refuelling PSA for TVO I/II. IAEA Technical Committee on Advances in Reliability Analysis and Probabilistic Safety Assessment, Budapest, Hungary, September 1992.

PROBABILISTIC EVALUATION OF RISK DURING SHUTDOWN

F. MONTAGNON
Service Etudes et projets thermiques et nucléaires,
Electricité de France,
Villeurbanne, France

Abstract

French PWR's have been designed on a deterministic basis. This deterministic approach is now backed up by a probabilistic safety study designed to check *a posteriori* that the overall risk of a severe outcome is sufficiently low for the unit as a whole, or, where appropriate, to provide for the installation of extra defences.

It was in 1986 that Electricité de France decided to launch the Probabilistic Safety Study at the Paluel power station, first-off of the PWR 1300 MWe series. The objective of this study is to identify all the scenarios which may lead to core damage (level 1 study) and to assess the probability of their occuring. All units states are studied, including cold shutdowns for servicing or reloading. Internal hazards such as fires and flooding are not taken into account.

The annual frequency of core damage is assessed at 1.5 10^{-5}/ unit year. This value is for all reactor states. With the unit under power, the calculated risk is only 4.6 10^{-6}/unit year. Risk during shutdown does, however, represent 70% of the overall risk.

This high risk during shutdown can be put down to:

- the high level of initiating events
- the inhibition of automatic protective devices
- diagnostic difficulties
- high rates of maintenance outage times.

The following describes the three predominant accident sequences brought to light during shutdown, and the measures adopted to reduce the risk of their occuring.

1. TOTAL LOSS OF THE RHRS DURING SHUTDOWN FOR SERVICING OR RELOADING

To carry out certain servicing operations on the primary circuit: reloading, work on the steam generators, primary pumps or pressurizer, it is necessary to open the primary circuit and to partially drain it.

While draining the steam generator tubes, sweeping with air and fitting steam generator plugs, the level must be lowered in the area of the primary loops known as the RHRS lower work area. In this area, there is a risk of a whirlpool appearing (water-air mixture) on the inlet side of the RHRS pumps, which may cause loss of prime.

Feedback from experience shows that RHRS cooling has been temporarily lost in this way several times on French units. Almost all French incidents concern draining operations which have not been interrupted soon enough because of lack of accuracy and reliability of the primary level measurements; these having been disturbed by gas circulation.

The accident sequence initiated by total loss of cooling leads to core dewatering if no corrective action is taken by the operator. The operating conditions in the RHRS lower

work area are characterized by a relatively short time lag before dewatering owing to the residual power and the position of the primary openings.

In order to reinforce safety when the primary level is in the RHRS lower work area, stopgap measures have been adopted. These involve a series of extra instructions appended to the Technical Operating Specifications whose aim is to restrict time spent in the RHRS lower work area, to prevent risks occuring and to limit the consequences of these. The following may be mentioned:

- the primary circuit may not be broken at the cold leg when all the hot legs are plugged. Opening the pressurizer manway becomes a prerequisite before any other opening. These measures aim at providing efficient prevention against the risk of core dewatering as a result of the piston effect,

- the primary circuit may only be put into half-open configuration (vessel and pressurizer vents open, primary level alignment depressurized, draining line open) two days after convergence,

- open configuration (removal of the pressurizer manway) is allowed only 3.5 days after convergence.

- opening of the steam generator manways is allowed only 5.5 days after convergence.

These requirements concerning opening times make it possible to guarantee a sufficiently low residual power such that the time before core dewatering is greater than 1 hour.

- containment must be guaranteed to limit the radiological consequences should a trend towards core deterioration start,

- in order to reinforce the primary circuit top-up facilities, the two CVCS pumps and the two LPSI lines must be available,

- servicing operations on systems which are indispensable for proper functioning of the RHRS are prohibited (heat sink, electrical power supply, instrumentation and control).

As incidents occuring in France have above all brought to light the inadequacy of reliable means of monitoring the primary circuit from the control room, actions have been undertaken to improve instrumentation. These consist of:

- developing and installing on each unit precise level measurements in the sensitive zone, made up of an ultrasonic probe in contact with a primary piping hot leg during each depressurized cold shutdown. As the probe does not withstand high temperatures, the system must be installed for a primary temperature of less than 70°C. Its measurement range is limited to the top half of the piping. High Level and Low Level alarms, designed respectively to prevent a wave from rising back up into the steam generator water boxes should the RHRS trigger, and to protect the RHRS pumps with respect to the appearance of the whirlpool, cause staff to be evacuated during plug fitting or removal operations in the steam generator water boxes and are passed on to the control room. In addition, the narrow range vessel level - which uses a different technology - now being installed on units to meet with the needs of the "Status Oriented Approach" should allow a certain amount of overlapping of measurements.

- developing and installing an early warning system for detecting whirlpool phenomena. The parameter judged to be the most representative is the pressure at the pump discharge. An alarm is produced by processing the discharge pressure signal. This alarm is passed on to the control room and to the reactor building to evacuate staff. The whirlpool early warning system provides complete diversification with respect to the measurement level,

- a feasibility study for temperature measurements at the core outlet, after disconnecting the In-core Instrumentation System thermocouples, which reached the conclusion that it is possible to install unit shutdown temperature measurement devices through the use of two mobile in-core chamber ducts via the vessel bottom. This study will only lead to practical developments if feedback experience from the measures mentioned above shows them to be necessary.

These measures have been backed up by increased training in water movements given to operators, and the presence of the SSA (Shift Safety Advisor) in the control room, required during draining phases, in order to provide redundancy.

All these considerations taken together - improved instrumentation, increased monitoring and human redundancy - mean that core dewatering initiated by total loss of the RHRS can be evaluated at:

3.6 10^{-6}/ unit year

Without waiting for the gain provided by these improvements on the initiating frequency to be assessed, it has been decided to install an automatic device for topping up the primary system in order to reduce this figure still further. A Low Pressure Safety Injection pump has been planned for this topping-up. Studies currently in progress concern the installation, if necessary, of a bypass on the 1300 LPSI regulating line, so as to limit the flow rate, if it should turn out that the safety of those working in the water boxes were no longer assured in case of the automatic top-up coming into operation automatically. The advantage of this device will be, in addition, to cover other accident sequences leading to the loss of the RHRS, especially homogeneous dilutions and breaks occuring.

2. LOSS OF PRIMARY COOLANT ACCIDENTS OCCURING OUT OF THE POWER PHASE

The risk of core damage ensuing as a result of a LOCA is distributed as follows:

- overall risk: 6.8 10^{-6}/unit year
- risk out of power phase: 5.3 10^{-6}/unit year
- risk with RHRS connected : to the primary 4.8 10^{-6}/unit year
- risk with primary open configuration : 2.8 10^{-6}/unit year

The risk calculated when the reactor is under power represents only 20% of the overall risk of LOCA, as against 80% in shutdown states. High initiator frequencies and the absence of automatic safeguard signals contribute to the high significance of shutdown states.

Concerning the initiators:

- the hourly rate at which breaks appear on the primary circuit during shutdown states is taken to be equal to that selected for rated pressures and temperatures, itself evaluated from international feedback experience on PWR reactors. This may appear to be a very conservative estimate. In reality, the breaks are mostly the consequence of erosion or corrosion phenomena and are more often revealed during transients than during stable operating conditions.

- when the RHRS is connected to the primary circuit, the frequencies of breaks occuring on the RHRS circuit are considered as being equal to the frequency of breaks on the primary circuit. With this hypothesis, the hourly rate of appearance of a break is doubled in configurations with the RHRS connected.

- when the circuits are depressurized, the size of the break is limited to 3". When the circuits are not under pressure, a cold break in piping can only occur as a result of an error of handling, which makes a break in piping larger than 3" very unlikely, given the design of the PWR 1300. For this reason, large breaks with the primary open configuration are not studied.

So when the RHRS is connected to the primary system with the primary full, closed and vented, the risk of core dewatering as a result of the LPSI not being put into operation by the operator is assessed at 1.9 10^{-6}/unit year. We should note that in cases where a large break occurs (>4"), the operator has only 18 minutes in which to react.

But the dominant sequence concerns the phases with reduced water inventory when the primary is open. Wherever the break may be situated, the loss of primary coolant is interrupted when the level reaches the lower end of the primary piping. However, cooling is quickly lost when the RHRS pumps are triggered. To ensure core safeguard, the operator must provide a top-up to compensate for evaporation (LPSI or CVCS pumps). For a 3" break, he has about an hour following the loss of cooling. The estimation made of the failure of the operator to provide a top-up is prior to the improvements in instrumentation described in the previous paragraph (ultrasonic level measurement, whirlpool detection), improvements which are likely to improve the accident diagnostics. In the configuration with the primary open and reduced water inventory, the risk is assessed at 2.8 10^{-6}/unit year.

The high degree of risk during shutdown states can be explained by the fact that the unit is not completely protected by the automatic start-up of the safeguard systems. Both systems and automatic devices are designed to protect the unit during operation.

3. DILUTION BY A PLUG OF WATER

Physical studies of reactivity accidents have brought to light a possible risk of severe consequences arising as a result of rapid sweeping of the core by a pocket of clear water.

The condition for the formation of a plug of water is the absence of flow linked to the loss of the primary pumps. The plug of clear water can only occur if the flow rate of the thermosyphon which is set up when the pumps have stopped is insufficient to ensure the mixing of primary fluid with the injected flow rate.

The initiating event chosen is the loss of primary pumps following total loss of electrical power occuring during rapid dilution in readiness for divergence. If the operator does not stop the dilution or does not restart a primary pump quickly, a pocket of pure water is formed, which, if it is not broken up when the pump restarts, is driven through the core, causing a reactivity accident.

Despite the uncertainty related to inadequate knowledge of the physical phenomena, particularly concerning the efficiency of the thermosyphon to mix the injected fluid with the primary fluid, and concerning the critical size of the plug of diluted water which will cause inacceptable consequences when it sweeps through the core on start-up of a primary pump, the risk has been quantified and assessed at: 3 10^{-5}/unit year.

Despite these uncertainties, the risk has been judged to be sufficiently high to set under way an immediate modification of the unit, the principle of which is to automatically switch over the suction of the pumps from the CVCS tank to the Reactor Cavity and Spent Fuel

Pit Cooling and Treatment System reservoir borated at a rate of 2000 ppm, upon loss of the forced circulation of the primary, concomitantly with a dilution in progress. This modification has made it possible to significantly reduce the risk identified above to 1.7 10^{-7}/unit year.

In addition to the temporary modification, neutronic and thermohydraulic calculations and mock-up tests have been undertaken. The first results provide new information on the characteristics of the thermosyphon and on the critical volume of the pocket of reactivity which can be inserted, i.e:

- even when unbalanced, a thermosyphon flow is always set up in all the loops, in the normal direction of flow, provided the RHRS is not connected. However, a risk of the thermosyphon's blocking by density remains, not because of the charging flow rate, but because of the seal water injection, which accumulates in the intermediate leg if the residual power is too low to provide a sufficiently efficient thermosyphon flow.

- but when the RHRS is connected, circulation may be blocked in certain loops, since the RHRS in operation works in the opposite direction to the thermosyphon.

- because of the mixing conditions in the downcomer, the critical pocket of $1m^3$ can only come from a plug in the loops of 2.5 m^3 at least.

These physical data modify the cause of the risk. Divergence situations after cold shutdown in which the dilution begins with the RHRS connected need to be distinguished from divergence situations after hot shutdown, these themselves to be differentiated according to whether the residual power is sufficient or not.

The level of risk is being revised to take into account these developments in knowledge. Once the results are known, defences whose efficiency will have been quantified beforehand will be proposed. Already, when the RHRS is connected, any dilution is procedurally prohibited.

SHUTDOWN RISK ANALYSIS OF AN OPERATING PRESSURIZED HEAVY WATER REACTOR POWER PLANT

V. VENKAT RAJ, A.K. BABAR, R.K. SARAF, V.V.S. SANYASI RAO
Bhabha Atomic Research Centre,
Trombay, Bombay,
India

Abstract

The shutdown state has generally been considered to be a very safe state for nuclear power plants till recently. However, operating experience has shown that these are susceptible to a veriety of abnormal situations, under shutdown state, which could have potential to affect public safety. Work related to shutdown risk assessment of Indian Pressurised Heavy Water Reactors (PHWRs) has been initiated. Preliminary assessments made, particularly with reference to an operating PHWR, are presented in this paper.

1. INTRODUCTION

It is generally believed that the shutdown state is a very safe state for a nuclear power plant since the reactor is shutdown and fission chain reaction is stopped. It is thought that, since only decay heat is to be removed, the potential for an accident is negligible. While this is generally true, it should be borne in mind that, even under the shutdown state, it is necessary to perform the relevant safety functions, which include: (i) removal of decay heat, (ii) maintaining the reactor in the shutdown state, and (iii) confinement of radioactivity. It is generally expected that the various safety systems provided can cater to all these functions. However, operating experience with various reactors has shown that many of the reactor systems are susceptible to a variety of abnormal events under shutdown conditions. It is reported [1] that in the case of PWRs and BWRs, these events have included problems related to the management of reactor coolant system inventory, removing decay heat and controlling the shutdown reactivity margin. Instances of heavy water leaks and inventory loss have been observed in PHWRs. It may be noted that such events, related to the safety functions mentioned above, have the potential to affect public health and safety, if left uncontrolled/unmitigated. Apart from those events which have an impact on public safety, other events which do not endanger public safety should also be considered because of their adverse effect on plant availability. In view of these considerations, it is necessary to make an assessment of the potential events under the shutdown state and estimate the risks involved. Work in this regard has been initiated for the Indian Pressurised Heavy Water Reactors (PHWRs). The objectives of the studies are: (i) To obtain an estimate of the contribution of postulated accident sequences, in the shutdown state, to Core Damage Frequency (CDF), (ii) Identification of critical human actions called for during various accident sequences in the shutdown state, and (iii) Development of appropriate and adequate procedures to mitigate the effects of dominating accident sequences. In view of the recent start, the work done so far is of a preliminary nature. This is briefly discussed in this paper.

2. PRESSURISED HEAVY WATER REACTORS

The PHWRs form the mainstay of the Indian nuclear power programme in the first stage and have been in operation for nearly two decades, the first unit in Rajasthan being operational since 1972. Design modifications have been incorporated in the subsequent units at Kalpakkam near Madras and further changes have been made in the next generation 220 MWe reactors built at Narora and Kakrapar. All these reactors have a horizontal core configuration. The primary coolant is heavy water, flowing in a figure-of-eight circuit (see Fig. 1), the temperature at core inlet being 249 deg. C and at core outlet being 293.4 deg. C. The fuel, in the form of short rod bundles, (about 495 mm long) is housed in the pressure tube (coolant channel), which is surrounded by the calandria tube. There are 306 coolant channels in the 220 MWe units, which are connected in parallel to the inlet and outlet headers through feeder pipes. The outlet header is maintianed at a pressure of about 85 bar. Each fuel channel houses 12 fuel bundles, which are 19 rod clusters in the case of 220 MWe units. The relatively cold moderator (average temperature of about 55 deg. C) surrounds the calandria tubes.

In the case of the earlier units in the Rajasthan Atomic Power Station (RAPS) and the Madras Atomic Power Station (MAPS), reactor shutdown is achieved by moderator dumping. In the subsequent reactors from Narora onwards, the shutdown function is performed by mechanical shutoff rods. This is known as the Primary Shutdown System (PSS). In addition, there is also another fast acting Secondary Shutdown System (SSS), which injects poison into tubes inside the core to perform the shutdown function in the event of failure of PSS. In view of the availability of these two independent and diverse fast acting shutdown systems it is not necessary to consider Anticipated Transients Without Scram. In addition, these new generation of reactors are also provided with a system known as ALPAS (Automatic Liquid Poison Addition System) to cater to maintenance of long term shutdown margins with respect to reactivity.

While the steam generators can cater to core heat removal under the shutdown state, a shutdown cooling system is also provided to perform the safety function of decay heat removal in the Indian PHWRs. A pump and a heat exchanger connected between the reactor inlet and outlet headers, at each end of the reactor, form part of this system (see Fig. 2). During normal operation, this system is isolated from the main primary heat transport (PHT) system. It is generally valved in when the PHT system is cooled down to a sufficiently low temperature, say in the range of 130 to 150 deg. C. The reactors are provided with a containment to contain the radioactive releases, if any. While the reactors at RAPS have a single containment with a dousing system for pressure suppression during LOCA, the reactors at MAPS have a partial double containment, with vapour suppression pool for limiting pressure during LOCA. The reactors at Narora and subsequent plants have full double containment.

3. SHUTDOWN RISK ASSESSMENT

It is important to realise the distinctive features in modelling the shutdown risk as compared to the standard Probabilistic Safety Assessment (PSA) methodology. Selection of initiators and plant response analysis are somewhat different in the case of shutdown risk assessment. When the reactor is in the

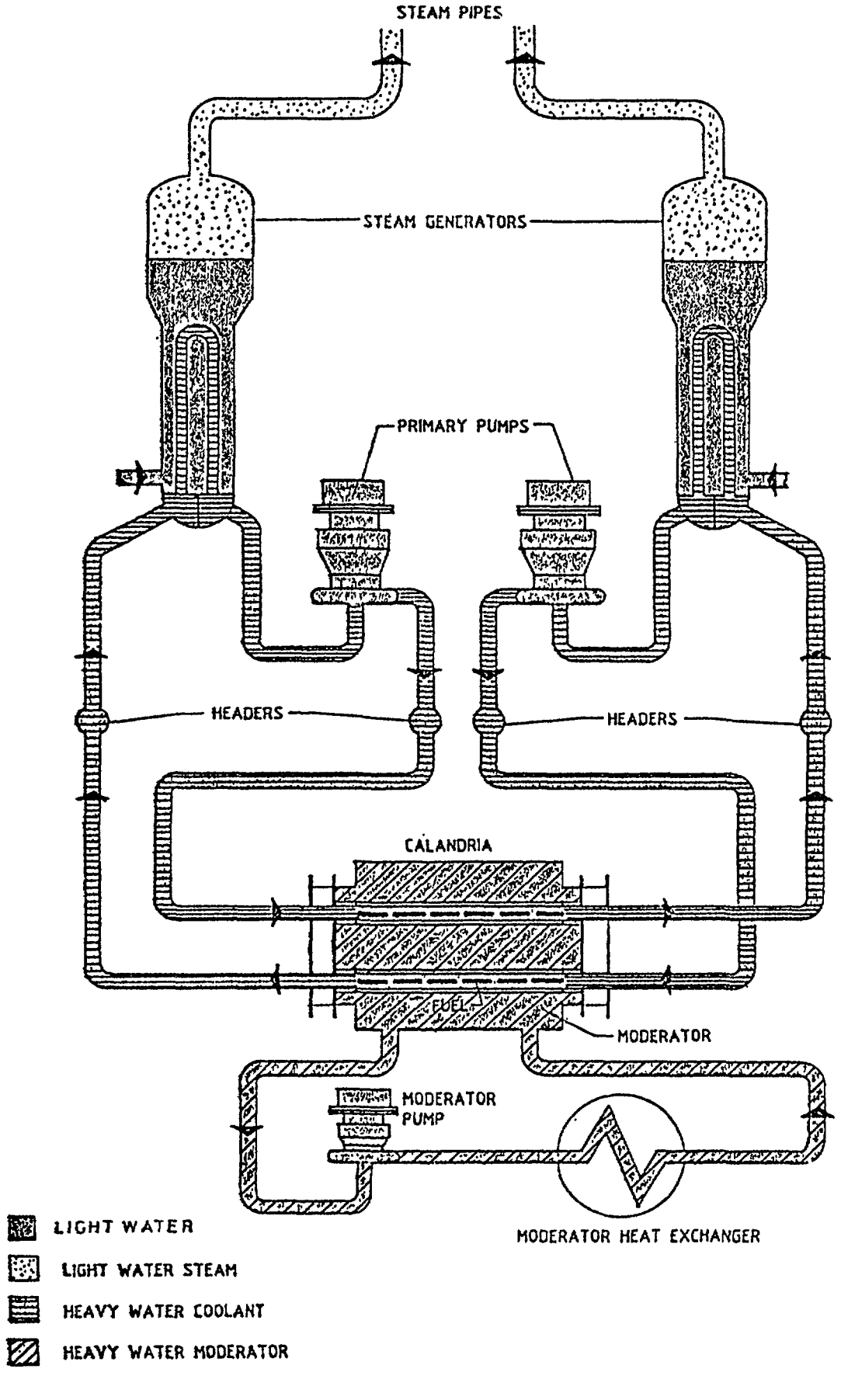


FIG. 1. PHWR simplified flow diagram.

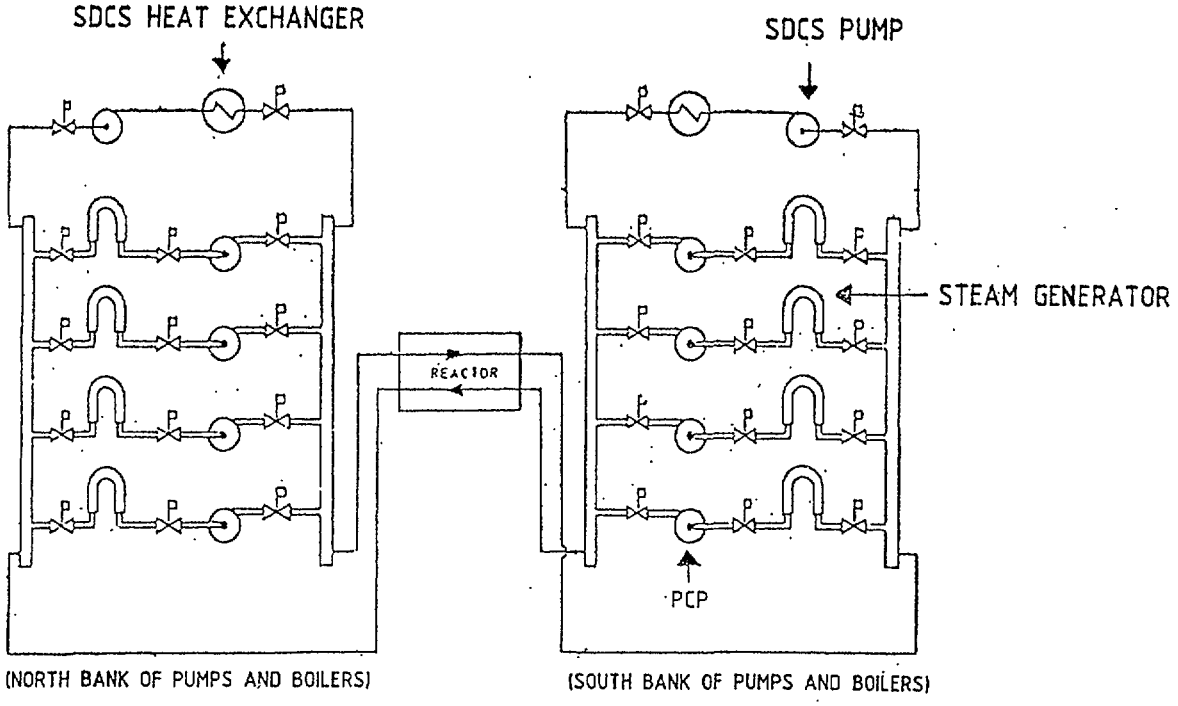


FIG. 2. PHT system schematic including shutdown cooling system (SDCS).

shutdown state (particularly long duration annual shutdowns), a large number of plant equipments could be unavailable over short/long durations, thus making the model developed for the PSA of full power operating mode only partially useful for shutdown risk analysis. There could be a large variety of equipment/plant configurations requiring operator intervention in many situations. This enhances the potential for human errors, which should be taken into account in shutdown risk analysis. However, the physical processes are, in general, much slower thus allowing considerable time for recovery before any core damage could occur. Such recovery actions need to be covered in the procedures developed for Human Reliability Analysis (HRA).

3.1 Dominating Initiating Events.

A preliminary PSA of an operating plant has been carried out recently. This includes the identification of Initiating Events (IEs) applicable to the design of the PHWRs at MAPS. Based on the analytical study of the identified Initiating Events (IEs) and the operating experience at the station, the following IEs are considered to be dominating for MAPS reactors, at power operation.

i) Loss of Coolant Accident (LOCA), particularly Medium Break LOCA
ii) Main Steam Line Break (MSLB)
iii) Feedwater System Failure
iv) Process Water System Failure
v) Compressed Air Failure
vi) Class IV (normal) Power Supply Failure

With regard to the dominating IEs under shutdown or low power operation conditions, while reactivity transients could be important, the contributions from MSLB, feedwater failures and

compressed Air failures are not significant. Thus, the dominating IEs identified as potential contributors to Core Damage Frequency (CDF) under shutdown conditions are as follows:-

i) Grid Power Supply Failure
ii) LOCA
iii) Reactivity Transients
iv) Process Water System Failures

A brief discussion of these IEs and the various Accident Sequences follows. In addition, the potential accident sequence during 'Header Level Control' operation, which is carried out when the maintenance of pumps, valves etc. in the Primary Heat Transport system is undertaken during a reactor shutdown, is also discussed.

3.2 Grid Power Supply Failure

During normal reactor operation, there are two independent sources of class IV power supply, namely (i) Station Generator, and (ii) Grid. When the reactor is shutdown, class IV power is provided by the grid system only. Hence, the probability of class IV power failure will increase and since the probability of failure of emergency Diesel Generators (class III supply) is same, the result will be a higher probability of Station Blackout. In view of the comparatively larger frequency of class IV power failures in the Indian context, this IE assumes a greater significance.

During long duration shutdown, the normal mode of cooling is through the operation of the Shutdown Cooling System which operates on the primary side with its two redundant loops of pumps, valves and heat exchangers (as shown in Fig. 2). In case of failure of class IV power and diesel generators (DGs), resulting in Station Blackout, forced circulation of primary coolant by shutdown cooling pumps will stop. Thermosyphon cooling of core with the help of steam generators is resorted to. However, emergency feedwater would also be unavailable and water is fed to the secondary side of the steam generators (SGs) from the Fire Fighting System (FFS) which operates with independent diesel engine driven pumps. However, the changeover from shutdown coolers to steam generators would necessitate: (i) Isolation of shutdown cooling system, (ii) Opening of PHT system valves, and (iii) Opening of valves in FFS, and a number of operator actions are envisaged. Because of the reasonably large SG secondary side inventory, considerable time is available. The probability of human error is low. Further, all the operator actions are rule/skill based, particularly in the operation of shutdown cooling and PHT systems. The Event Tree (ET) for the IE is shown in Fig. 3.

3.3 Loss of Coolant Accident (LOCA)

In PHWRs, with a large number of coolant channels and the associated feeder pipes, the probability of medium LOCA is somewhat high. In the case of standardised PHWRs (wherein the moderator is not dumped on a reactor trip), even LOCA coupled with the loss of ECCS is not likely to lead to fuel melting since the pool of cold moderator acts as a heat sink. However, in the case of reactors at MAPS, the moderator is dumped on reactor trip and a spray system is provided for cooling the coolant channels. During a cold shutdown when the PHT system pressure is quite low,

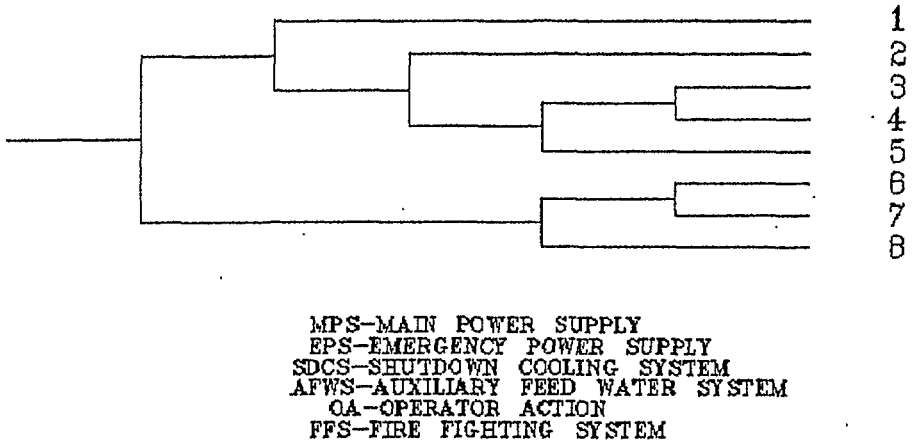


FIG. 3. Event tree following class IV supply failure.

ECCS may be bypassed. In case of LOCA under such conditions, the revival of ECCS would call for operator intervention involving opening of the ECCS injection valves from the control room.

3.4 Reactivity Transients

In the operating PHWR under consideration (MAPS), coarse reactivity manipulations involve moderator level changes in the core. During a shutdown, the moderator is dumped which introduces a large negative reactivity. Hence, the probability of a positive reactivity insertion offsetting such a large negative margin is practically non-existant. However, during startup, an uncontrolled moderator pumpup is a potential source of reactivity transient. The primary trip parameters in such cases are high lograte or reactor power > 1.1 times full power and if the Reactor Protective System function is assumed normal, the transient would be terminated without any significant effects. However, moderator pumpup transient followed by the failure of shutdown system could result in reactor power excursion. In the event of fast pumpup under certain conditions the coolant channel may rupture and the coolant will discharge into the moderator and the subsequent pressure rise will initiate dumping of the moderator and reduction in the neutron power. It has been assessed that if the containment isolation function is effective, there will be no consequences in the public domain. The probability of the IE, viz. the failure of the moderator level control system (2 out of 3 channel failures including common cause contribution), resulting in reactivity transient is about $1x10^{-4}$ /yr.

3.5 Process Water Failures

Process water system is an important support system which provides cooling for the moderator system, boiler feed pumps etc. during normal reactor operation, and for shutdown cooling system during shutdown. In case of process water system failure leading to loss of heat sink for shutdown cooling heat exchangers, a

provision has been made in the PHWR to inject Fire Water automatically into the heat exchangers. Thus, the accident sequence involves failure of process water and fire fighting systems. The fire fighting system comprises of 3 diesel driven pumps and 1 electrically driven pump and the availability of any one of the pumps would suffice in the shutdown state. A probability of failure of about $1x10^{-3}$ has been estimated for the FFS when 2 out of 3 pumps are needed. Under shutdown condition, a CCF involving all diesel driven pumps would be the dominant mode of FFS failure. In case class IV power is available, the electrically driven pump may be used. However, no credit has been taken for this in the computations. The frequency of this accident sequence leading to core damage is estimated to be about $3x10^{-5}$/yr.

3.6 Header Level Control Operations

Header level control is required during the maintenance of main PHT system pumps and valves. When the shutdown cooling system is in operation, it is permissible to have any or all of the main steam generator units empty. When the temperature is low enough, the suction connections of the primary coolant pumps (PCPs) may be drained and opened to permit maintenance of the pumps. The water level in the primary system headers may safely be taken down to the point where the pump isolating valves and the boiler inlet isolating valves may be opened for maintenance, without interfering with the operation of the shutdown cooling system.

The header level control operation is done after the PHT system has been cooled down to 55 deg. C and 24 hours have elapsed after reactor shutdown and the emergency diesel generator is in the operable state. Header level control operation essentially involves heavy water inventory control in the primary heat transport system without interruption of the decay heat removal function. The heavy water inventory control in this operational mode can be achieved with the help of any one operating shutdown cooling pump and by suitably throttling two valves (one each on the suction and discharge sides of the shutdown cooling pump) which control heavy water inputs from and to storage tank.

Failure under this operation would be mainly due to the following reasons:-

i) Failure of the shutdown cooling pump
ii) Class III (diesel generator) power failure

In case of header level control failure, a heavy water spillage will occur. There will be no primary coolant flow in the core. However, the fuel remains submerged and all feeders will be full. Thus, fuel temperature is not expected to rise much. Reasonable amount of time will be available before boiling occurs. It is important to realise that such maintenance activities are carried out under strict administrative control and adequate arrangements for blanking the opening can be promptly made. The operator would have reasonably adequate time to take the required mitigating action so that fuel damage can be avoided.

4. CONCLUDING REMARKS

Studies related to shutdown risk assessment of Indian PHWRs have been initiated. Dominating IEs under shutdown/low power operation are somewhat different and have been identified. The accident sequences have been examined and preliminary assessments have been made for an operating plant. Further studies are to be carried out.

ACKNOWLEDGEMENTS

The authors wish to thank Mr. Anil Kakodkar for useful discussions.

REFERENCE

1. S.P. Kalra and V.K. Chexal, Assessing and Managing Plant Risk During Shutdown Plant Conditions, Nuclear Safety, Vol. 32, No. 3, July - Sept. 1991.

INTERIM SHUTDOWN RISK PROGRAM

J.A. BECERRA, A. RODRIGUEZ
Comisión Nacional de Seguridad Nuclear y Salvaguardias,
Mexico City, Mexico

Abstract

The Mexican Regulatory Body and the National Utility have been implemented a PSA application for the Laguna Verde Power Station (U1). A risk based technical specifications is considering in an stepwise approach for this process the first step is a risk-based prioritization of the Allowed Outages Times (AOT) and the Surveillance Test Intervals (STI) from the Technical Specifications (TS). Some other applications are taking place, among them are; configuration control, maintenance prioritization, strategies to optimize AOT's STI's. In the mean time an operational event happened in the plant during full power, one train of the shutdown cooling system was taken out for maintenance for a longer period than the allowed by the current Technical Specifications. Thus through the PSA application program it was detected that the shutdown as imposed actually by the TS for this case is a condition of higher risk than the continued operation. Several alternatives are suggested in order to reduce the risk, among them are: additional test requirements, reliability programs, operators training, review of recovery procedures and configuration control.

INTRODUCTION:

The Laguna Verde Power Station (LV) has two units of the BWR/5 reactor type and Mark II containment. At present, Unit one has been subject to the second refueling and the Unit two is expected to be loaded with the first fuel at the end of the next year.

For Unit one a PSA Level 1 has been developed, a peer review and update process is underway. Additionally a PSA application program has been initiated between the regulatory body (CNSNS) and the national utility (CFE) by a supported program with the IAEA ().

The PSA application program was initiated with the risk important prioritization for all events considered in the Laguna Verde PSA.

A risk-based Technical Specification (TS) program has been initiated with the Allowed Outage Time (AOT) and Surveillance Test Interval (STI) prioritization.

As a result of the risk-based AOT prioritization have been defined three risk classes: among the class 1 are the risk significant events, and some of the critical ones are the high pressure spray system events and the shutdown system events; for risk class 2 and risk class 3 we have respect moderate to marginal contributors and marginal to insignificant contributors.

Lost of the shutdown cooling system (one train) is identify as a major contributor to the risk, and is a major safety concern inside the regulatory body and some members of the utility staff.

A refueling process or controlled shutdown with a one shutdown cooling loop unavailable are expected to significant increase the risk level of the plant.

PRESENT TECHNICAL SPECIFICATIONS

The Laguna Verde Operational Technical Specifications (OTEs) are based in generic OTEs. For the shutdown cooling is allowed to

operate with one out of the two trains for 72 hours for repair or test and maintenance otherwise, the reactor has to be in a cooldown condition in less than 24 hour.

During full power operation a 7 days extended AOT was required by the utility in order to deal with repair activities because a high conductivity was detected up stream the RHR-B heat exchanger.
At the time of shutdown cooling event a PSA application program for Technical Specifications was underway and the exception could not be granted, thus with our calculation the risk-based AOT would be 5 hours or less and some alternatives were identify using the PSA application program. Among the alternatives are configuration control, reliability program, the review of recovery procedures, operators training, and promoted a PSA level 1 for shutdown an low power conditions.

RISK-BASED OTES

The Allowed Outage Time (AOT) and the Surveillance Test Intervals (STI) are two issues that can be treated with probabilistic technics. The risk-based AOT could be calculated by using the PSA Level 1 results like the importance calculation.
For the shutdown cooling heat exchanger when it is down the associated risk contribution is assessed with the repair downtime and the risk increase:
For Laguna Verde (1) NPP , at present

Baseline risk = 1.0E-4/reactor year
dC_i = Risk increase
= Risk when the component i is downed - baseline risk
AC_d = Risk contribution
= Risk increase*downtime = dC_i*d
T(years) = T(days)/8760

for the heat exchanger RHR-HX001-B, dC_i = 1.6E-3/yr:

Case of 3 days AOT (72 hrs)

$$AC_d = 1.6E-3*72/8760$$
$$AC_d = 1.3E-5$$

The Figure 1 shows the risk increase when a train is out of service during full power operation, also shows the risk contribution due to an AOT of 3 days
Nevertheless the shutdown risk was not calculate for this configuration the risk increase during shutdown is expected to be greater than the risk increase for one shutdown cooling train down, as is shown in the figure 1 for the shutdown sketch.

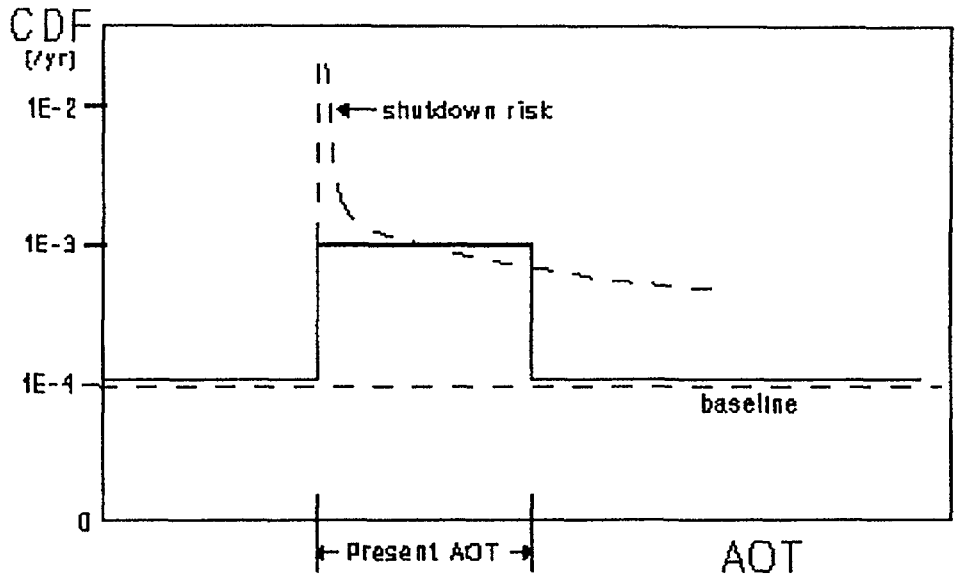


FIG. 1. Risk increase for the AOT (case of 3 days).

For an extension of the AOT required by the utility the risk increase can be also calculated but has to be compared with the risk criteria.

Case of 7 days AOT (168 hrs)

$$AC_d = 1.6E\text{-}3*168/8760$$

$$AC_d = 3.1E\text{-}5$$

The Figure 2 shows how the risk contribution is increased for an extension of the AOT to 7 days during full power operation. There is no change in the risk increase.

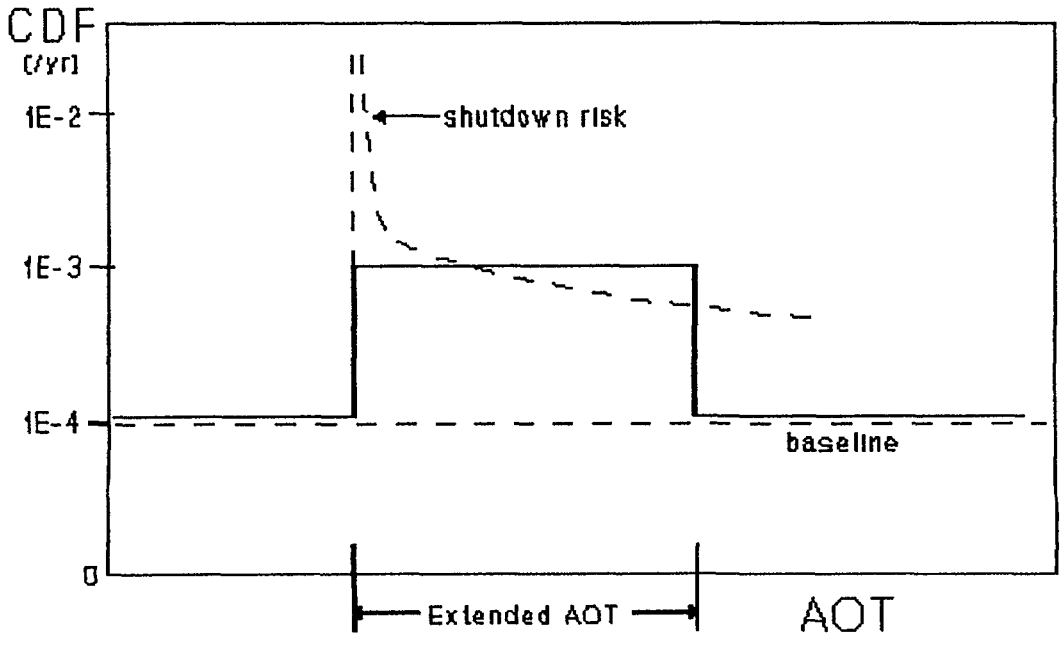


FIG. 2. Risk increase for the AOT (case of 7 days).

For Laguna Verde the risk criteria has been selected as the 1% of the baseline risk; 1% of the risk is taken to account the uncertainties and the cumulative risk for the safety function. Using this criteria is possible to calculate the downtime based in risk consideration.

$$\text{with} \quad AC_d^* = (1\%) * 1.0E\text{-}4 = 1.0\ E\text{-}6$$

$$d^* = 5hr$$

For an acceptable risk contribution 1E-6 the risk-based downtime (AOT) should then be less than or equal five hour and the present AOT is one order of magnitude different; see Table 1. In order to carry on any maintenance or repair activity in a shutdown cooling train and keep the risk contribution low some other alternatives are suggested.

TABLE 1.

AOT CONDITION	AOT	AC_d	SHUTDOWN RISK CONTRIBUTION
Present	3 days	$1.3x10^{-5}$	$>1.0x10^{-4}$
Extended	7 days	$3.1x10^{-5}$	$>1.0x10^{-4}$
Risk-based	5 hours	$1.0x10^{-6}$	$<=1.0x10^{-6}$

AOT ALTERNATIVES TO REDUCE THE RISK

Additional test requirements could be selected further remaining shutdown cooling loop to make sure that would be available if it is required. Configuration control management based in the cutset approach can be used, to find events in the same cutset, thus the risk contribution can be reduced by testing those additional components in the cutset. See Figure 3.

INTERIM REGULATORY POSITION.

As a result of this preliminary study inside the regulatory body is suggested an interim shutdown program:

Additional Test Requirements: For a refueling on any controlled shutdown additional test an the preferred shutdown cooling train should be carry out. Additional test requirement could be selected further remaining shutdown cooling loop to make sure that would be available if it is required.

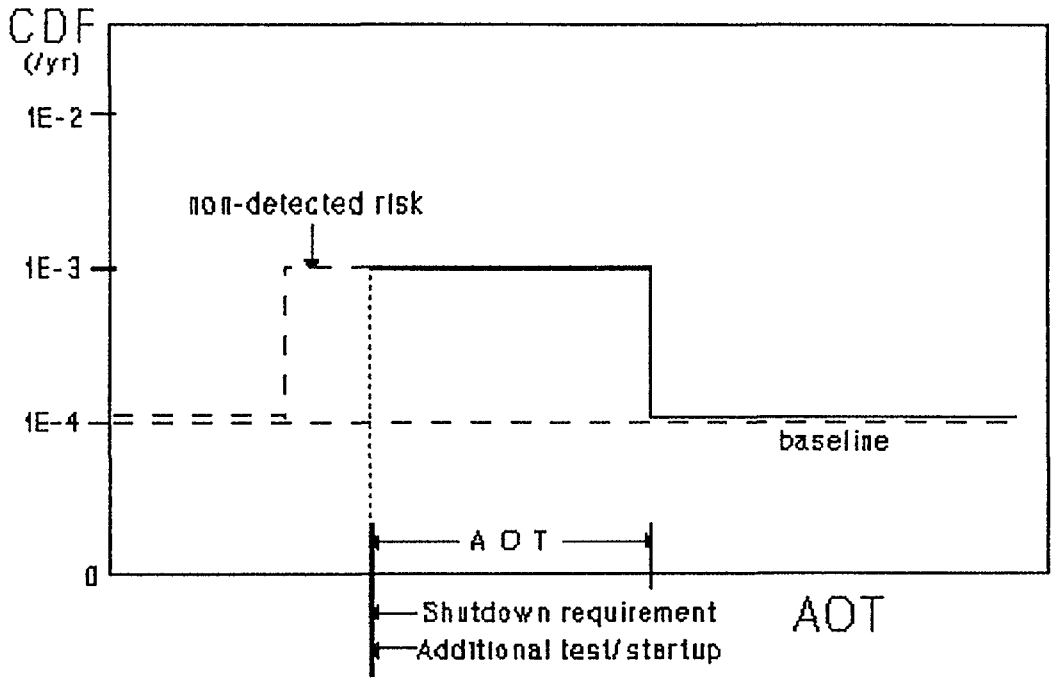


FIG. 3. Risk increase for the AOT (additional test requirements).

Reliability programs: For selected support systems are advised on to an reliability of those systems which are support to the shutdown cooling function of the reactor like the Service Water System, the instrument air, Diesel Generators.

Operator training: Operators should be aware of the risk increase during refueling or any shutdown activity through additional procedures, training in the operator reactor simulator, and PSA advise.

CONCLUSIONS

The critical event of shutdown with the shutdown cooling systems degraded can be diminished by executing appropriate actions.
For the remaining shutdown cooling train, surveillance tests were executed in order to assure the availability of the system.
For every programmed or requested shutdown activity it is recommended to reduce the time of surveillance test intervals in order to have available the preferred train for the shutdown.
In case of another event in the shutdown cooling system in which the required maintenance would time be greater than the AOT from the technical specifications is recommended to identify by mean of the Configuration Control all the risk contributors within the same cutset, in order to reduce the total risk of core damage.
The regulatory body has suggested an interim program to diminish the risk during events of plant shutdown or low power operation and is promoting in the development of a PSA of this nature.

REFERENCES

1) T. Mankamo, I.S. Kim & P.K Samanta, "Risk-Based Evaluation of Allowed Outages Times (AOTs): Considering Risk of Shutdown". Technical Committee Meeting Advances in Reliability Analysis and PSA; Budapest, 7-11 September 1992.

2) D.W. Whitehead, B.D. Staple, T.D. Brown, "Status of the Low Power and Shutdown Accident Sequence Analysis Proyect for the Grand Gulf Nuclear Power Station"; Sandia National Laboratories. 1992.

3) J.A. Becerra & J.L. Delgado, "Stepwise Approach for a Risk-Based Technical Specifications"; National Commission of Nuclear Safety; México. Technical Committee Meeting Advances in Reliability Analysis and PSA; Budapest, 7-11 September 1992.

4) W. Vesely, "Workshop on PSA Applications"; Laguna Verde, Ver. México. Octubre 1992.

METHODS USED AND RESULTS GAINED FROM SHUTDOWN ANALYSES AT VATTENFALL NPPs

L. BENNEMO, A. ENGQVIST
Vattenfall,
Vällingby, Sweden

Abstract

Barrier analysis methodology and its use to assess the risk in shutdown is analysed. The results of a PSA for shutdown which was performed by Framatome for Ringhals 2 NPP are discussed. The results of the barrier approach and PSA are compared and a possible combination of the two approaches proposed.

1 INTRODUCTION

Traditionally, safety analyses have been focused on operational modes with critical reactor and large power output. In recent years, however, an increasing interest has been focused on the shutdown mode.

At Vattenfall, a method using a barrier analysis technique has been developed and tested in two cases. Furthermore, a limited PSA analysis has been performed by Framatome. This paper describes the methods and the most important results from the analyses.

2 BARRIER SHUTDOWN ANALYSIS METHOD DESCRIPTION

Briefly, the method can be described as an analysis of the amount of barriers and their strength against a number of chosen undesired events.

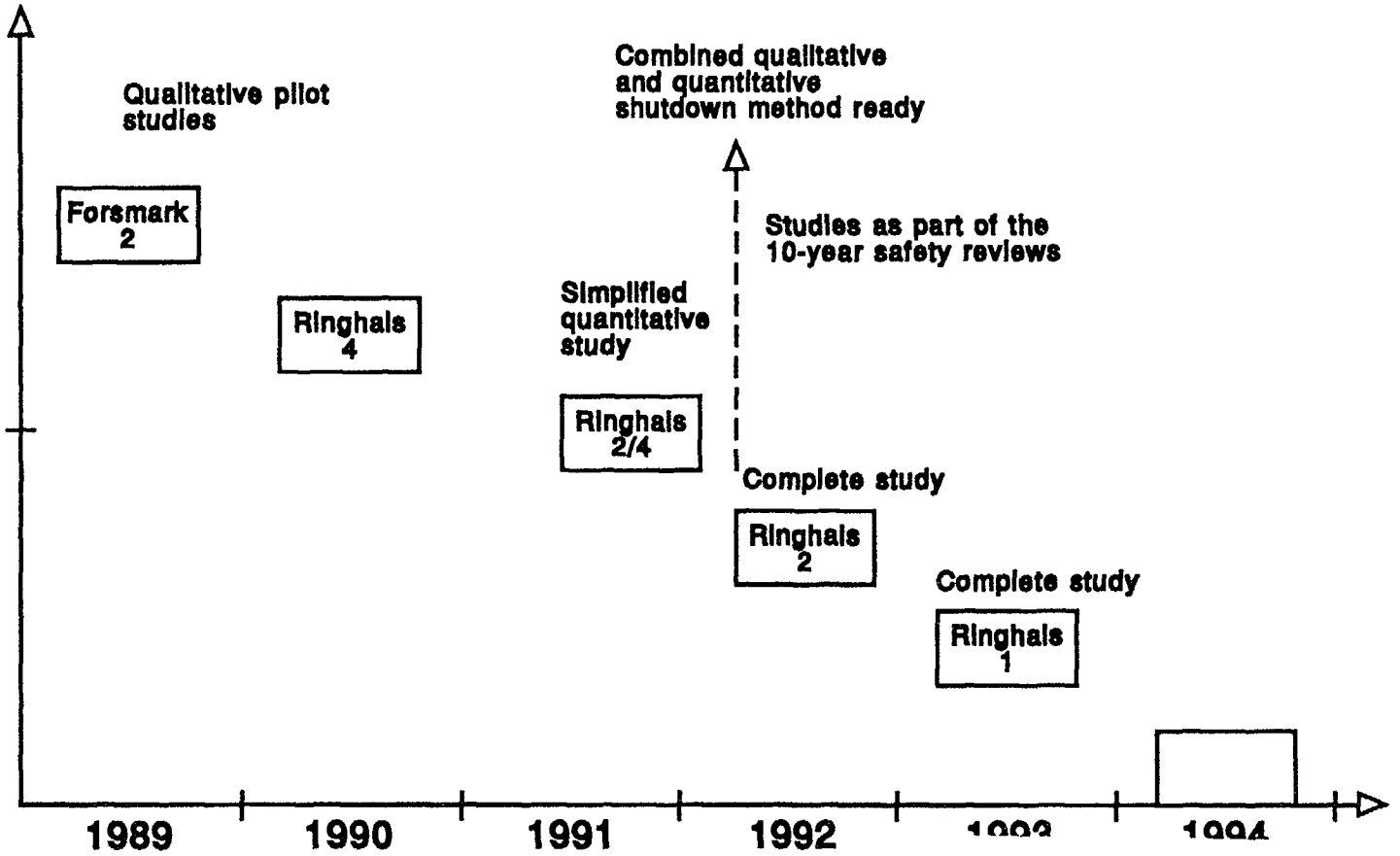
The purpose of the analysis is to assess the safety margins against a number of undesirable events. The result is a qualitative judgement based on the number of barriers and their strength.

The analysis is carried out in three steps; preparation, observation with collection of data and evaluation. In the preparation step the most critical work sequences during the outage are identified and selected for analysis. The observation step is performed during the shutdown period, where the selected critical work sequences are followed and data collected. In the final step, the evaluation, all the information obtained is analyzed and conclusions are drawn with respect to available safety barriers.

Examples of undesirable events are:

- Primary system leakage
- Criticality
- Cold pressurization of reactor pressure vessel
- Cold pressurization of steam generator
- Deviation from TS
- Refuelling accidents
- Personnel injuries

SSPB Cold Shutdown Analysis Method Project



The concept of "undesirable events" also includes actions which may not lead to an accident, but disregards available technical specification rules for sufficient safety margins. To perform critical tests with the shutdown system inoperable would be one example.

B/T-diagram

To show the barriers for each undesired event during different phases of the outage, barrier time diagrams are created. On the y-axis of the diagram there is a list of the different physical and administrative barriers against the identified undesired event and on the x-axis of the diagram the time is shown. By comparing the B/T-diagrams for the undesired events for the different work sequences, the most critical sequences can be selected.

The barrier method gives the basis for estimation of the qualitative safety margins with respect to a specific undesirable event. The evaluation also has to consider the seriousness of the consequence of the event.

Straight recommendations based on the results of the barrier analysis should be supplied with the analysis. The recommendations are to be prioritized according to the assessed strength of the barriers and the judgement of the analysis group.

3 LIMITED PROBABILISTIC SAFETY ANALYSIS METHOD DESCRIPTION

The Ringhals 2 PWR PSA study for the shutdown mode has been performed by Framatome.

The purpose of the limited probabilistic safety analysis of the shutdown mode was to assess the risk and to identify the most critical sequences.

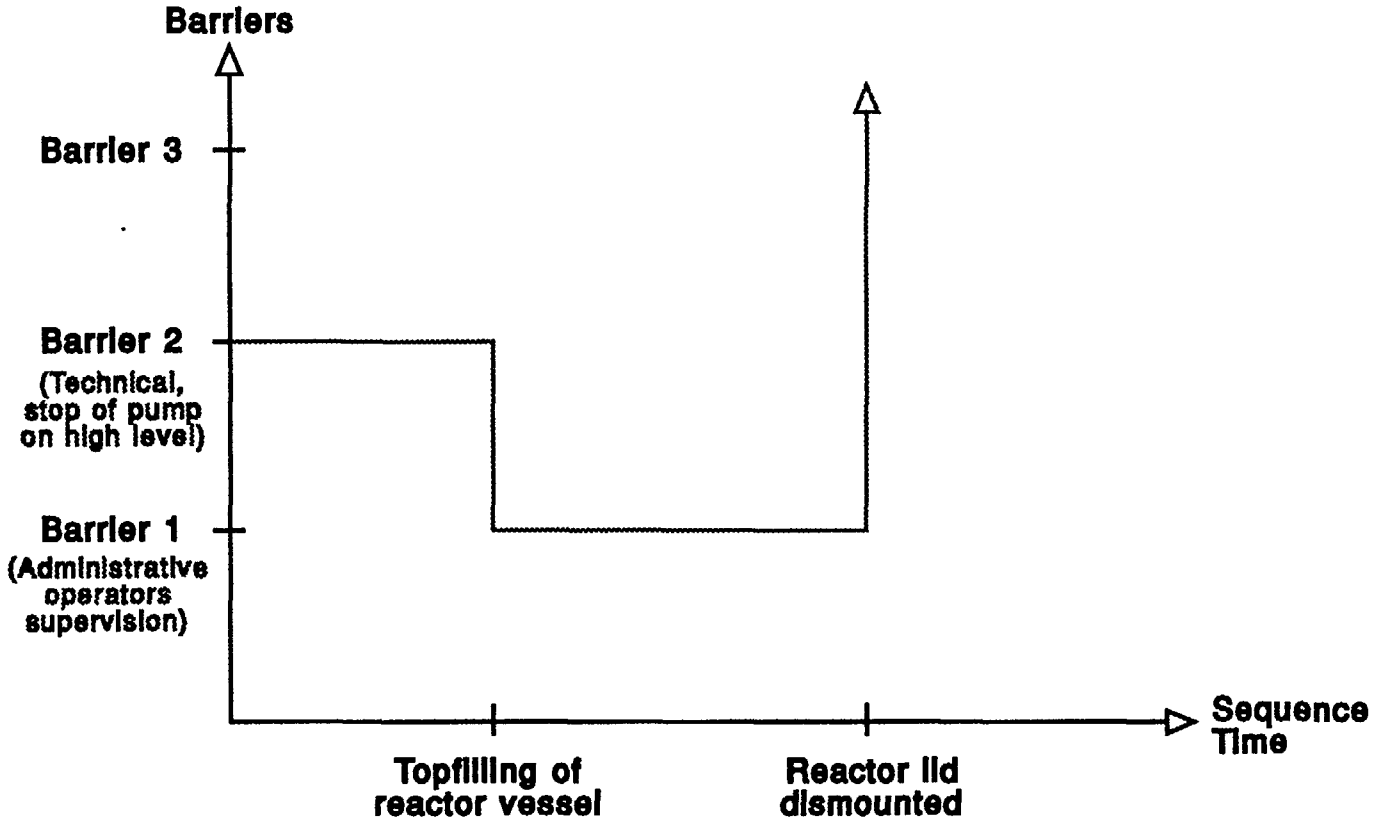
The modes for which the analyses were performed are the following:

- Hot standby (mode 3)
- Hot shutdown (mode 4)
- Cold shutdown (mode 5)
- Static shutdown (mode 5*)
- Refuelling (mode 6)

The accident sequence analysis is performed by means of event trees. The trees are quantified starting from the analyses performed in Ringhals 2 PSA for power operation.

The initiating events considered in the study were (Based upon international experience and the results from the earlier barrier analyses):

- Loss of the RHR system
- Loss of coolant accidents
- Reactivity incidents due to inadvertent dilution
- Cold pressurization of the reactor vessel
- Cold pressurization of the steam generator
- Refuelling incidents



Example: cold pressurization of reactor vessel (BWR), in the sequence when the reactor lid is dismounted)

Framatome also classified the consequences associated with each sequence into the following categories, according to expert judgement and existing analyses:

- Severe safety consequences
- Significant safety consequences
- No significant safety impact but public opinion impact
- No significant impact

An example of a severe safety consequence is an unscheduled level drop with no operator action before core uncovering.

A significant safety consequence is for instance an unscheduled level drop with operator action before core uncovering but no containment evacuation within stipulated time limit.

If you drop a spent fuel assembly inside the fuel building but makes a successful evacuation and ventilation isolation it is considered as a public opinion impact matter.

Finally a jamming of a spent fuel assembly inside the gripper tube mast, followed by an operator action to unjam the assembly without dropping it is an example of an event with no safety impact.

All accidents leading to the first three consequences above has been quantified.

Quantifications have been performed starting from the reliability data bank and the reliability system analyses used in the Ringhals 2 PSA for power operation. Also French and international data was used if no specific Swedish data were available.

4 RESULTS

Results from the barrier method

So far two shutdown analyses have been performed using the barrier method: the first in 1989 at Forsmark 2, an ABB Atom 1000 MW BWR with internal circulation pumps, the other in 1990 at Ringhals 4, a Westinghouse three-loop 900 MW PWR.

Examples of findings were:

-Before dismounting the cover lid of the reactor pressure vessel, top filling is performed using the high head auxiliary feedwater pumps. These pumps have a pressure head far above 1 MPa, which is the maximum allowed pressure in this mode. The safety barrier for preventing over pressurization is purely administrative and consists of the supervision by the control room operators. It was recommended to add a technical barrier by using the low head auxiliary feedwater pumps.

-During maintenance of the internal recirculation pumps work is performed during a six hour period in which leakage from the loops is prevented by one single mechanical barrier only. Accidentally removing this barrier, consisting of a sealing lid, could cause a loss of coolant from the vessel at a rate of 500-700 kg/s. Adding safety barriers by introducing means to protect the sealing lid and to reduce the consequences of a leakage will increase the safety margins.

-During mid-loop operation with open steam generators and ongoing mounting of the nozzle dams, the equipment hatch of the containment is allowed to be open. If residual heat removal is lost, the estimated time to boiling in the core is 15-20 minutes. It was recommended to keep the equipment hatch closed in this mode in order to have the containment barrier intact.

-The mounting of nozzle dams must be performed in the right sequence. The last nozzle dam must be mounted on the hot leg. If the order is reversed combined with loss of residual heat removal a steam bubble can be formed and press water out of the core. The safety margins were improved by making the administrative barrier when mounting the last nozzle dam more strict i. e. improving the communication between the control room staff and the personnel working with the steam generators.

The recommended modifications have been implemented at the plants and the work procedures for the outage revised accordingly.

Results and dominant contributors from the limited PSA method

The results of the analysis gave, with conservative assumptions, the following overall annual frequencies:

- severe safety consequences: $<= 7.6 \times 10^{-4}$/year
- significant safety consequences: 1.9×10^{-3}/year
- public opinion impact consequences: $<= 3.2 \times 10^{-2}$/year

The main contributors for sequences leading to severe safety consequences were judged to be:

Loss of RHR in mode 5* (mid-loop). $2{,}5 \times 10^{-4}$/year
Failure of operator action before
core uncovering.

Small LOCA in modes 4 and 5. $1{,}5 \times 10^{-4}$/year
Failure of operator action before
core RCS level drops under mid-loop.

Spurious SI in mode 3 · $1{,}2 \times 10^{-4}$/year(*)
Failure of operator to stop SI and
rupture of reactor vessel due to PTS.

(*): Estimated with a value of conditional probability of rupture of reactor vessel assumed equal to $p = 10^{-2}$.

The high value of the figures are connected to dominant contribution from human error and from the estimated risk for reactor vessel rupture when cold pressurized.

Better procedures and new calculations for the risk of reactor vessel rupture will lower the figures considerable.

The analysis has resulted in a reviewing and rewriting of the operating procedures.

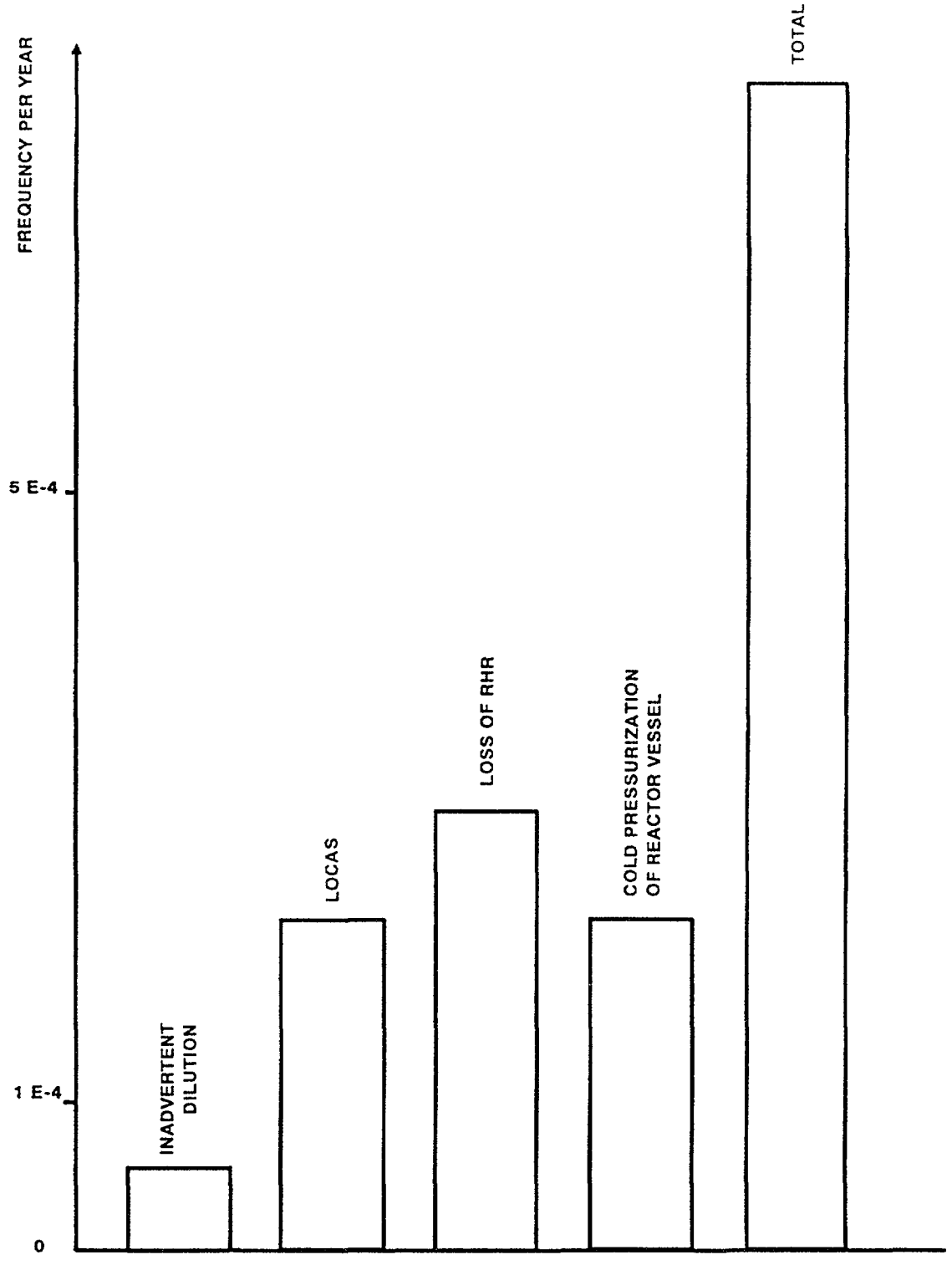


FIG. 1. Comparison of sequences leading to severe safety consequences by initiating events.

5 FURTHER DEVELOPMENT

Results obtained so far indicates that the barrier method combined with PSA technic will with reasonable confidence discover weaknesses during the outage.

Accordingly Vattenfall will continue the development of the shutdown analysis method as a part of our 10 year safety reviews. The approach for the coming studies will be to start with a limited PSA analysis and thereafter complete the shutdown analysis with a barrier analysis based on the results from the limited PSA.

OVERVIEW OF SAFETY MARGIN TOOL, STATUS IN PLANNING

R. HÄUSERMANN
Kernkraftwerk Leibstadt AG,
Leibstadt, Switzerland

Abstract

The objective of safety management changed at different stages in plant lifetime and as new methods and approaches became available. The improvement in safety management should be done through a learning process with effective experience feedback. Several steps for the safety management process are discussed including the goals for safety management, the strategy and the methods needed to keep in line with the strategy. Finally, the overview of the status of implementation of the concept at Leibstadt NPP is given.

1. INTRODUCTION

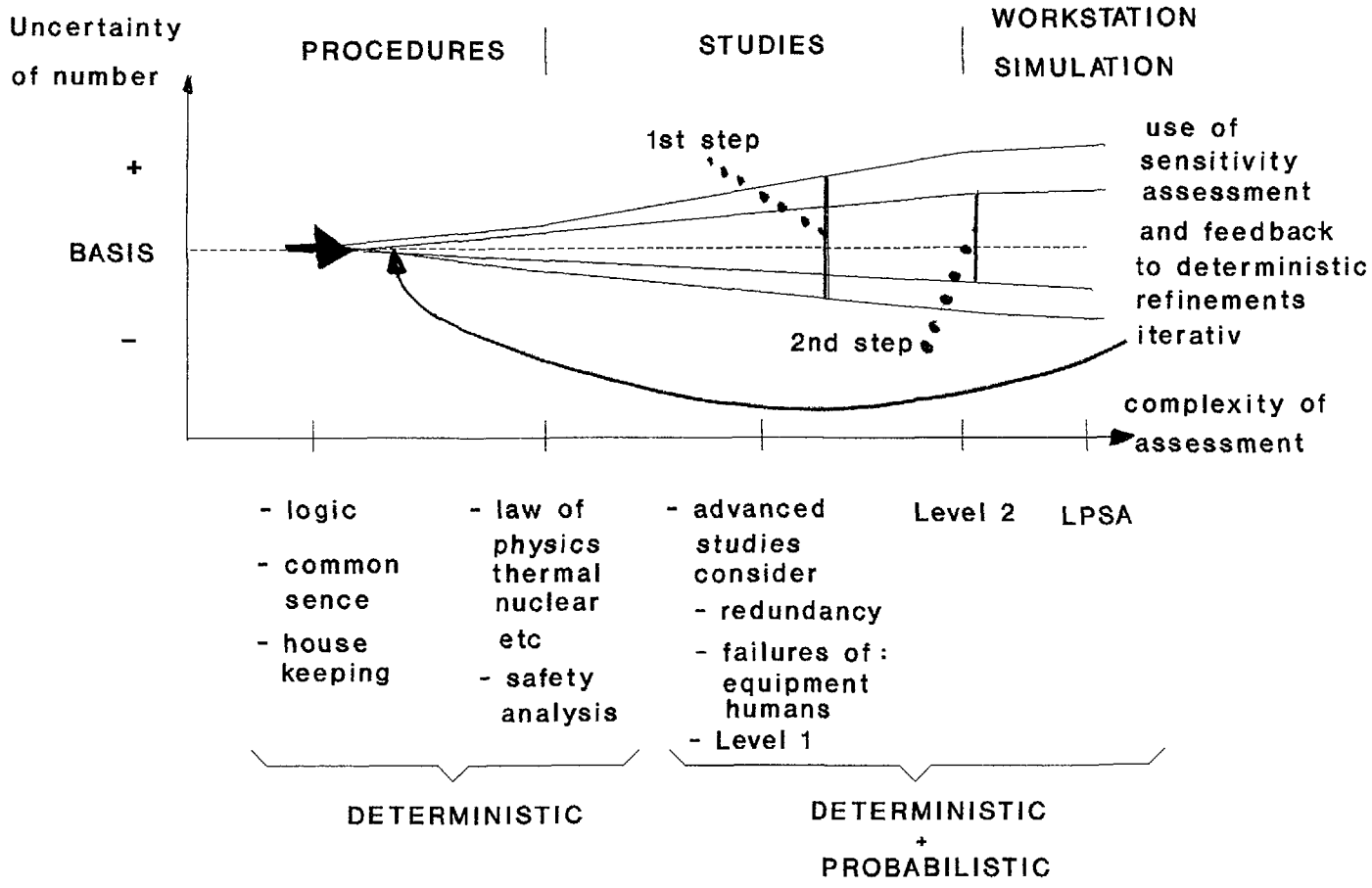
This paper is based on previous IAEA publications (see Ref. 1 - 3).
The differences in safety management methods are considerable when looking at the starting point of the first commercial operation. The progress is significant. In the Overview the key steps are shown. The point s that the assessments on safety are interactive on deterministic and probabilistic methodology. Procedures used for the plant-management are deterministic instructions for successpaths. The competent team: Must understand the procedures without asking about everything.

Management methods prove to be effective as long as they are used in practice with personnel always keeping the plant's quality needs in mind. The management system must be workable, understood and have a built-in flexibility, such that motivation is not ruled out by perfectionisme. It is geared to clear instructions, controls and corrections. The latter however must be the exception.

It is worthwhile to mention that there is always room for improvement through a LEARNING PROCESS (see Fig.1).
The "First time" is indicative for the situation with no specific experience available to perform correctiv actions. For a control engineer it is clear that deviations from an actual process value (IS) to an achievable value (SHOULD) are used to correct the process by FEEDBACK of the deviation. It took a while to have an agreement on the detail goals (SHOULD) and the methods to measure the actual status (IS) by adequate performance indicators. Each member of the crew had its own past professional experience and methods in achieving good results. To integrate the experience into the KKL-needs without neglecting new helpful practical ideas, was a demanding managerial task. All the tasks are performed under ALARA (As Low As Reasonable Achievable) criteria and industrial safety principles.

The paper describes the use of the "Safety margin tool" which is considered an additive to the existing decision making tools.

Deterministic-Probabilistic
Approach to assessments



Overview

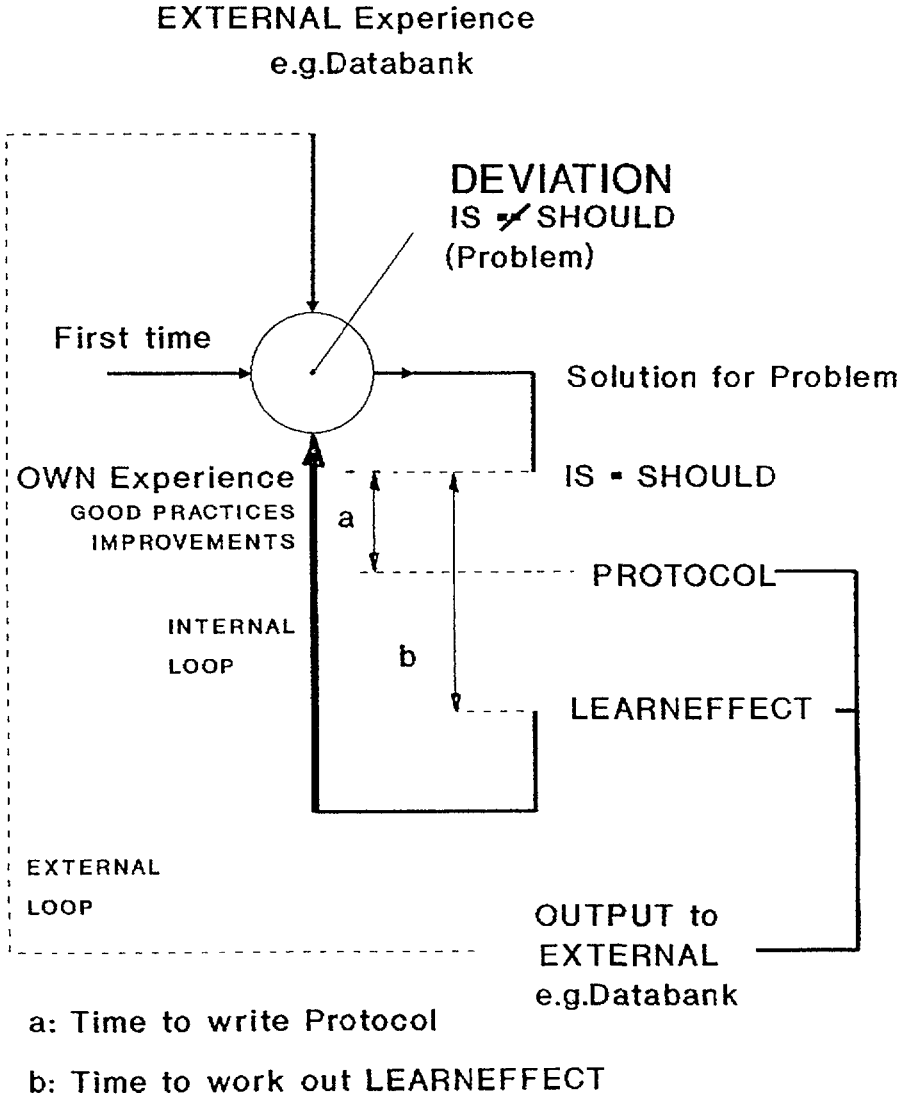


FIG. 1. Control loop for experience exchange.

2. GOALS FOR SAFETY MANAGEMENT

The key-goal is to maintain as much as possible of the availability-margin for all the mechanical and electrical equipment. This will increase the chance of continued operation even in the case of unexpected equipment failure or operational error. This is to ensure safe energy production in accordance with procedures and at the requested load program (ordered by the load dispatcher). KKL is in a situation that the electricity demand is the highest in winter i.e. the highest reliability of the plant during that time period is required.

Other important goals were set prior to plant start up. These included: **high safety, high plant availability, high thermal performance, low personnel accident rates, low doses, small amount of waste and all this cost effective.**

For all of those goals an approach as shown in Figure 2 was chosen. Important was to have a control mechanism to detect the deviations (ΔQ) from the desired results so that the adequacy of the implemented methods and procedures could be determined. Deviations from the desired results can be twofold:

-Methods are not properly understood by the user
-Methods are not adequate.

In KKL we had to iterate and perform corrections in both areas. The time involved for training and convincing the users of the necessity to adopt the common KKL approach was underestimated. The deviations however were discovered quite quickly and in the learning process corrected.

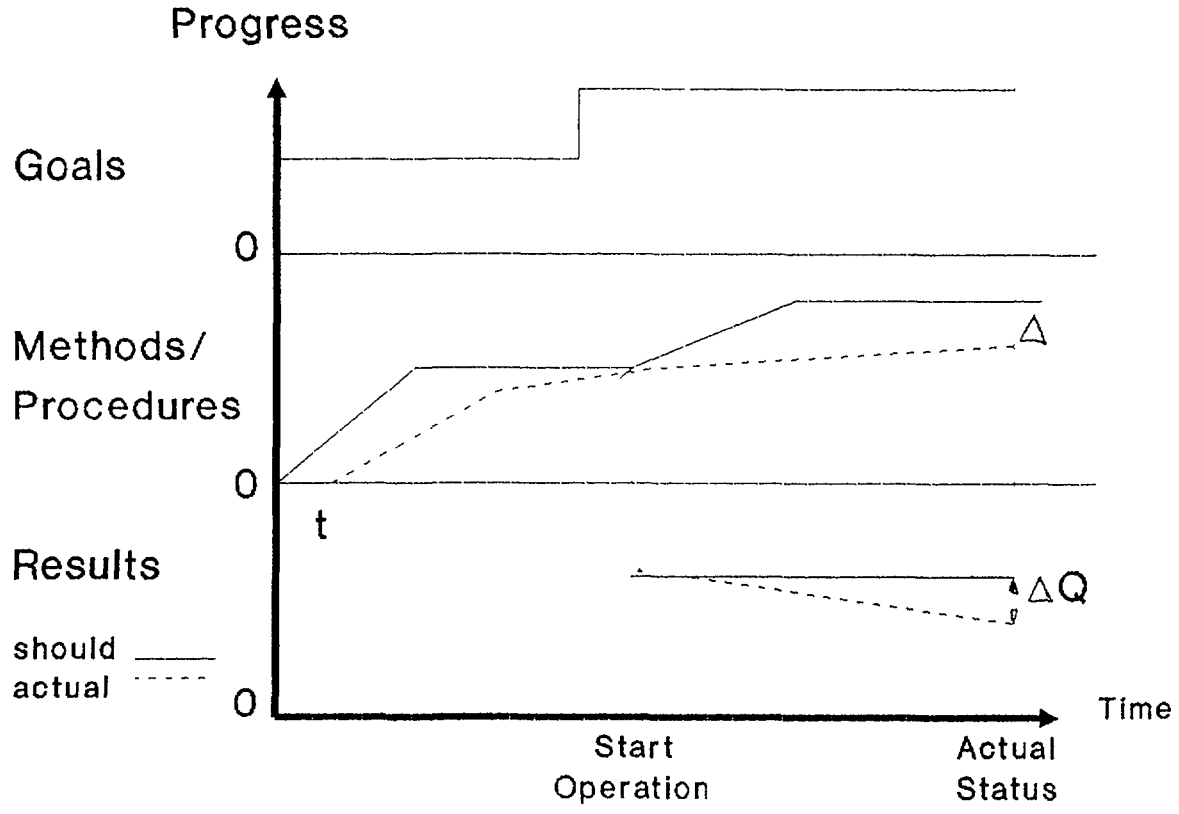


FIG. 2. Goals, methods/procedures and results (time dependent/interactive).

3. STRATEGY FOR GOOD PERFORMANCE

The most straight-forward strategy in any undertaking is geared to cost-effectiveness without neglecting safety. It was a challenge, as depicted in Figure 3 to look into areas where unnecessary costs would occur during the production as a result of inadequate preparation of management procedures and training of them during the project phase. The operating procedures were tested on the simulator by the operators. The maintenance and shop-procedures were tested by our employees in doing work for the contractors at the site with our own work- and safty-tagging system and billing the contractors for material and workhours.

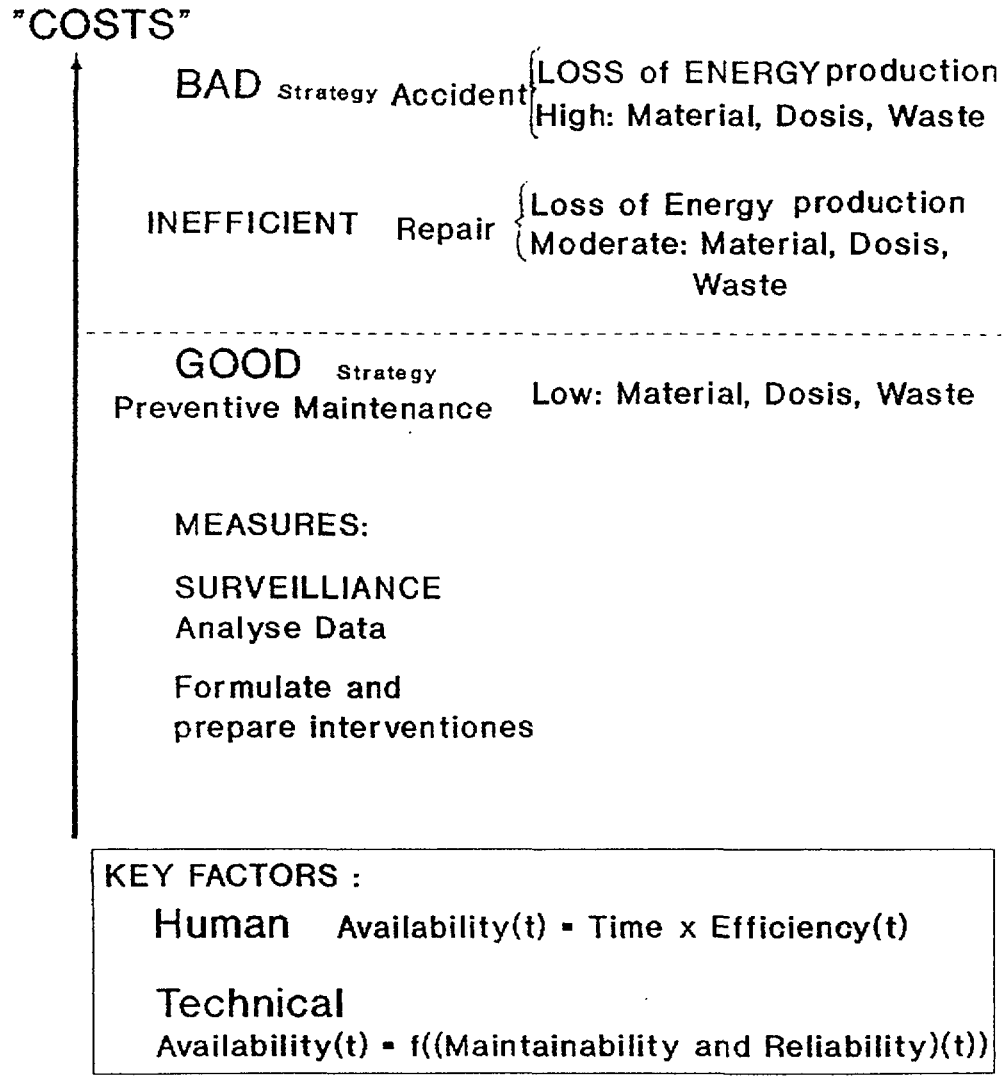


FIG. 3. Performance strategies; status dependent "costs".

In Figure 3 the definition of the human- and the technical-availability is given as both together (synergetically) are part of the strategy. Availability defined in that form is a measurable performance indicator. This beeing the case, the role of a workable organisation and management structure by efficient employees becomes evident in the overall strategy.

How could this be brought in line with the above depicted safety goals? A thorough analysis revealed that if the availability strategy for production systems is also applied to the safety systems and keep them in a state of readyness, both objectives are satisfied: **Safety and production** controlled by qualified (efficient) humans, composed to teams, prepared to share work and responsability.

The systematic analysis of incidents and accidents in the nuclear industry (precursers) allowed KKL to build up an organisation to keep similar incidents low. In other words KKL was in a position to learn from the experience made by others, and make things right from the plant start-up.

Refering to Figure 2, the management monitoring tools must show deviations Δ Q quick enough to perform fine improvements.

4. METHODS TO KEEP IN LINE WITH STRATEGY

The generic Figure 2 was applied for all the important performance factors. Adequate methods for each factor were defined, data collection methods introduced and the results displayed in tables and/or trends. The goals are compared to the achieved results.

Figure 4 shows the status dependent main groups of plant activities. The breakdown is quite coarse, reflects however the plant status which require special procedures.
Note: the status Refueling/Outage the topic of this meeting.

Figure 5 shows a generic detailed Plant Management flowchart. It is the practice that in more than one module simultaneous work activities take place. Note the importance of the LPSA in the graph as a "safetynet" for work which can be planned.

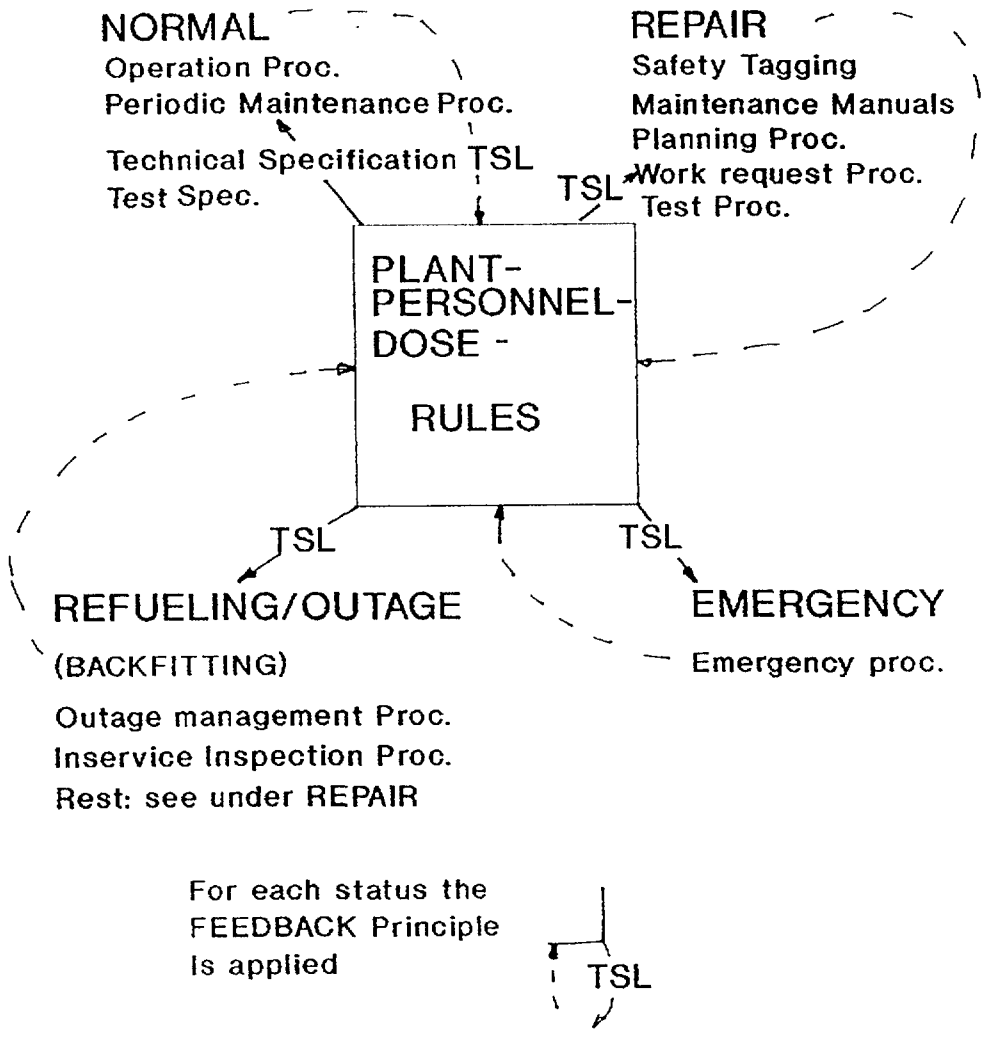


FIG. 4. Status dependent procedures; normal, refueling, repair, emergency.

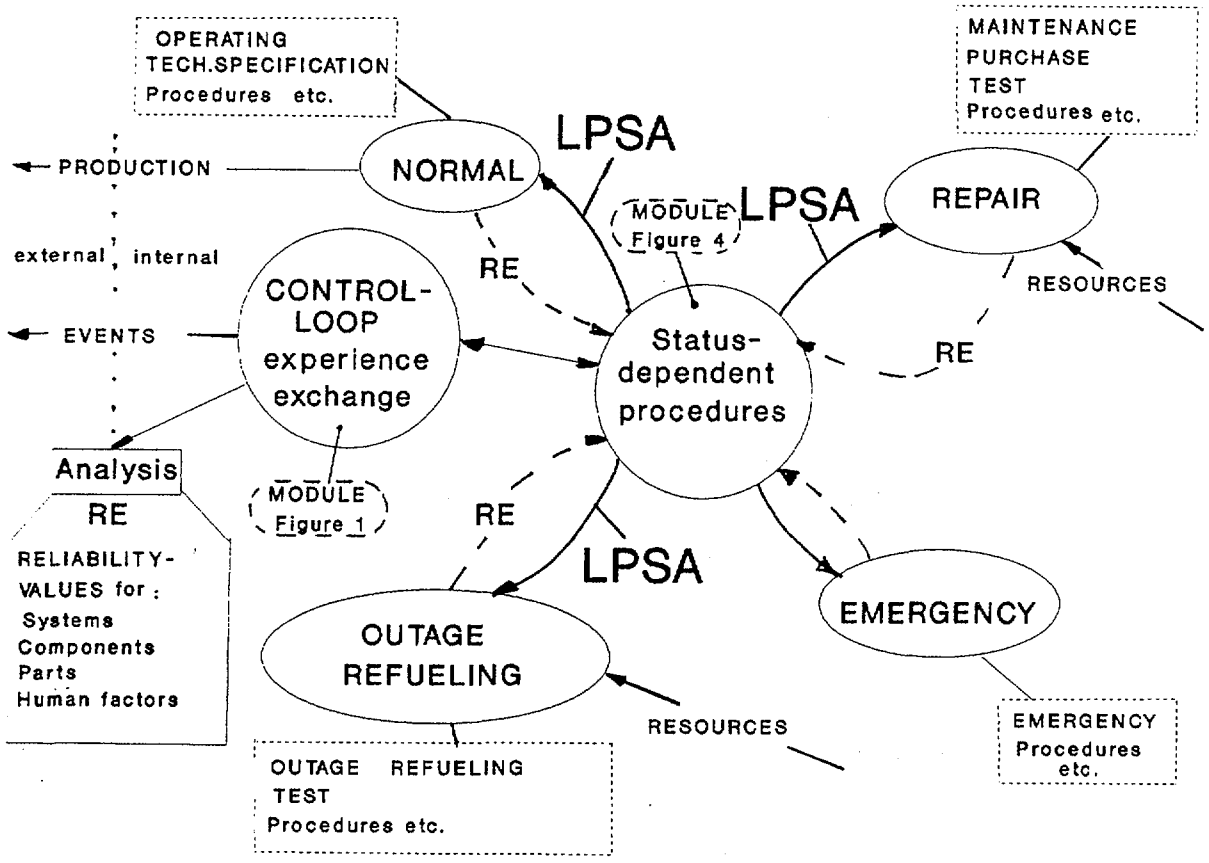


FIG. 5. Plant management, generic.

The findings of all the activities are reviewed, analysed and stored in accordance to Figure 1. This will include low risk configurations for preventive maintenance and testwork.Good practices are considered those which gave results as planned, others are stored as learning elements which have to be improved (See internal loop). Findings which are reportable to the authorities or into an operator- (e.g.WANO) or supplier-feedback-system are fed into the external loop.

Good practices for one module : REFUELING / OUTAGE are summarised in [4].

5. KKL OVERVIEW

In spite of the progress described above some areas remain in need of further attention:

We have learned that only with a well maintained technical installation good or excellent results can be achieved. The fundamental understanding is tought in lectures on "Maintainability engineering". The Figures 6 and 7 give in a brief form a summary of the relevant PSA input-data.

KKL has decided to improve the PRA tools and will introduce a LIVING-PRA model at the site as a workstation (see Figure 8).

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. With this workstation we intend to determine the Safety Margins M(A) in respect to the TSL (Technical Specification Leibstadt) and to the limits defined with the realistic success criteria M(tech) (see Figure 9). Figure 9 shall be considered the generic strategy where not yet all the numbers are available.

The plan on how to take full advantage of the LPSA is shown in Fig. 10.

During the safty-tagging procedure it will be possible to investigate the LPSA-Model for components which are made unavailable and are part of the model. If so, appropriate safty precautions will be taken. It will not always be necessary to requantify the LPSA. Delta risk changes may be good enough. The importance of the components can be used to make a judgement whether a detailed assessment is required.

In regard of lowpower production no significant configuration change takes place in the plant. The major difference is the factor time as an accident scenario starts at a lower power. For the success-criteria we may use the same as for the 100% power. This is, as we can judge today conservative.

In regard of the shutdown situation, we have to define a new set of success-criteria. We like to call them END States.

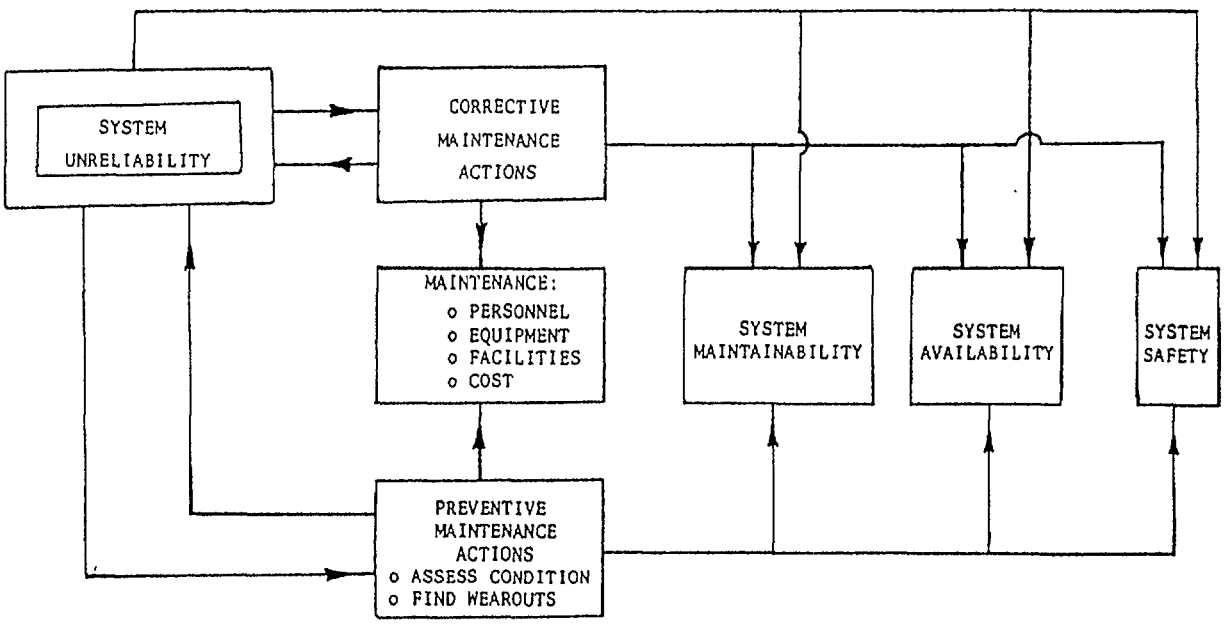


FIG. 6. The cycles of unreliability, maintainability, availability and safety.

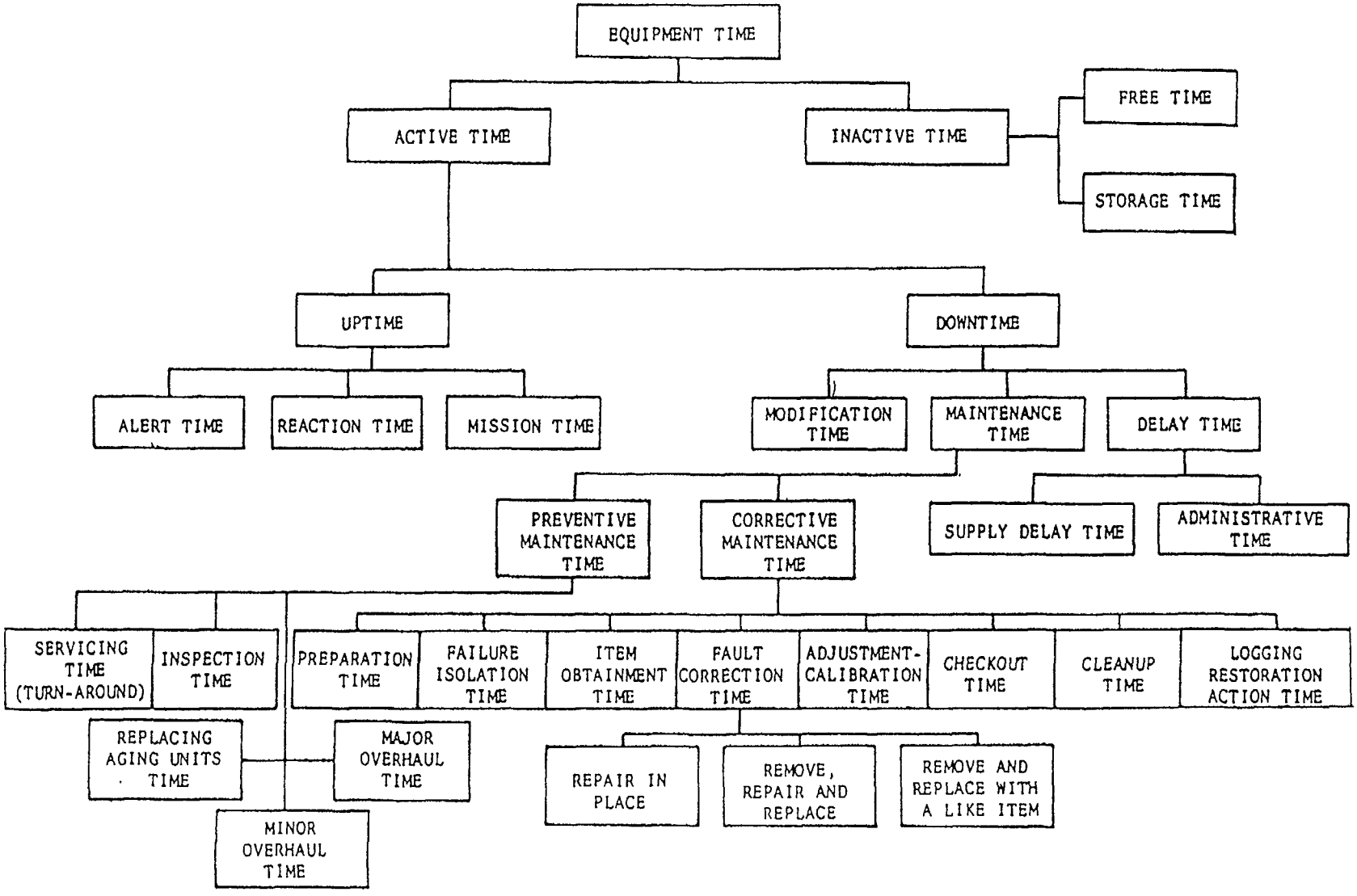
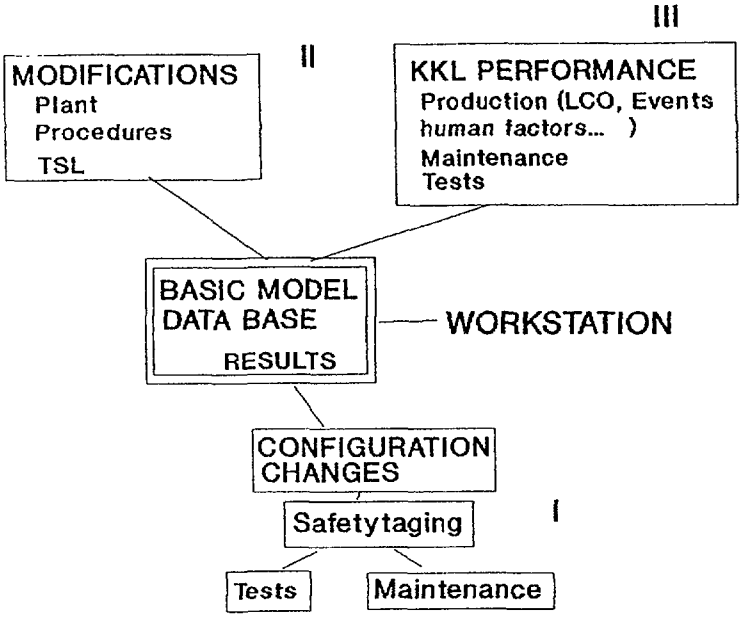


FIG. 7. Preventive and corrective maintenance times and their relationship to all other times associated with the life of equipment.



I CONFIGURATION CHANGES :
In conjunction with appropriate Success Criteria

II Review of proposed Modifications

III UP-DATES :
Based on new KKL reliability values

FIG. 8. Use of living PSA, simulation.

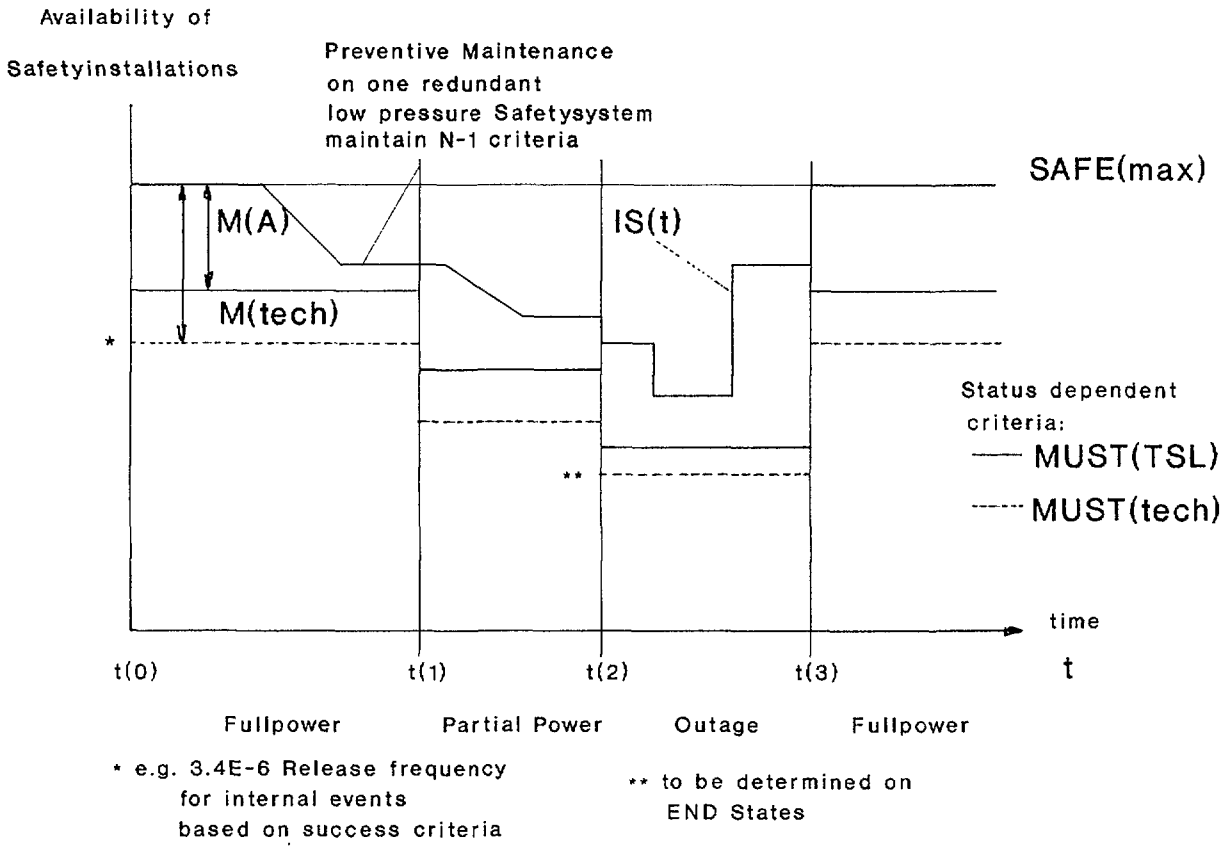


FIG. 9. Safety margins in relation to MUST (TSL)/MUST (tech).

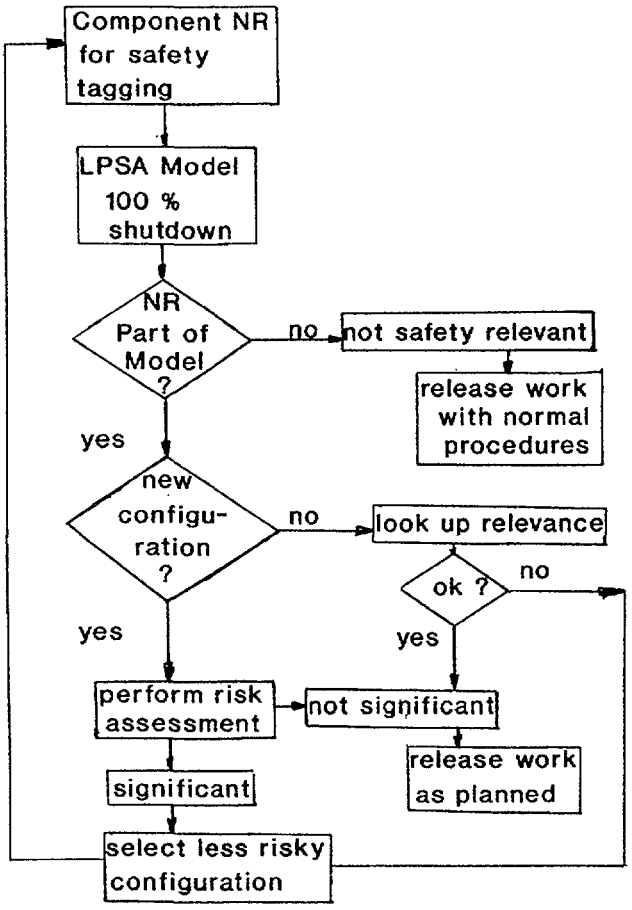


FIG. 10. Screening process to spot for risk; 100% power and shutdown.

The most important safety-significant changes are:
- RPV is open.
- The breach of the primary containment (Material hatch is open). Only the secondary containment is still in place.
- The RCIC System, a steam turbine driven pump will not be available.
- Components are removed from systems leaving "holes". A potential for "LOCA's".

It has to be assured that enough cooling capability is available from the opening the RPV, preparation and fillup of the refueling vault. No preventive work on the low pressure injection and cooling systems are performed during the shutdown. This work is done during full power operation when these systems have least value in terms of safety. (See Fig. 9). This is possible due to the fact that a high degree of redundancy in the ECCS-systems in KKL exists.
An other system the SGTS (Standby Gas Treatment System) has its highest safety value during the refueling time when the dropping of a fuelelement is realistically possible. The preventive maintenance for the two SGTS-systems, which do not meet the n-2 criteria are maintained when the containment is closed and no irradiated fuel elements are transported in the fuel pit.

6. CONCLUSIONS

It can be concluded that an active and determined plant management, combined with a continious learning effort and substituted by a periodic review of the plant experience with PRA-methods, is a good safety strategy. It is planned to perform a periodic reevaluation of the original PRA-studies with actual plant-specific performance data to spot for the possible changes in weak points.
The collection of the shut-down-data has to be organised. The particular area of importance are the plant-configurations if they change in the course of the shutdown from the original shutdownplan.

References

[1] Lecture 54.4.3 from ANL/IAEA Interregional Training Course "Use of PSA in the Nuclear Power Plants: Risk-Based Prioritisation of Operational Task" 27 January -14 February 1992.
- Optimisation Of Technical Specification; Swiss Approach- (R.Häusermann) .

[2] Lecture 54.2.6 from ANL/IAEA Interregional Training Course "Use of PSA in the Nuclear Power Plants: Risk-Based Prioritisation of Operational Task" 27 January -14 February 1992.
- Use of PSA in Safety Management (R. Häusermann)

[3] Lecture 54.7.4 from ANL/IAEA Interregional Training Course "Use of PSA in the Nuclear Power Plants: Risk-Based Prioritisation of Operational Task" 27 January -14 February 1992.
- Use of PSA in Safety Management KKL Status Report (R. Häusermann)

[4] IAEA-TECDOC-621 "Good Practices for Outage Management in Nuclear Power Plants". September 1991.

SHUT-DOWN RISK MANAGEMENT AT THE RIVER BEND STATION

J.L. BURTON, J.J. LYNCH
Gulf States Utilities Company,
Saint Francisville, Louisiana

R.N.M. HUNT
Halliburton NUS Environmental Corporation,
Gaithersburg, Maryland

United States of America

Presented by J. Julius

Abstract

During the upcoming refueling outage (RF-4) at the River Bend Station, the installation of several major modifications will result in temporary system alignments which could affect the availability and reliability of some critical plant safety systems. The paper provides a brief description of an approach which will be implemented to monitor and control the overall plant outage configuration by assessing its effect on plant risk, measured in terms of core damage frequency and the likelihood of a release of radio-isotopes from the plant.

Introduction

River Bend Station is a 940 Mwe, G.E. BWR-6/Mark III nuclear generating station operated by the Gulf States Utilities Company (GSU), which went into commercial operation in June of 1986. During its initial five years of operation the plant has exhibited excellent performance characteristics demonstrated by the 71.5% average capacity factor experienced over the past 36 months, and the two record setting continuous runs at power of 151 and 184 days achieved during fuel cycles one and two, respectively.

Over the past three years, the management of the River Bend Station have been pursuing the development of an effective in-house risk and reliability assessment capability to provide the quantitative decision-making support needed to enhance the excellent performance that the plant had already exhibited. When extensive remedial actions were proposed for the RF-4 outage to correct severe microbial induced corrosion (MIC) within the open cooling water systems, plant management required the activities to be conducted in a way which minimized shut-down risk.

The proposed approach, described below, is intended to identify risks inherent with the outage work, to control plant configuration to minimize risk and to provide the framework

within which contingency plans can be assessed. The planned outage work includes extensive primary system decontamination, chemical cleaning of the standby service water system, partial replacement of the service water cooling system piping and conversion of the existing open cooling system to a closed system.

This work will adversely affect the availability of the existing service water cooling systems and emergency on-site power generating systems. Therefore, the RF-4 outage risk management program was developed to control overall plant configuration to ensure that the impact on risk is minimized and held to an acceptable level.

The RF-4 Risk Management Program

The program objective is to develop a set of technically sound controls, techniques and tools which will allow the plant operating and outage management staff to effectively manage facility risk whenever important safety systems are unavailable or in a degraded condition.

There are several plant states of concern. The most important of these will be when the complete core is being offloaded and transferred to the fuel building for about 180 days. The risk management approach adopted by the Engineering Analysis group involved an examination of various probabilistic risk assessment techniques and the integration of selected methods to form a set of integrated risk based outage controls.

The result of this assessment was a three part approach which exploits three existing on-site capabilities, such as:

- the ability to perform thermal hydraulic analyses to gain practical, "best estimate" knowledge of plant transient behavior
- experience in the application of quantitative risk analysis and knowledge of the importance, reliability and risk sensitivity of individual components and systems
- knowledge of the hierarchy or interdependencies between all plant systems which affect plant risk

These capabilities allow River Bend to predict plant and system capability, estimate the probability that these systems will perform when needed, and provide a visual display of the way in which the plant works, so that threats to critical functions can be monitored and recognized at a glance.

Thermal Hydraulic Analysis

One of the authors developed a best estimate model of the spent fuel pool with the RELAP5 computer code. This analytical activity provided the necessary insights about the inherent fuel pool convection flows, mixing characteristics and heat-up rates following various postulated loss of cooling scenarios.

The results from a "thermal mixing" study provided confirmation of adequate fuel pool circulation flows and mixing, and the "hot channel" study provided evidence of adequate fuel cooling under the postulated conditions. The studies also provided an understanding of the phenomena involved, the timing and rate of temperature change for various pool conditions, and the minimum pool make-up requirements following loss of cooling and surface bulk boiling. This information was important to the definition of success criteria for the probabilistic risk assessment.

Probabilistic Risk Assessment

Using the information gained from the thermal hydraulics analysis to define success criteria, members of the group were able to construct fault tree models for each of the plant cooling systems and their associated support systems. The results of these analyses were used to establish the expected system failure rates and provide estimates of core damage frequency and the relative importance of each of the contributing components.

The results of these analyses provided an understanding of the plant vulnerabilities and a prediction of the expected likelihood of a loss of cooling event under the conditions assumed to exist during the RF-4 outage. The conclusion reached was that, under the expected outage conditions, the expected core damage frequency was acceptable. The two analytical approaches used to this point in the overall evaluation appear to meet all of the requirements for risk management.

However, the large number of outage related activities and the unusual plant configurations which could possibly result, left the impression that there may be additional vulnerabilities not fully accounted for. For instance, inadvertent or unanticipated changes to the plant configuration could result in its moving beyond the conditions assumed during the PRA.

This additional concern led to the application of the third element of the outage risk management program. Develop a means for control of the plant configuration to maintain the validity of the assumptions made in the PRA. To achieve this capability, the detailed knowledge of plant interdependencies was exploited. A special diagram, known as a Master Plant Logic Diagram (MPLD) was developed for each of the expected modes of plant operation.

Qualitative Analysis - The Master Plant Logic Diagram (MPLD)

This type of model, called a "Master Plant Logic Diagram" (MPLD), was originally developed to support the quantification of a conventional PRA (reference 1). The MPLD is designed to provide a visual display of all of the detailed plant system inter-dependencies which are important to, or affect plant risk. It is intended to be used as a "preventive defense" to help ensure that the plant is not inadvertently placed in a risk important configuration during the evolutions to be encountered in the upcoming RF-4 outage.

Not only does the MPLD identify the systems which play a role in determining plant risk, but, it also displays them in terms of their natural hierarchy to provide cause and effect relationships. This capability is the source of the effectiveness of the MPLD for risk management. The MPLD can be modified on a real time basis to reflect proposed or existing system configurations, availabilities or status. The resulting effects of the configuration can be propagated throughout the MPLD to verify that the proposed plant configuration will pose no unacceptable threat to a critical function.

A preliminary MPLD has been developed for the River Bend containment and fuel buildings for the refueling outage displays all important hierarchal relationships between the hardware systems, sub-functions and functions which must be successfully maintained to minimize the release of radio-isotopes from the plant. Release of radio-isotopes to the environment is the event which has been considered as risk controlling.

MPLD Description

The MPLD has two top level release events, one for the containment building and one for the fuel building. The front line systems for each are linked together via a common integrated dependency network so that the overall effects of changes in plant configuration can be viewed "in toto" for both buildings. Typical of the functions included in the MPLD are:

- Maintaining fuel energy removal capability in excess of decay heat requirements by maintaining energy transport or transfer capability from the primary system.

- Scrubbing, retaining and removing any fission products local to the point of release before it can enter the containment atmosphere.

- Removing fission products from the containment atmosphere, if and when they may be released, to ensure that if containment integrity is lost, the concentration of any released fission products will be minimal.

- o Maintaining control over all containment penetrations (active or passive) so that they can be isolated on demand.

- o Maintaining functional integrity of the containment boundary by ensuring adequate filtration capability for any normally open penetrations and maintaining adequate containment energy removal capability

General MPLD structure and attributes

The MPLD has a "top-down" structure which associates each "critical function" with its hierarchically derived subfunctions, plant hardware systems, sub-systems, components and human actions. These hardware systems and associated human actions represent the physical "success paths" which must operate to achieve each function and facilitate the overall objective of preventing a release to the environment, the ultimate "safety" issue.

The hierarchy of the interconnecting systems, both primary and support, are displayed in the form of an integrated matrix or network, with the solid "dots" representing dependencies (see Figure 1). The MPLD is drawn with SUCCESS ORIENTATION so that the viewpoint is consistent with that of the operating staff. The embedded logical relationships are "AND" wherever a branch is shown without an explicit logic gate. Whenever alternatives are possible, or more than one viable success path exists for a particular function, an "OR" gate is explicitly drawn on the diagram.

Application of the MPLD to support the RF-4 outage

The objective in using the MPLD for outage management is to provide a means for "mimicking" the actual or proposed plant configurations, and verify that there are, or always will be, an acceptable number of success paths available. The anticipated steps to be followed in using the MPLD are as follows:

1. Outage management staff will maintain a copy of the MPLD which displays the actual real-time plant configuration and existing boundary conditions (off-site power available, etc.). Modifications from the original MPLD can be made with a red pen.

2. Whenever a change in the plant is proposed, and components, subsystems or systems are to be taken out of service or realigned, the outage managers will modify the MPLD to reflect the new configuration. Any new interconnections needed to represent temporary connections or alignments between components or subsystems would also be added.

Master Plant Logic Diagram Structure
- Showing Hierarchy between:
  - o Plant Objectives
  - o Plant Critical Functions
  - o Plant Front Line Systems (FLS)
  - o Plant Support Systems

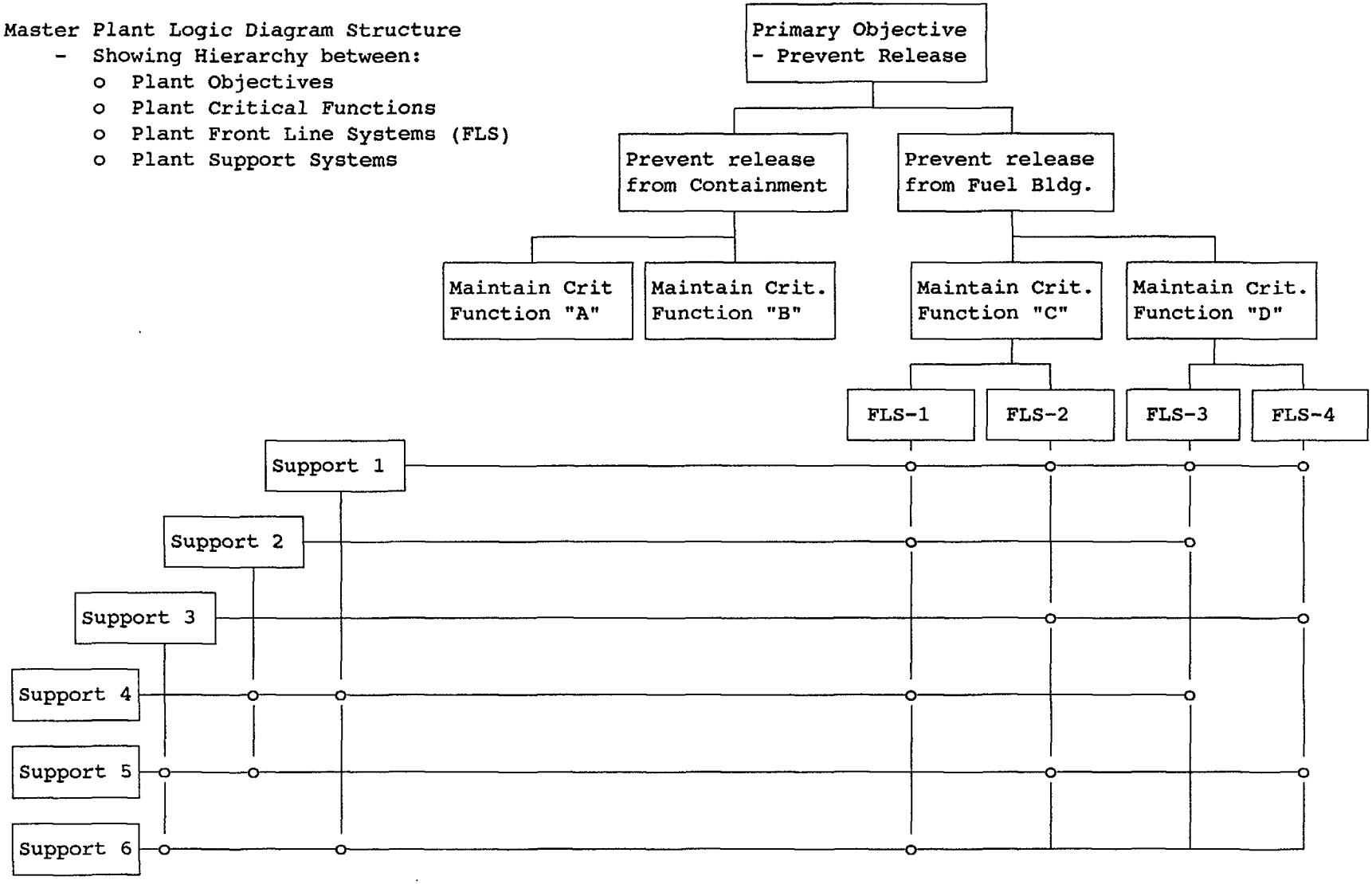


FIG. 1. Structure of MPLD.

The plant staff can cover the MPLD in clear plastic so that changes can be made with a grease pen using multiple colors to distinguish between those changes proposed and those which have been implemented

The effects of these changes will be traced upwards through the MPLD, until their full impact on the critical functions can be identified. If the proposed change does not result in a reduction in the number of success paths for any critical functions, it can be implemented without concern. If success paths are lost, the acceptability of the configuration must be confirmed before its implementation. If the change is judged unacceptable, other alternatives must be considered.

3. Each dependency in the MPLD is documented on an associated "master dependency list", which identifies individual component dependencies which are implicitly included at each MPLD node.

Summary

The goal of the MPLD application is to provide a way in which existing plant configuration can be assessed at a glance to verify that viable success paths are, and will continue to be, available for each plant critical function, and that any proposed change in plant configuration can be assessed BEFORE IT IS IMPLEMENTED.
The MPLD also provides the information needed by the outage management staff if they are to identify viable contingency plans which could be implemented for any plant configuration. The MPLD shows which required support systems are/are not available.
A risk based "living" model of the plant thus exists.
It is not intended that the MPLD model supplant the other PRA approaches. However, the MPLD provides augmentation to the PRA by providing a mechanism for control so that the plant does not enter an unsafe condition. Preventing unacceptable conditions from occurring is the prime goal for the MPLD.

Staff Acceptance of the Approach and Methodology

So far, acceptance has been high from the operating and outage management staff, The concept is still under development and has not been tested "under fire". The existing format seems acceptable, but it may change before the outage. Some consideration has also been given towards the use of the model to develop a set of "ad hoc" technical specifications for the outage.

Additional benefits that have become apparent, are that the MPLD makes the world of risk assessment more visible and real to non-analysts and may increase their sensitivity, awareness and understanding of risk based issues. This may lead to an important contribution to increased plant safety.

DEVELOPMENT AND IMPLEMENTATION OF TECHNICAL SPECIFICATIONS FOR LOW POWER AND SHUTDOWN CONDITIONS

M. REINHART
United States Nuclear Regulatory Commission,
Washington, D.C.,
United States of America

Abstract

Risk insights gained through major PSA projects were used in the USNRC technical specifications improvement programme. The revision of future technical specifications will also include provision to control the risk in shutdown. Several low power and shutdown risk studies suggested the needs for new or revised technical specification requirements on the following subjects: outage planning and control; RCS, ultimate heat sink; power sources; and containment integrity.

From 1987 through most of 1992, the U.S. Nuclear Regulatory Commission (NRC) worked with the nuclear industry to develop improved Standard Technical Specifications (STS) as part of the Technical Specifications Improvement Program (TSIP). A feature of the TSIP was to use available risk insights to improve technical specifications. Contemporaneously, during 1990, the international nuclear community started to become more sensitive to managing the risk associated with low-power and shutdown (LPS) conditions. The NRC, in participation with the international effort, initiated a study[1] of LPS risk. The study--which included plant visits--evaluated LPS operations, activities, and events; shutdown PRAs; and other technical analyses (e.g., thermal-hydraulic and boron dilution). The study also evaluated existing guidance and requirements, including technical specifications. The goals of the comprehensive study were to integrate all aspects of LPS conditions, to understand LPS risk, and to reduce the risk, if necessary. Past efforts had addressed similar issues, but one at a time.

The results of this LPS study and a regulatory analysis indicate that plant risk during certain shutdown conditions can be significant. The primary shutdown concern is the ability to remove a high level of decay heat from a PWR during reduced reactor coolant inventory. This concern is especially serious during mid-loop operation.[2] Related dominant accident sequences are loss of all ac power, loss of reactor vessel coolant level control, and loss of reactor coolant inventory.

Current technical specifications were written under the assumption that the plant was at significantly less risk during shutdown conditions than during power operations. In contrast, the study suggests that revising some regulatory requirements, including technical specifications, could contribute to reducing the shutdown risk. The revisions would involve administrative

and equipment requirements. Administrative requirements would address outage planning and control. Equipment requirements would address primarily, but not exclusively, additional or redundant equipment during reduced reactor coolant inventory. To implement these revisions, newer plants would mostly have to change some existing technical specifications; older plants would also have to develop some additional technical specifications.

Overall, the study suggests five areas to be evaluated by regulatory analysis:

- Outage planning and control.
- Fire protection.
- Operations, training, procedures, and other contingency plans.
- Technical specifications.
- Instrumentation.

Of these five areas, all except fire protection and instrumentation can be addressed by technical specifications. Note that the first area, "outage planning and control," logically includes the third area, "operations, training, procedures, and other contingency plans."

Proposed revisions to technical specifications would address outage planning and control, anticipate operational needs and contingencies, and build defense in depth. Some of these proposed revisions--those to equipment operational requirements--fall into three tiers. The first tier increases the availability of equipment to remove decay heat and to add coolant to the reactor vessel. The second tier increases the availability of equipment to support the first-tier equipment. A third tier increases the availability of equipment to mitigate the consequences of an LPS accident. A provision being considered could allow flexibility to apply technical specifications requirements as a function of decay heat, reactor coolant inventory, and subcooling. Development of this provision, however, would probably be a long-term effort.

The LPS study suggests the need for new or revised technical specifications requirements during LPS conditions as follows:

- An outage planning and control program.

  This administrative control is the most important provision to reduce shutdown risk. Such a program would contain eleven essential elements:

  - Clearly defined and documented safety principles for outage planning and control.

  - Clearly defined organizational roles and responsibilities.

- A controlled procedure defining the outage planning process.
- Pre-planning for all outages.
- Strong technical input based on safety analysis, risk insights, and defense in depth.
- Independent safety review of the outage plan and any revisions.
- A controlled information system to provide critical safety parameters and equipment status on a real-time basis during the outage.
- Contingency plans and bases.
- Realistic consideration of staffing needs and personnel capabilities with emphasis on control room staff.
- Training.
- Feedback of shutdown experience into the planning process.

The Nuclear Management and Resources Council's document, NUMARC 91-06, "Guidelines for Industry Actions to Assess Shutdown Management," December 1991, may provide a useful structure to address the eleven essential elements of this administrative control program.

- Reactor coolant loops, decay heat removal, component cooling water, service water, and the ultimate heat sink.
  - Two trains of systems necessary to transport decay heat to the ultimate heat sink.
  - One train with a flooded refueling cavity.
- Emergency core cooling, the refueling water storage tank, and low temperature overpressure protection.
  - Two trains of systems necessary to provide makeup coolant to the reactor vessel.
  - One train with a flooded refueling cavity.
  - Low temperature overpressure protection available when needed.
- Power sources: onsite and offsite with a possible provision for augmentative power sources.

- Two onsite and one offsite ac source.

- One onsite and one offsite ac source with a flooded refueling cavity.

- The dc power sources, inverters, and the ac and dc distribution systems necessary to support equipment which is required to be operable.

- Augmented or temporary power sources may provide some safety credit on a plant-specific basis.

- Containment integrity for PWRs, containment spray and cooling, and hydrogen ignition.

  - Containment integrity would be established unless specified conditions exist, for example:

    - Decay heat level and reactor coolant temperature are below prescribed limits.

    - A steam generator is available.

    - The refueling cavity is flooded.

  Containment integrity in a PWR or the ability to establish it before reactor coolant boiling starts is critical to mitigate the consequences of an LPS accident. Once boiling starts, the atmospheric conditions (steam, temperature, pressure, and radiological) inside containment restrict the operators' ability to establish containment integrity. To have the ability to establish containment integrity, operators would have to be able to establish it manually and without ac power.

While developing improved STS, the NRC's Technical Specifications Branch (TSB) identified existing technical specifications requirements that addressed LPS conditions. The TSB then compared these existing requirements with those suggested by the study on LPS conditions. As a result of this comparison, the TSB proposed revised technical specifications as an input to the LPS study. However, this input was independent of the improved STS, and the TSB did not incorporate proposed changes to LPS requirements into the improved STS. In parallel, the nuclear industry proposed some changes to improved STS that address LPS conditions. While the NRC evaluated industry's input and identified areas of agreement and disagreement, it did not incorporate these changes into the improved STS. Improved STS, Revision 0, was issued in September 1992. The NRC anticipates incorporating the LPS requirements into a later revision of the improved STS.

In addition to revising certain technical specifications, other actions to ensure safety during LPS conditions would include the following:

- Ensure that a fire would not prevent the capability to remove decay heat.

- Improve instrumentation capability to indicate reactor coolant temperature, pressure, and level for the operator. Level is especially important during PWR mid-loop operations.

Notes:

1. NUREG-1449, "Shutdown and Low-Power Operation at Commercial Nuclear Power Plants in the United States," February 1992 (draft).

2. Reduced reactor coolant inventory is considered to be an open reactor coolant system with the water level less than 23 feet above the reactor vessel head flange.

   Mid-loop operation exists when the reactor coolant level is below the top of the inside diameter of the hot legs at the junction with the reactor vessel.

POINTS OF VIEW ON SHUTDOWN COOLING EVENTS AMONG THE MEMBERS OF THE WANO-PARIS CENTRE

V. HOENSCH
World Association of Nuclear Operators,
Paris

Abstract

The average NPP spends about 25 % of the total lifetime in shutdown. Several safety significant events proved that due attention should be paid to safety in shutdown. WANO organized an expert meeting to review the status of shutdown safety. The paper identified several important problems in shutdown. These include: human factors, instrumentation, procedures, planning of activities. Recommendation on how to improve the situation in each of those is given.

1. Overview

Approximately 25% of total plant life is the plant in shutdown condition. Experience has shown that the likelihood of experiencing significant operating events is increased when performing tests and off-normal activities such as those frequently performed during outages. The tempo of activities is significantly increased during outage periods and many contractors personnel are in site. The necessity for operator awareness and possible actions is increased since among automatic safety system functions are disabled during outage.

While technical specifications provide some assurance of safety, they were developed under the premise of a very low risk of core damage during a shutdown.

Following an INPO evaluation from 1973 to 1989 plants which were shutdown and in a condition of reduced coolant inventory lost decay heat removal capability 52 times [1]. Three of these events led to boiling in the reactor core. There are numerous examples of reactor cooling system inventory loss and events which could have led to inadvertent criticality.

Recent events such as :

Vogtle [2], Prairie Island 2 [3], Diablo Canyon [4], as well as results of studies those published by the French [5], have indicated that risk due to events occurring during shutdown modes might contribute significantly to the overall risk associated with operation of a nuclear power plant. The French Probabilistic Safety Assessment (PSA) has highlighted four potential initiators for non-power accidents. The presentations within the WANO experts' meeting have confirmed these findings. The four invitatiors are :

- Loss of Heat Sink
- Fast Dilution
- Total Station Blackout
- Loss of Coolant Accident

The Loss of Heat Sink is significant in terms of the core melt frequency. This was the topic of the experts' meeting in question. The was the topic of the experts' meeting in question. The Fast Dilution initiator is also important and a serious incident has a potential to cause

an off site radiological release. This initiator will be the topic of another WANO-Paris Centre experts' meeting in the Spring of 1993. The total station blackout and loss of coolant initiators can be addressed as a sub-set of the loss heat sink case.

We all know that plant technical specifications generally do not provide complete risk protection during shutdown. Technical Specifications like operating procedures, system designs, plant layouts and our colleagues as well, are attuned to operations at power. During outages we are dependent on knowledgeable people to apply the technical specification as a minimum set of requirements. We must establish a higher level of control if we are to assure risk minimisation during outages.

Unfortunately, and this was also the opinion of the experts' meeting, risks during shutdown are almost entirely related to human errors or to lack of paper actions by plant personnel in responding to failures when automatic actuation's are requested but are disabled. In addition the mid-loop operation is a separate and distinct mode for PWR's, which provide the bigest contribution to the risk during outage.

2. Mid-loop operation mode.

Mid-loop operation means :

- Reactor sub critical
- Reactor coolant temperature < 50°C
- Decay heat removal by residual heat removal (RHR) system
- Level in main coolant line approximately 3/4 filled.

Mid-loop operation is necessary during :

- Start-up of the plant to evacuate the upper plenum of the reactor cooling system, especially with U-tubes steam generator with a reactor coolant pressure approximately 0,3 bar.

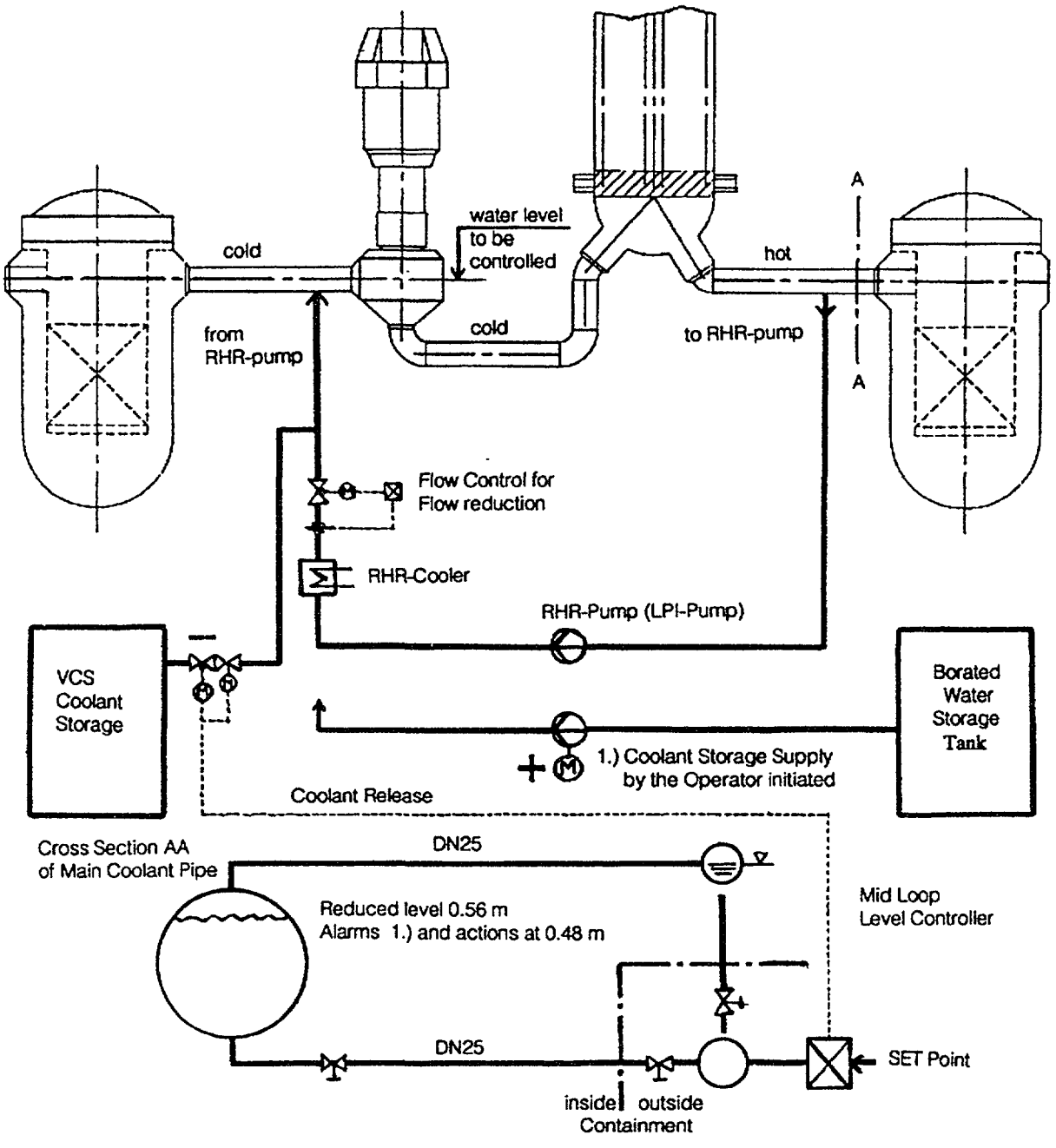
- Shutdown of the plant to drain pressurizer and the tubes of the steam generators and to purge the head of the reactor pressure vessel with nitrogen before opening with a reactor coolant pressure approximately atmospheric pressure.

3. Conclusions of the WANO experts' meeting.

Identification of the main risks; The identification are drawn from the presentations, and from the discussions in subgroups. First step was to discover to real generic points that means common circumstances and problems that have contributed to the risk of loss of coolant and of heat sink during the shutdown period and especially in the mid-loop operation mode.
The problem areas are not given in any order of priority of significance and because of the limited time of my presentation elaborate only with one typical example.

3.1 Human Factors

- Lack of awareness of the high risk associated with shutdown conditions.
  For example in the Vogtle incident [2] the operations personnel were unaware that the new reactor coolant system sight class level instrument was not available for use.



Mid-loop operation level control devices.

- Programme pressure to achieve shorter outages.
  The incident at Prairie Island 2 [3] was among other things caused because the briefing did not adequately discuss the level instrumentation (including the effects of pressure) to be used to control the evaluation of the expected sequence of the evaluation. The shift manager conducted the briefing.

- Lack of understanding of plant status and of plant status and of plant control.
  For the incident in Tricastin NPP on the 3th June 1990 was one of the salient facts, that the night shift crew wanted to complete the hold point procedure before the shift takeover. That led them to carry out several different tasks in a hurry.

- Low questioning attitude of shaft of all grades.
  The above mentioned incident is a confirmation for this statement. The morning shift crew believed that the situation was stable and the only thing to do was to correct the boron concentration of the boron injection tank. In fact, the situation was unstable, and the parameters were not correctly managed.

3.2 Plant

- Inadequate displayed information on shutdown cooling parameters, and on plant and system status.
  The event [4] revealed inadequate design and installation of the instrumentation. The both permanent and temporary systems for indicating and alarming reactor vessel water level and for measuring core temperature could not provide the shift crew with readout and low-level alarm in the control room. Incomplete knowledge of plant status, system review, and work planning combined with personnel and communication errors resulted in an unexpected loss of reactor coolant inventory.

- Inadequate back-up measurement of plant parameters.
  The core temperature monitoring via core thermocouples might not be feasible during evaluations such as removal or installation of the reactor vessel head. If core thermocouple temperature monitoring will not be available for extended time periods, a backup means to monitor core temperature needs to be provided.

- No automatic protection in the shutdown state.
  During the referenced event [4], delays in restoration core cooling occurred because the lack of available makeup water sources, alternate means for injection including gravity feed and pumped injection and at least one source of borated makeup water to the reactor coolant system.

- Inadequate design for filling, venting, seal injection, and draining.
  Insufficient water level is evident whenever a residual heat removal pump shows symptoms of caviating even if the level detectors indicate adequate water level. Steam can collect in the suction line of residual heat removal systems designed with loop seals in the suction line. This steam cannot be condensed by saturated liquid from the hot leg or exhausted with the limited capacities of the vacuum priming system used by some plants.

- Potential for loss of RHR pumps.
  This potential configuration exists when the reactor coolant hot legs are isolated (e.g. steam generator nozzle dams installed or loop isolation valves closed) in combination with a large cold leg opening (e.g. an open steam generator manway or reactor coolant pump).

3.3 Procedures

- Absence of adequate Technical Specifications.
  Since mid-loop operation cannot be eliminated, the Technical Specification should include this operation mode to ensure adequate monitoring, control, and the capability for restoration of reactor vessel water inventory and were cooling.

- Inaccuracy of operating procedures.
  Four similar events [6] with premature lifting and excessive blowndown of residual heat removal relief valves made evident that operating procedures should be reviewed to ensure that reactor coolant system evaluations conducted while the RHR-system is in operation are performed at pressures that provide the greatest margin to the setpoint of the RHR-system relief valves.

- Lack of water balance procedures and drain down control.
  In the events[4] especially in the Diablo Canyon plant, a drain valve was opened without operator knowledge and was not monitored locally for continuing leakage. Therefore, when the volume control tank water level decreased, the plant operators could not properly diagnosed the problem.

3.4 Planning

- Maintenance and operational tasks increase risk by reducing redundancy, prevention capability, and detection capability.
  The event in the Quad Cities 1 [7] is in this context significant because he documents that control over equipment and system status is made more difficult during plant outage due to the extent of maintenance and modification work in progress and the large number of outstanding system danger - do-not operate tags.

- Lack of contingency planning
  The event [3] demonstrated the necessity of contingency in the outage schedule. Contingency are indepensible when difficulties are possible in restoring residual heat removal cooling flow during mid-loop operation mode.

- Introduction of unplanned work
  All events revealed that the some risk is present if the outage schedule is changed to incorporate unanticipated work, not only can the completion date of the outage be seriously jeopardised, but contingency plans and risk assessments can be invalidated. In such situations the original scheduling logic must be used to evaluate the changes and additions to ensure the same core is factored into the modified schedule.

4. Recommendations

From the above mentioned conclusions on the generic risks to shutdown cooling, the participants of the experts' meeting agreed on the 41 recommendations. These recommendations were offered for consideration by WANO Interface Officers, Plant Managers and staff involved in outage management.
The following list is a selection of the recommendations given in the same order as the generic points. No order of priority is chosen.

4.1 Human Factors

- Awareness
  Provide initial and continuing training to operations and maintenance personnel on specific events in question. The training should stress the role of human error in these events, potential consequences in terms of fuel damage and the associated risk.

- Program pressure
  Consideration should be given to providing on each shift, an additional operator or engineer, preferably licensed, who is independent of the outage programme. He should be on site at all times during the outage, or at least during operations at low water inventory, with the sole responsibility for monitoring shutdown safety.

- Understanding
  Attention must be given to the shift change over procedures during sensitive plant operations. If practicable plant status changes during mid-loop operation mode should be avoided or, if possible, interrupted before shift change over.

- Attitudes
  Management must be seen to support an enhanced safety culture. That means e.g. guidance used to maintain proper plant configuration status during outages as well as other operating modes should be reviewed to incorporate lessons learned from events during shutdown activities.

4.2 Plant

- Information
  Adequate displayed information should be available, to ensure that the operators are aware at all times of on going maintenance activities, and of plant alignments.

- Back-up Measurement
  Ultrasonic detectors are filled on the hot and cold legs during the mid-loop operation mode and have proved to be very accurate.

- Automatic Protection
  An engineering assessement should be carried out to identify alternative methods of increasing primary circuit water inventory, and of providing emergency secondary cooling capability. This is possible by means of gravity feeding from the refuelling water storage tank to a vented primary system. This can be an effective means of providing makeup water unless steam from reactor coolant system increases the pressure of the primary system above the available gravity head.

- Filling and Draining
  Review the provision of draining, filling, venting and seal injection systems with the objective of reducing the potential for incorrect operation. Use of a single path would provide better control during draining operations.

- Residual Heat Removal (RHR) Pumps
  Determine and test the specific operating margins to be sure to have excellent Net-positive suction head (NPSH) - conditions by :
  - - Low NPSH valve of RHR-pump
  - - Large vertical difference between loop and RHR-pump
  - - Low pressure losses in suction line (RHR - cooler on discharge side).

4.3 Procedures

- Technical Specifications
  Technical Specifications should exist for all operating modes including cold shutdown especially for mid-loop operation mode and refuelling.

- Operation Procedures
  Provide emergency procedures for use in the event of loss of RHR-system during operating at low coolant inventory.

- Water Balance
  Review the procedures supporting residual heat removal system operation to ensure that methods (such as graphs) exist to determine reactor core heat-up and boil-off rates as a function of reactor coolant system volume and the time since shutdown, assuming worst case power history.

4.4 Planning

- Reducing Risk
  The use of standardised and proven outage work packages should be encouraged.

- Contingency
  When plant configurations increase the risk by, for example reducing redundency, contingency plans should be developed and available. Contingencies are not only established by procedure, but additional equipment is also prepared to support abnormal or unexpected plant conditions. Examples of this kind of equipment are e.g. :
  - - Steam generator nozzle dams
  - - Additional air compressors for service air and instrument
  - - Temporary power supplies
  - - High Efficiency Particluate Air (HEPA) - filter

4.5 Unplanned Work

Administrative controls should be rigorous enough to ensure that rescheduled activities are subjected to the same technical reviews and risk assessments as those applied to the original work packages.

5. Good Practices

A number of good practices were suggested during the discussions. WANO-Paris Centre is still preparing and reviewing the observed practices into good practice documents. After formally approving we will distribute the good practices for consideration by the WANO-members.

6. Conclusion

The events such as at Vogtle [2], Prairie Island [3], Diablo Canyon [4] as well as results gained from different probabilistic safety studies, have indicated that the risk due to events occurring during shutdown especially mid-loop operation mode contribute significantly to the risk associated with routine operation of a nuclear power plant.

Thus the outage has to be planned with significant foresight and consideration of system and functional redundancy and availability. The most probable risk is from the potential for losing decay heat removal when the containment and reactor vessel are open. A loss of residual heat removal capability can result in the boiling

of cooling water, with the potential for core uncovery and damage. The loss of residual heat removal cooling can also lead to airborne radioactivity releases, increased radiation levels due to loss of core shielding, and equipment damage. The experts' meeting gives recommendations to cope with such situations and proposed some Good Practice in this area.

References

[1] 1991 INPO Outage Managers Workshop, July 16th - 18th, Atlanta, Georgia.

[2] OE 4986 I TYNAN (GPC) Vogtle Unit 1

[3] IS 1074 I COWAN (INPO) Prairie Island 2

[4] WANO- EAR ATL 89-033/INPO SOER 83-3 Rev. 1

[5] EDF, Etude Probabiliste de Sûreté EPS 1300, Rapport de Synthése, 31.5.1990

[6] WANO - EAR-ATL 90-10/INPO SER 5-90

[7] WANO - EAR-ATL 91-017/INPO SER 7-91

LIST OF PARTICIPANTS

BELGIUM

Landsheere, C.	AIB–Vinçotte Nuclear, Koningslaan 157, B-1060 Brussels
Fossion, P.A.H.	TRACTEBEL, Av. Ariane 7, B-1200 Brussels
Schene, R.M.	Westinghouse Energy Systems International, 73, rue de Stalle, B-1180 Brussels

BRAZIL

Araujo Goes, A.G.	National Nuclear Energy Commission (CNEN), General Severiano, 90, Botafogo, 222 94 Rio de Janeiro

CZECHOSLOVAKIA

Aldorf, R.	Nuclear Research Institute, 250 68 Řež
Bezák, S.	Nuclear Power Plant Bohunice, 919 31 Jaslovské Bohunice
Cillík, I.	VUJE – Nuclear Power Plant Research Institute, Okruzná 5, Trnava 918 64
Klepác, J.	VUJE – Nuclear Power Plant Research Institute, Okruzná 5, Trnava 918 64
Malacka, M.	Nuclear Research Institute, 250 68 Řež
Markech, B.	VUJE - Nuclear Power Plant Research Institute, Okruzná 5, Trnava 918 64
Rehácek, R.	Czechoslovak Atomic Energy Commission, NPP Dukovany, 675 50 Dukovany

FINLAND

Himanen, R.P.	Teollisuuden Voima Oy (TVO), SF-27160 Olkiluoto
Pyy, P.T.	VTT Laboratory of Electrical and Automation Engineering, Otakaari 7B, 02150 Espoo

FRANCE

Montagnon, F.	EdF/SEPTEN, 12/14 avenue Dutrievoz, 69628 Villeurbanne Cedex
O'Connor, M.	TECHNICATOME, Rue A. Ampère, B.P. 34000, F-13791 Aix-en-Provence Cedex 3
Tricot, N.	CEA/IPSN, 60-68 avenue du General Leclerc, F-92265 Fontenay-aux-Roses Cedex

GERMANY

Bläsig, H.	RWE Energie AG, Kruppstraße 5, D-4300 Essen
Eder, D.	NIS-Ingenieurgesellschaft mbH, Donaustraße 23, D-6450 Hanau 1
Hoeld, A.	Gesellschaft für Anlagen-und Reaktorsicherheit (GRS) mbH, Reaktorstation, Forschungsgelände, D-8046 Garching
Meyer, A.-W.	Siemens AG, Berliner Str. 295–303, D-6050 Offenbach
Pertz, M.	Gesellschaft für Anlagen-und Reaktorsicherheit (GRS) mbH, Schwertnergasse 1, D-5000 Köln 1
Wurst, K.H.	Gesellschaft für Anlagen-und Reaktorsicherheit (GRS) mbH, Schwertnergasse 1, D-5000 Köln 1

INDIA

Venkat Raj, V.	Bhabha Atomic Research Centre, Engg. Hall No. 7, Trombay, Bombay 400 085

JAPAN

Nishio. M.	Japan Institute of Nuclear Safety, Fujita Kankou Toranomon Bldg. 7F, 3-17-1, Toranomon, Minato-ku, Tokyo 105

MEXICO

Becerra Perez, J.A.	Comisión Nacional de Seguridad Nuclear y Salvaguardias, Dr. Barragan 779, Col. Vertiz Narvarte, 03020 Mexico, D.F.
Huerta Bahena, A.	Comisión Nacional de Seguridad Nuclear y Salvaguardias, Dr. Barragan 779, Col. Vertiz Narvarte, 03020 Mexico, D.F.
Rodriguez Hernandez, A.	Comisión Nacional de Seguridad Nuclear y Salvaguardias, Dr. Barragan 779, Col. Vertiz Narvarte, 03020 Mexico, D.F.

NETHERLANDS

van der Borst, M.	EPZ – Locatie Zeeland, Wilhelminahofweg 3, 4454 PM Borssele, Postbus 130, NL-4380 AC Vlissingen

ROMANIA

Comanescu, L.	ISPE-ON Magurele, P.O. Box 5204 MG4, Bucharest

RUSSIAN FEDERATION

Siryapin, V.N.	OKB Gydropress, c/o Ministry of the Russian Federation for Atomic Energy, International Relations Committee, Staromonetny pereulok 26, 109180 Moscow

SLOVENIA

Cerjak, J.	Nuclear Power Plant Krsko, Vrbina 12, 68270 Krsko
Kozuh, M.	Jozef Stefan Institute, Jamova 39, 61000 Ljubljana
Levstek, M.F.	Slovenian Nuclear Safety Administration, Kardeljeva ploscad 24, 61000 Ljubljana

SOUTH AFRICA

Hill, T.F.	Council for Nuclear Safety, P.O. Box 7106, Hennopsmeer 0046

SPAIN

Faig, J.	Asociación Nuclear Ascó, c/ Tres Torres, No. 7, E-08017 Barcelona
Fiol, M.J.	UITESA, Juan Bravo 49 D., E-28006 Madrid
Isasia Gonzalez, R.	Consejo de Seguridad Nuclear, Justo Dorado, 11, E-28040 Madrid
Otero, Ma.T.	C.N. Vandellos II, Trav. De Les Corts 55, E-08028 Barcelona
Sabate, R.	C.N. Vandellos II, Trav. De Les Corts 55, E-08028 Barcelona
Torres Puya, M.	TECNATOM, S.A., Km. 19, Ctra. N-I Madrid - Irún, E-28709 San Sebastián de los Reyes, Madrid

SWEDEN

Andersson, B.	Forsmarksverket, Vattenfall, S-742 00 Östhammar
Andersson, K.	Karinta-Konsult, Box 6048, S-183 06 Täby
Bennemo, L.	Vattenfall, PT, S-162 87 Vällingby
Carlsson, L.	Swedish Nuclear Power Inspectorate, Box 27106, S-102 52 Stockholm
Engqvist, A.	Vattenfall, PT, S-162 87 Vällingby
Erixon, S.	Swedish Nuclear Power Inspectorate, Box 27106, S-102 52 Stockholm
Godas, T.	Swedish Radiation Protection Institute, Box 60204, S-104 01 Stockholm
Hellstrom, P.E.	RELCON AB, Box 2057, S-171 02 Solna

Ingemarsson, K.F.	Forsmarksverket, Vattenfall, S-742 00 Östhammar
Jönsson, J.	Sydkraft Konsult AB, Carl Gustafs 4, S-20509 Malmö
Karlsson, C.	Swedish Nuclear Power Inspectorate, Box 27106, S-102 52 Stockholm
Karnik, P.	ES-Konsult, Box 3096, S-16103 Bromma
Landelius, M.	OKG AB, S-570 93 Figeholm
Letho, T.	Forsmarksverket, Vattenfall, S-742 00 Östhammar
Liwang, B.	Swedish Nuclear Power Inspectorate, Box 27106, S-102 52 Stockholm
Malmqvist, L.	Swedish Radiation Protection Institute, Box 60204, S-104 01 Stockholm
Nilsson, E.T.R.	Swedish Nuclear Power Inspectorate, Box 27106, S-102 52 Stockholm
Nilsson, P.G.O.	Forsmarksverket, Vattenfall, S-742 00 Östhammar
Nyman, R.	Swedish Nuclear Power Inspectorate, Box 27106, S-102 52 Stockholm
Schwartz, F.	OKG AB, S-570 93 Figeholm,
Wilson, D.G.	RELCON AB, Box 2057, S-171 02 Solna

SWITZERLAND

Häusermann, R.E.	Kernkraftwerk Leibstadt AG, CH-4353 Leibstadt
Richner, M.	Nordostschweizerische Kraftwerke AG, Kernkraftwerk Beznau, CH-5312 Döttingen

UNITED KINGDOM

Hinchcliffe, A.J.	Department of Nuclear Science and Technology, Royal Naval College, Greenwich, London SE10 9NN

UNITED STATES OF AMERICA

El-Bassioni, A.	US Nuclear Regulatory Commission, Washington, DC 20555
Julius, J.	Halliburton NUS Corporation, 910 Clopper Rd, Gaithersburg, MD 20878
Reinhart, M. *(Chairman)*	US Nuclear Regulatory Commission, Washington, DC 20555-0001 Mail 11 E22
Torri, A.	Risk and Safety Engineeering, 1421 Hymettus Ave, Leucadia, CA 92024

WORLD ASSOCIATION OF NUCLEAR OPERATORS

Hoensch, V.R.	WANO Paris Centre, 39 Avenue de Friedland, F-75008 Paris, France

INTERNATIONAL ATOMIC ENERGY AGENCY

Tomic, B. *(Scientific Secretary)*	Safety Assessment Section, Division of Nuclear Safety, International Atomic Energy Agency, Wagramerstrasse 5, P.O. Box 100, A-1400 Vienna, Austria