IAEA-TECDOC-547

THE USE OF PROBABILISTIC SAFETY ASSESSMENT IN THE RELICENSING OF NUCLEAR POWER PLANTS FOR EXTENDED LIFETIMES

A TECHNICAL DOCUMENT ISSUED BY THE
INTERNATIONAL ATOMIC ENERGY AGENCY, VIENNA, 1990

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

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

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

THE USE OF PROBABILISTIC SAFETY ASSESSMENT
IN THE RELICENSING OF NUCLEAR POWER PLANTS
FOR EXTENDED LIFETIMES
IAEA, VIENNA, 1990
IAEA-TECDOC-547
ISSN 1011-4289

Printed by the IAEA in Austria
February 1990

FOREWORD

Probabilistic Safety Assessment (PSA) can provide important information related to the spectrum of possible accidents for a particular Nuclear Power Plant or other industrial installation. Such information, when based upon reliability data obtained from experience with that particular plant, concerns the accidents leading to core damage, the human, system and component failures which constitute these accidents and the safety level of the plant. Following the accident at Three Mile Island in the USA (TMI-2) and more recently at Chernobyl in the USSR, PSA was used to understand how these accidents happened.

PSA Level-1 which identifies the accident sequences and their relative contributions to the probability of core damage, is particularly applicable to safety decisions related to the prevention of accidents. Once the accident sequences which are the major contributors to the safety of the NPP are known the main component and human contributors to safety can be identified. A plant specific PSA and changes in reliability of different components and systems can be used to: determine the safety level of the plant at any given time, monitor the safety level of the plant up until the present and predict, from safety performance trending analyses, the safety level of the plant for some period of time in the future.

Over the next few years decisions must be made for a number of nuclear power plants as to whether to decommission and replace or refurbish and extend their useful life. Probabilistic Safety Assessment (PSA) can provide important insights regarding the safety of a nuclear power plant as a function of plant age. PSA can also provide information critical to decisions regarding which components and systems should be completely renewed and when such renewal should take place.

The Agency engaged expert consultants to document the latest information available on the use of PSA to provide assistance in licensing the extended lifetimes of nuclear power plants.

It is intended that this document give guidance in the major ways PSAs can be used for NPP life extension applications utilizing given PSA criteria.

The Agency engaged expert consultants to document the latest information available on the use of PSA to provide assistance in licensing the extended lifetimes of nuclear power plants.

It is intended that this document give guidance in the major ways PSAs can be used for NPP life extension applications utilizing given PSA criteria. This document also covers the specific steps for using presently available PSA models, data and criteria to assist life extension decision making and the research that could be carried out to extend the applicability of PSAs in this field.

The work of the participants in drafting and review of this document is greatly appreciated. In particular the contribution to this document and the previous work of Dr. William Vesely is clearly recognized.

EDITORIAL NOTE

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

The views expressed do not necessarily reflect those of the governments of the Member States or organizations under whose auspices the manuscripts were produced.

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

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

CONTENTS

1. INTRODUCTION

Probabilistic Safety Assessments (PSAs) can be used in various ways to help guide the relicensing of extended lifetimes of nuclear power plants. This technical report describes: 1) the different major ways PSAs can be used for life extension applications; 2) the analyses which are involved in applying PSAs to life extension evaluations; and 3) the modeling and data developments which can be carried out to extend the applicability of PSAs for life extension applications.

The report is organized according to the specific topics which are addressed. These topics are:

1. The different ways PSAs can be used for life extension applications.

2. The basic analyses which are involved in applying PSAs to life extension applications.

3. The specific ways in which PSA criteria can be utilized for assisting life extension decision making.

4. Specific steps which can be implemented for using presently available PSA models, data, and given criteria for assisting life extension decision-making.

5. Modeling and data developments that can be carried out to extend the applicability of PSAs for assisting life extension-decision making.

The main body of the report which follows describes these topics and gives example applications. Appendices A and B give further supporting considerations and experiences.

2. THE DIFFERENT MAJOR WAYS PSAs CAN BE USED FOR LIFE EXTENSION APPLICATIONS

There are three, major ways a PSA can be used to assist in the relicensing of extended lifetimes of a nuclear power plant:

1. The PSA can be used to evaluate the safety of the plant's design and procedures;
2. The PSA can be used to monitor the safety implications of the performance of the plant; and
3. The PSA can be used to predict the safety of the plant, accounting for the plant's design and performance.

To use the PSA for life extension applications, it is first of all important that a plant specific PSA be constructed to evaluate the safety of the plant's design and procedures. This is the first major way the PSA can be used to provide guidance in relicensing of extended lifetimes of nuclear power plants. If a PSA has not been previously constructed for the plant then it is important that one be constructed.

As illustrated in Figure 1 when the PSA is applied to evaluate the design and procedures of the plant, there is basically one set of results obtained which represents a snapshot of the core melt frequency (and other PSA

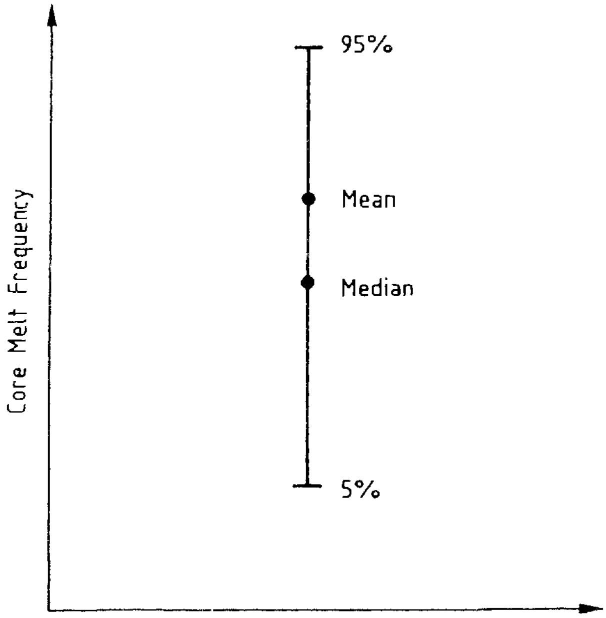

FIG. 1. PSA core melt frequency values produced when applying the PSA to evaluate the plant's design and procedures.

results) for the given models used and data used. The PSA results are generally characterized by th^ir median value and mean value, and error bars are given to represent the 95th percentile and 5th percentile of the results.

Life extension considerations involve not only considerations of the design and procedures but also involve considerations of time varying effects and aging effects. The second major way that a PSA can be used to provide guidance for life extension is to provide a tool for monitoring plant safety performance in real time. Figure 2 illustrates the type of output which is obtained when the PSA is applied to monitor the plant's core melt frequency in real time at periodic intervals. Associated error bars represent the uncertainty associated with the monitored core melt frequency levels.

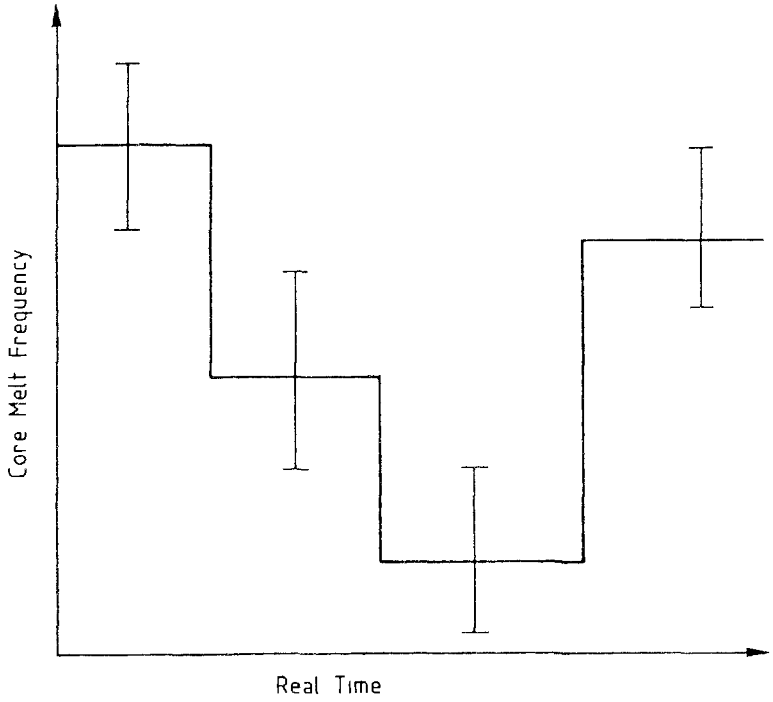

FIG. 2. PSA core melt frequency values versus monitored time produced when applying the PSA to monitor the plant's performance.

Monitoring of plant performance can provide an important means of controlling time varying plant configurations so that they do not result in large core melt frequency increases or large risk increases. Monitoring can also provide an important means of detecting deteriorating time trends in safety, enabling these time trends to be corrected before they result in accidents.

The third major way a PSA can be used in life extension applications is to provide a tool for predicting future safety performance, incorporating the time varying effects and aging effects which have been observed or are considered. This third way is really an extension of the second major way, that is using the PSA as a monitoring tool, where now the monitored results are used to predict future safety performance. Figure 3 illustrates the time dependent or age dependent output which is obtained when the PSA is applied to predict the future performance of the plant. Figure 3 also shows the associated uncertainties (error bars), which generally increase with predicted time. When the PSA is used as a predictive tool then it can provide an important means for predicting future safety implications of observed time trends and aging effects.

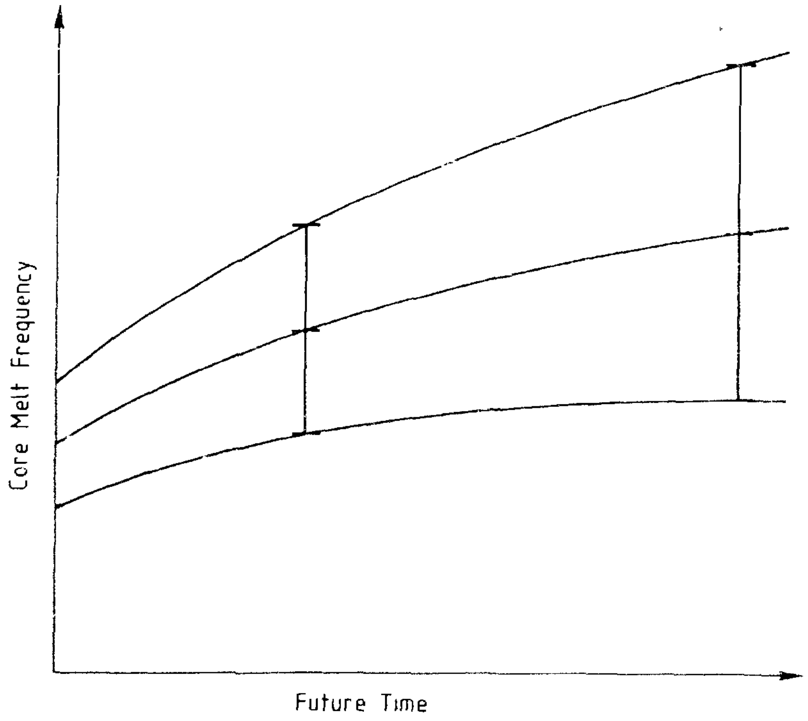

FIG.3. PSA core melt frequency values versus future time (or future age) produced when applying the PSA to predict the plant's future performance.

The following sections discuss in more detail these three major ways a PSA can be used to provide guidance for life extension considerations - as a design evaluation tool, as a monitoring tool and as a predictive tool.

2.1 Evaluation of the Plant's Design and Pr^^cedures

When the PSA is used to evaluate the design and procedures of the plant then the objective is to evaluate the safety of the plant's design and procedures in terms of the attained core melt frequency and system unavailability. This is basically the standard use of PSAs except that for life extension applications it is exceedingly important that plant specific data be used to reflect the current condition of the plant. Current accident sequence models (event trees) and current system models (fault trees) should be used for the PSA plant model. To quantify the models, the most up to date component failure rates, human error rates, initiating event rates, and common cause prcbabilities should be utilized. If a PSA already exists for the plant then it is important that it be updated to reflect the current conditions of the plant.

There are no time varying effects or time trending incorporated into this use of the PSA to provide guidance in life extension. However, the PSA can be an important tool for showing whether the licensing requirements for the plant are adequate to provide acceptable safety in terms of providing acceptable, long run core melt frequencies, accident sequence frequencies, and system unavailabilities. If the plant was initially licensed under different requirements than the requirements which presently exist, the PS/ can show whether the initial licensing requirements provide adequate safety under the present requirements.

Table 1 summarizes the objectives of carrying out a PSA to evaluate the plant's design and procedures to provide guidance in relicensing of extended plant lifetimes. For each of the objectives, the plant is evaluated witb current data and current models, reflecting the current condition of the plant at the time of relicensing.

2.2 Monitoring the Plant's Safety Performance

A major consideration in life extension applications is the impacts of time varying effects and aging effects on the plant's core melt frequency and system unavailabilities. In the second use of PSA, the PSA is therefore used to monitor the safety performance of the plant in real time. The safety impacts of different plant configurations and different components being down can be evaluated by calculating the pointwise core melt frequency as a

TABLE 1. OBJECTIVES OF CARRYING OUT A PSA TO EVALUATE THE PLANT'S DESIGN AND PROCEDURES

To evaluate the long run, or time independent, core melt frequency and system unavailabilities associated with the design and procedures.

To compare the PSA results with numerical safety criteria or with other PSA results.

To evaluate the adequacy of licensing requirements when the plant was originally licensed.

To evaluate the safety impacts from plant design changes and procedures changes.

To evaluate the impacts of safety issues which are pertinent to the plant.

To evaluate the effectiveness of surveillance and maintenance procedures.

To determine and prioritize human error contributions to focus administrative and procedural upgrades.

To define dominant accident sequences for use in simulation and operator training.

To define and prioritize contributions which should be focused on in start-up activities.

To evaluate dependencies and common cause failure contributions.

To evaluate sensitivities and uncertainties.

function of time. The safety impacts of time trends in failure rates and unavailabilities can also be evaluated by inputting these time trends into the PSA models to determine the time trends in safety performance.

In monitoring the safety performance of the plant, every event which occurs can vary the safety of the plant at that time, and the objective of the second use of PSA is to calculate the PSA results as a function to time to quantify the time variation of the results. The events which are monitored can include components which are down, component failures and downtimes which occur, human errors, initiating event and system demands which occur, and precursor events and common cause failures which occur.

There are basically two approaches which can be used to monitor the plant's safety performance. The plant configuration (which components are up and down) can be determined at given points in time, for example once a day, and the PSA can be calculated at each point in time for each given configuration. Alternatively, components which went down in a given time interval can be recorded along with the time the component went down and the time it came back up. This time interval data can be used to calculate the component and system unavailabilities for the interval including overlapping of component downtimes, which can be input to the PSA to calculate the core melt frequency and other results for the interval. Either the configuration approach and the time interval approach can be used to monitor the plant's performance, as it varies with time, as will be described in more detail later.

In monitoring the safety variations by either the configuration approach or the time interval approach, the objective is to evaluate the plant safety in real time. Plant configurations and component statuses can be identified which cause the core melt frequency to significantly increase at a given point in time. The configurations and statuses can thereby be controlled to limit the core melt probability. Deteriorating time trends can also be identified which result in the system unavailability and core melt frequency increasing with time. The causes for these deteriorating time trends can be identified and can be corrected before an accident occurs.

Deteriorations in structures and materials cannot generally be accurately monitored for their core melt frequency impacts since at present there are no generally available approaches which relate structural failure probabilities to changes in material properties. However approaches hopefully will be developed and will be assembled in the next several years which will allow structural failure probabilities to be more accurately modeled in the PSA. At present, limited probabilistic fracture mechanics models are available, and expert opinions, empirical models, and sensituity studies can be used.

Even with the structure monitoring limitations, the PSA when used as a monitoring tool can provide important information on the real time core melt frequency variations and system unavailability variations from those contributions considered in the PSA.

By having a PSA monitoring process in place for the plant which is being considered for life extension, a mechanism can thereby be established for explicitly monitoring and auditing plant safety in real time. The PSA monitoring process can provide assurance that the core melt frequency and system unavailabilities are being controlled, both before the life extension consideration and after the lifetime is extended, when it is extended. Any unacceptable variations can thereby be quickly identified and can effectively controlled. Table 2 summarizes the objectives of using a PSA to monitor the real time core melt frequency and system unavailabilities of the plant to provide guidance on relicensing and life extension decisions.

2.3 Prediction of the Plant's Future Safety Performance

Finally, as a third use, the PSA can be used to predict the future core melt frequency of the plant, incorporating the plant's design and procedures, as well as the information collected in the monitoring process. In using the PSA to predict the future plant safety performance, the time varying events which are recorded in the monitoring process are analyzed to obtain predictive failure rates and predictive probabilities. These predictive failure rates and predictive probabilities are usually obtained by fitting explicit, parametric models of the time dependent failure rate or probability to the observed data. Unknown parameters in the models are estimated using statistical techniques such as regression analysis or maximum likelihood analysis. Also, engineering information can be incorporated by using Bayesian analysis. The predictive rates and predictive probabilities are then input into the PSA models to predict the future core melt frequency and future system unavailabilities.

TABLE 2. OBJECTIVES OF USING A PSA TO MONITOR THE SAFETY PERFORMANCE OF A PLANT

To check the PSA models, assumptions, and data for their validity in real time.

To monitor the safety impacts from time varying plant configurations.

To monitor the safety impacts from time trends in component failure rates and component unavailabilities.

To track the time-varying impacts of design changes, procedural changes and new regulatory requirements.

To determine the time-averaged core melt frequency, accident frequency, and system unavailabilities over given time intervals to compare with numerical criteria.

To determine the time-varying core melt frequency, accident frequency, and system unavailability from plant records.

To identify abnormally high level of core melt frequency and system unavailability which should be corrected within given action times.

To monitor and audit the real-time effectiveness of maintenance and surveillance testing procedures.

To provide level indicators and trend indicators for reliability centered testing and maintenance.

To evaluate the likelihood of a core melt or a severe accident from a given event, for precursor evaluations.

To evaluate the time-varying impacts of human intrusion and to identify methods for their control.

With regard to providing guidance in relicensing of extended lifetimes, the predictive PSA results can be used to identify future core melt frequency and system unavailability impacts of the time-varying and age-varying failure rates and failure probabilities. The predictive evaluations can thereby be used to identify future time periods of predicted safe operation and time periods in which corrective actions need to be taken. The plant can furthermore be monitored in these future periods to assure that the core melt frequency is maintained and to identify and correct any detrimental variations or trends.

Table 3 summarizes the objectives in using the PSA to predict the plant's future safety performance. The use of the PSA as a predictive tool is the last of the three major uses of PSA for providing guidance in relicensing of extended lifetimes.

TABLE 3. OBJECTIVES IN USING A PSA TO PREDICT FUTURE PLANT PERFORMANCE

To evaluate the future safety implications in terms of core melt frequency and system unavailability implications from time trends and aging deteriorations which are observed.

To evaluate the tolerance of the safety systems and the plant in accommodating various degrees of aging and time trends.

To evaluate the changes in the contributors to core melt frequency and system unavailabilities when aging and time trends occur.

To identify the future time period in which safety in terms of core melt frequency and system unavailability is acceptable to provide a basis for relicensing periods.

To evaluate the effectiveness of proposed aging management and aging control programmes in terms of core melt frequency and system unavailability control.

To identify and prioritize contributors to predicted deteriorating safety performance and to identify effective fixes for these contributors.

To identify further data and analyses needed to reduce uncertainties in predicted core melt frequency and safety system unavailabilities.

To identify the future time periods in which the safety will have to be re-evaluated to reduce the uncertainties and to account for changes and trends in performance.

3. THE ANALYSES WHICH ARE INVOLVED IN APPLYING PSAs TO LIFE EXTENSION EVALUATIONS

As indicated in the previous section, the different applications of PSA can provide important information for life extension decision-making by evaluating the plant's design and procedures, by monitoring the plant's safety performance , and by predicting the plant's future safety performance. Each of the different applications of the PSA involve different analyses. The following sections describe the analyses which are involved in each of the different PSA applications and give specific examples of the analyses.

3.1 Analyses Involved when Using the PSA to Evaluate the Safety of the Plant's Design and Procedures

The requirements for using a plant specific PSA to evaluate the plant's design and procedures are the usual requirements for a standard PSA. However, as was indicated, for life extension applications it is especially important that current event tree and fault tree models and current data be used. The model and data requirements are summarized in Table 4. Table 4 is useful as a checklist since it highlights the requirements which are important for life extension applications. The PSA Handbook (1) prepared by IAEA describes the models and data required for a PSA and hence further details are not given here. Standard PSA requirements are also given in References 2 and 3. Appendix C gives the internal initiating events which generally should be considered for a PWR and a BWR. Appendices D and E give the safety functions and safety systems which generally considered for a PWR and a BWR.

3.2 Analyses Involved When Using the PSA to Monitor the Safety Performance of the Plant During Operation

As indicated in the previous sections there are two basic approaches which can be used to monitor the plant's safety performance - to monitor the plant configurations and to monitor the time interval changes. When the PSA is used to monitor plant configurations, then the PSA is basically recalculated at different points in time with components known to be down and other components known to be up at each time point. The core melt frequency and other PSA results are then calculated for the particular configuration.

TABLE 4. MODELING AND DATA REQUIRED TO EVALUATE THE PLANT'S DESIGN AND PROCEDURES

A set of event trees for all the initiating events which are considered, including external events considered. The event trees need to be developed to a system level.

A set of fault trees for all the system failures which are considered, which includes both front line system failures and support system failures. The fault trees need to be developed at least to a major component level.

A list of the components which have interdependencies and for which common cause failure probabilities are quantified (e.g. using the beta factor approach).

A list of accident sequence minimal cut sets for which recovery actions are included and are to be quantified.

A list of components which cannot be down at the same time because of technical specification requirements or regulatory requirements.

A list of all the components whose configurations are changed when a given component is down.

A failure rate data base consisting of initiating event frequencies, component failure rates, human error rates, recovery probabilities, common cause probabilities, and with their uncertainties.

An external data base set consisting of initiating frequencies, transmission and response probabilities and component fragilities, along with their uncertainties, for all the external events considered.

A computer code package which determines the accident sequence and system minimal cut sets, and which quantifies the core melt frequency and other PSA results along with their uncertainties.

By calculating the core melt frequency (and other PSA results) at a set of time points a time history is thereby obtained of the pointwise core melt frequency.

In terms of the actual calculations required, let

F_i = the core melt frequency at time point t_i (1)
for a given configuration C_i

When C_i is a given set of components known to be up and other components known to be down, then F_i is calculated by initializing those components to be down or up in the fault trees. The initialization of the components involves turning component fault states "on" for those components which are down and turning component fault states "off" for components known to be up. The core melt frequeny F_i is then calculated under this condition.

Figure 4 illustrates the type of results that will be obtained when the core melt frequeny F_i is calculated at different time points t_i. The figure shows the core melt frequency monitored every hour, although any other time sequence could be used. In general, the core melt frequency can vary

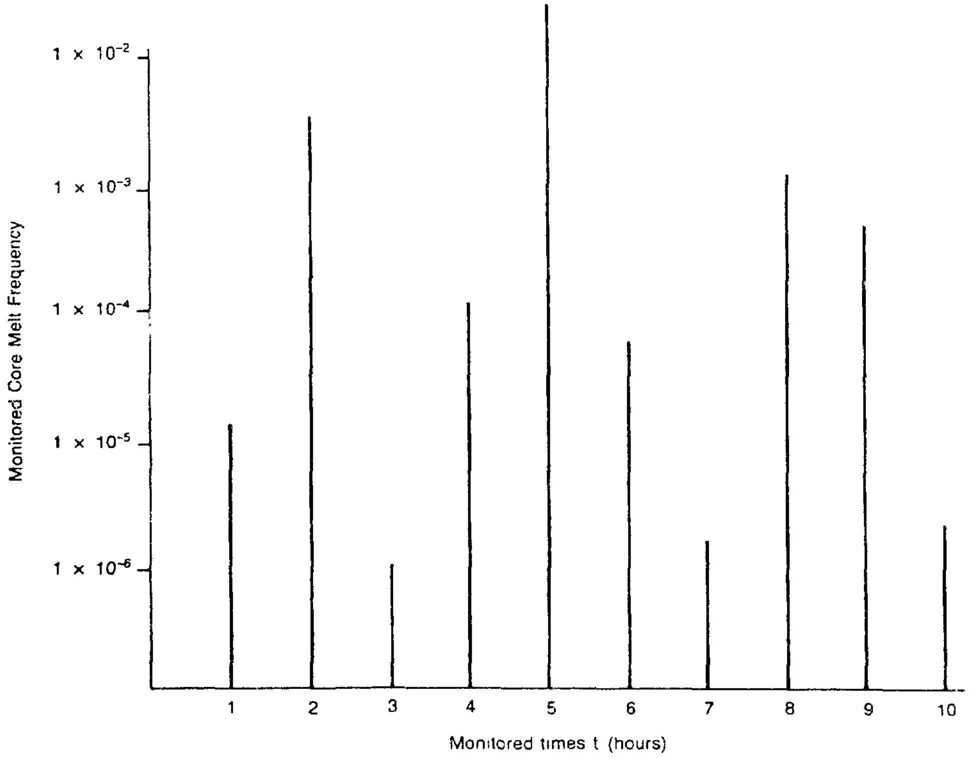

FIG.4. Monitored core melt frequency as a function of plant configuration.

significantly, by orders of magnitude, when multiple components are up and down, and hence optimally the time points need to be spaced to cover every configuration change. The time-averaged core melt frequency over a period, such as over three months or over a year, are obtained by averaging the pointwise core melt frequency.

If

F_T = The average core melt frequency in an interval T which contains $t_1, t_2 \ldots\ldots t_n$ then (2)

$$\bar{F} = \frac{\sum_{i=1}^{n-1} F_{i+1} (t_{i+1} - t_i)}{t_n - t_1} \qquad (3)$$

The above formula calculates F_T as a simple histogram approximation. More detailed numerical integration formulas can also be used such as Simpson's rule are detailed quadrature formulas. It is the time-averaged values F_T which should be compared to numerical criteria or should be evaluated for trends. In comparing to numerical criteria, T can be taken to be one year and in evaluating for trends T can be taken to be a smaller period such as three months. For trend evaluations F_i can also be smoothed using various smoothing algorithms.

As was indicated, because F_i can vary significantly, the points t_i should be close enough to include major configuration changes. In using the PSA models to calculate F_i, standard PSA evaluations are performed except that the configured component fault states are set "on" or "off" as was indicated. If a list of minimal cut sets is used to calculate F_i then the cut sets should have a low truncation point (eg. 1×10^{-12}) to ensure that neglected cut sets do not become important when multiple components are down. A better approach is to use the original event trees and fault trees to obtain new minimal cut sets for each configuration and then quantify these new minimal cut sets. Table 5 summarizes the analyses which are involved in using the PSA to monitor plant configurations.

TABLE 5. ANALYSES AND DATA INVOLVED IN USING THE PSA TO MONITOR THE SAFETY IMPACTS OF PLANT CONFIGURATIONS

The basic PSA models and data in Table 4 are required plus the following:

As additional data, the components which are known to be down and those which are known to be up at a given time.

Other components which are reconfigured because components are down need to be incorporated in the PSA models.

Components which are not known to be up or down are assigned the most current failure rate data.

Components which were just recently tested but which are not known to be up or down, can be modeled more precisely by using as the test interval the time since the last test.

If the statuses of only a few components are known then there can be little information obtained from the PSA evaluation; this can be used to determine whether new calculations need actually be performed.

The computer package used to quantify the PSA should be highly efficient to allow the PSA results to be obtained in little time (e.g. less than 5 minutes).

If the duration of a configuration is known, for example defined by technical specifications, then the duration can be used in the integration of the pointwise PSA results to yield more accurate time-averaged results.

As an alternative to monitoring plant configurations, the plant safety performance can also be monitored by evaluating the failures and downtimes which occur in successive time intervals. The failures and downtimes which occur in a time interval are used to update the component unavailabilities for the time interval. The updated component unavailabilities are then input to the PSA to obtain an updated core melt frequency for the interval. These evaluations are repeated at successive time intervals to obtain a sequence of core melt frequency values for the successive time intervals.

The type of results which are obtained from time interval monitoring is illustrated in Figure 2. The specific data which needs to be collected for each time interval (such as each month) consists of:

The number of hours the reactor was operating (the critical hours)

The component that was taken down or was failed and the time the component was taken down (or was detected to be down)

The reason the component went down (i.e. for maintenance or testing, or because of failure)

The time the component was restored to operation

Whether the component was still functional during the downtime (if the downtime was due to test or maintenance)

The time the component was last tested or demanded (if the downtime was due to failure)

The cause of the downtime (e.g. the component subpart that failed or that was maintained)

The component downtime data in the above list are recorded for all these components which are to be monitored. The cause of the downtime (the last item above) is not absolutely necessary but it is important in allowing causes of trends and causes of unacceptance behaviors to be diagnosed. Less detailed data than that given above can be recorded, however the monitoring will be accordingly less detailed. The appendix gives an example of a less detailed but still extremely useful scheme.

With the above data, the safety impacts of failure rate changes and unavailability charges, including configuration impacts, can be monitored. The component unavailability q for the interval is computed as

$$q = \frac{D}{L} \qquad (4)$$

where

D = the total component downtime in the interval (5)

and

L = the critical hours in the interval (6)

The total downtime D in the interval is determined as from the equation:

$$D = D_M + D_F \qquad (7)$$

where

D_M = the downtime due to repair and maintenance (8)

and

D_F = the additional undetected downtime due to failure (9)

D_M is the measured maintenance and repair downtime and is the difference between the time the component was restored and the time the component went down (or was detected to be down) as recorded in the database. D_F is the undetected downtime during which the component was failed and is estimated as one half the difference between the time the component was detected and the time the component was last tested or demanded. For periodic surveillance testing D_F can be estimated as one half the test interval. If the component is continously monitored then $D_F = 0$.

The above component unavailabilities q can be directly input into the PSA evaluations, however they are generally first smoothed before they are input. Various smoothing schemes can be used such as exponential weighting, running average smoothing or a Bayesian updating. The appendix describes a smoothing approach using the past three downtimes which has given useful results in practice.

Plant configuration impacts are handled by accounting for components which are down at the same time. For example, if from the recorded data two components, say component 1 and 2, went down at different times and had an overlapping downtime interval of D_{12} then the unavailability contribution q_{12} from both components being down is

$$q_{12} = \frac{D_{12}}{L} \tag{10}$$

Where again L is the critical hours in the interval. This unavailability contribution can be included in the PSA evaluations and can replace the independent contribution (where the two individual component unavailabilities q_1 and q_2 are simply multiplied).

If technical specifications or other regulatory requirements do not allow two components to be down for maintenance or repair at the same time then this can be reflected in the system unavailability which is constructed from the monitored component unavailabilities q. For example, the unavailability Q_{12} of two components being down, corrected for technical specification, can be calculated as:

$$Q_{12} = q_1 q_2 - q_{1M} q_{2M} \tag{11}$$

Here q_1 and q_2 are the total component unavailabilities (Equation (4)) and q_{1M} and q_{2M} are the maintenance downtime contributions,

$$q_{1M} = \frac{D_{1M}}{L} \tag{12}$$

and

$$q_{2M} = \frac{D_{2M}}{L} \tag{13}$$

and where D_{1M} and D_{2M} are the component maintenance and repair downtimes on the interval. Again the smoothed values for q_1, q_2, q_{1M} and q_{2M} can also be used in Equation (11).

Figures 5A and 5B illustrate specific examples of the output obtained from interval monitoring at a plant. The monitoring was applied at a system level and gives the system unavailability per quarter (every 3 months). The numbers on the x-axis refer to specific quarters, e.g.

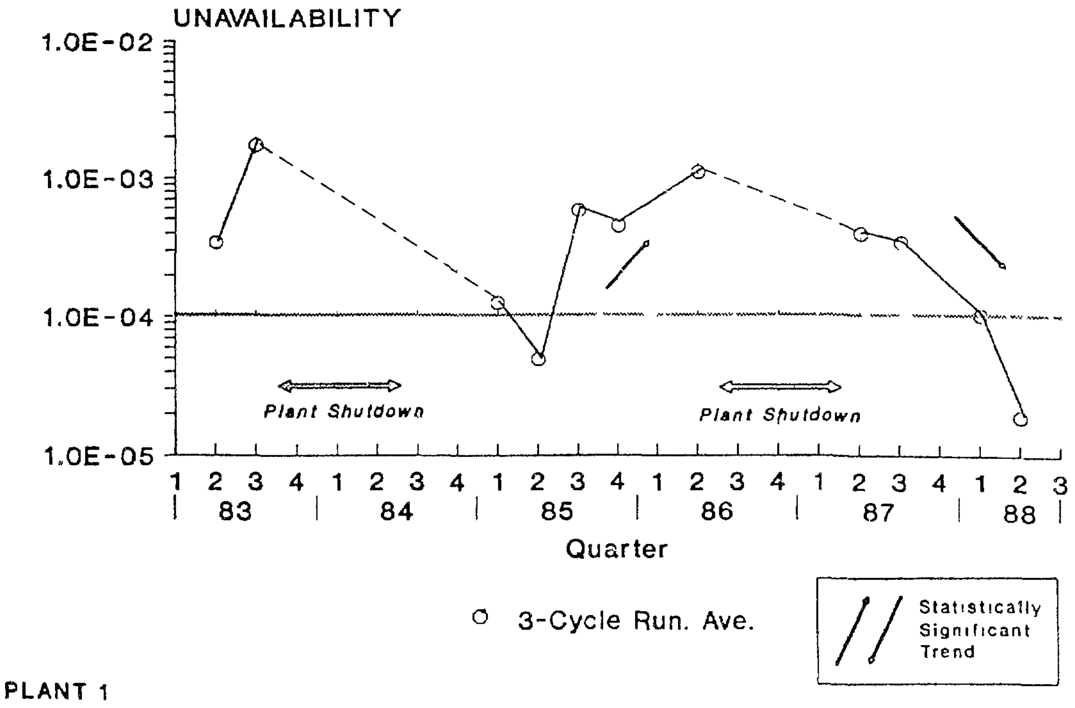

FIG.5A Quarterly aux-feed system unavailability based on (per train)**3.

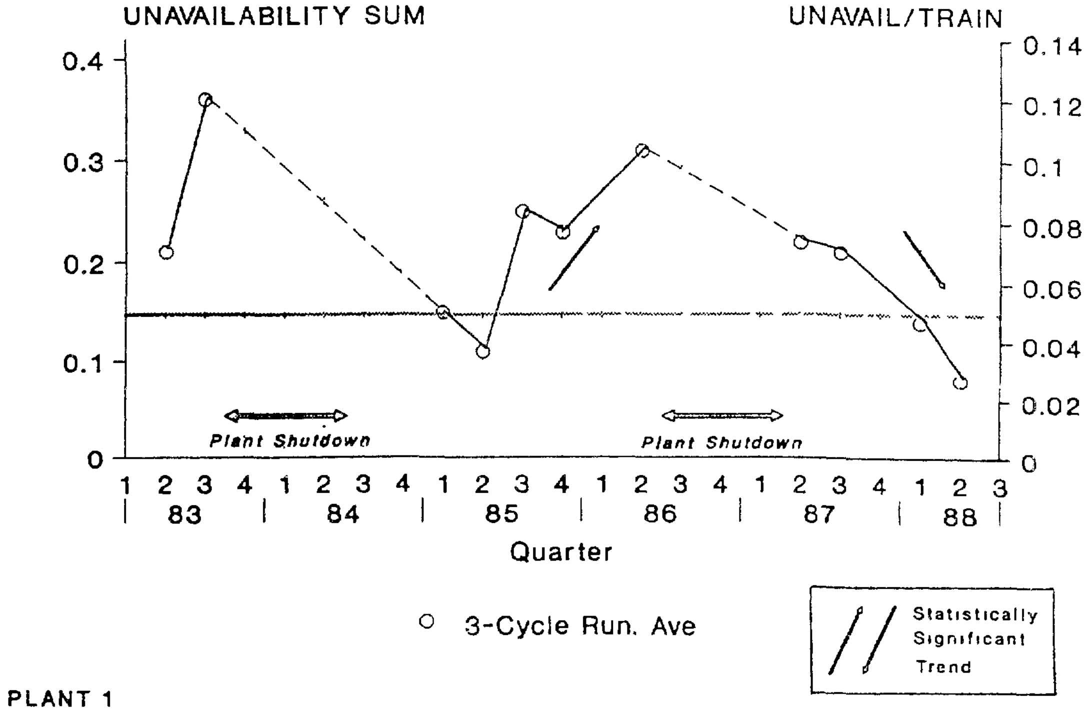

FIG.5B. Quarterly aux-feed system unavailability (3-train aggregate).

84-1 is the first quarter of 1984. The horizontal line is the guideline valve (at 95% confidence). More details of the analyses are given in Appendix F. Table 6 summarizes the analyses and data which are involved in using the PSA to monitor the plant safety performance through time interval monitoring.

TABLE 6. ANALYSES AND DATA INVOLVED IN USING THE PSA TO MONITOR SAFETY PERFORMANCE THROUGH TIME INTERVAL MONITORING

The basic PSA models and data in Table 4 are required plus the following:

The times of downtimes and the duration of downtimes need to be recorded for each component along with the reason and cause for the downtime.

The times of occurences of initiating events can be recorded to also update the initiating event frequency in the interval.

The interval in which data are recorded represencs the lag in the process; quarterly or monthly intervals have worked reasonably well.

The monitoring can focus important active components for which data are generated most frequently.

Different individual components of the same type can be aggregated to reduce uncertainties; the individual component data can be checked to assure they are statistically similar.

The interval estimates of the component unavailabilities should generally be smoothed before inputting to the PSA to better identify time trends.

If component and structural failure rates have been related to engineering variables and material properties, then the engineering variables and material property changes can be monitored to obtain failure rate changes and unavailability changes.

Uncertainties can be propagated for the monitored results by using standard PSA propagation techniques on the time interval data.

3.3 Analyses Involved When Using the PSA to Predict the Future Safety Performance of the Plant

To use the PSA to predict future plant performance, component failure rates which are not constant must be expressed as explicit functions of time. Similarly, non-constant initiating event frequencies must be expressed as explicit functions of time. If structural failure rates are utilized in the PSA and they are modeled as being non-constant then they also must be expressed as explicit functions of time. This is futhermore true for any other data used in the PSA such as human error rates if the effect of observed or hypothesized time dependence on aging is to be considered.

To obtain explicit functions of time, the usual approach is to fit a parametric function to the data. The Weibull model is often used to predict future performance since it is a flexible model and straight forward to apply. Computer codes also exist which utilize Weibull future rates in PSA evaluations (9,10). If $\lambda(t)$ is the time dependent component failure rate then the Weibull failure rate model is given by

$$\lambda(t) = at^{b} \qquad (14)$$

where a and b are parameters which are estimated from the data and where t is time or another relevant age measure. If $b = 0$ then the Weibull failure rate reduces to the standard constant failure rate allowing statistical tests to be performed to test for time dependence. If $b = 1$ then the Weibull model reduces to the linear failure rate model which has been used in aging evaluations (11).

Sometimes a translation parameter t_o is incorporated in the Weibull failure rate model, which then becomes

$$\lambda(t) = a(t-t_o)^{b} \;;\quad t \geq t_o, \qquad (15)$$

where for $t < t_o$ the standard constant failure rate model is used.

If $\lambda(t)$ represents only the time dependent contribution then the total component failure rate is the constant failure rate due to random causes plus the time dependent failure rate. If $\lambda_T(t)$ represents the total component failure rate and λ_o the constant failure rate then $\lambda_T(t)$ is given by

$$\lambda_T(t) = \lambda_o + \lambda(t) \qquad (16)$$

The data requirements for the above models are basically the same as the data requirements for using the PSA as a time interval monitoring tool and given in the previous section. There is one piece of additional data required if the variable t in the equations is taken to be the age of the component. In this case, the extra piece of data required for the component is the time of installation of the component, or the time at which the component was overhauled or basically renewed. If t_I is the time of installation or renewal of the component and t_p is the present time then t in the above equations is replaced by

$$t = t_P - t_I \qquad (17)$$

To actually use the above models in practice the times of failure of a component are fit by a likelihood function which describes the probability of the data being observed. The likelihood function L for one component is defined to be

$$L = \lambda(t_1)\ \lambda(t_2)\ \ldots .\ \lambda(t_n) \exp\left(- \int_o^{t_{max}} \lambda(t)\, dt\right) \qquad (18)$$

where $t_1,\ldots t_n$ are the failure times and t_{max} is the maximum observation time. If the component is observed only until the nth failure then t_{max} = t_n. If the component is observed to a fixed time, then t_{max} is the fixed time. The failure rate $\lambda(t)$ is given by equation (14) (or by equation (15) or (16) if the more detailed models are used). The equations for $\lambda(t)$ can be substituted into equation (18) to obtain the likelihood as an explicit function of the parameters a and b (and t_o and λ_o for the more detailed models).

The likelihoods of similar components which are assumed to have the same failure rate can be multiplied together to obtain the overall likelihood. The assumption of the same failure rate can always be tested using standard likelihood ratio approaches. The likelihood function is then maximized to obtain the best estimates (maximum likelihood estimates) of the parameters. Alternatively, Bayesian approaches can be used to obtain posterior estimates of the parameters. Uncertainties can be obtained from the information matrix which is obtained in the maximum likelihood approach or from the Bayesian distributions.

The above approaches model minor repairs on the component (such as replacing specific pieceparts) as not affecting the overall failure rate. If the component is replaced or overhauled then this is treated as a new component with the associated installation time. In more detailed modeling, each piecepart of the component (e.g. a pump shaft, pump rotor, etc) is modeled as having its own failure rate.

Once the parameters of the time dependent failure rates are determined, then PSA computer codes can be used to predict the core melt frequency and other PSA results. Either time dependent fault tree evaluation codes can be used (e.g. FRANTIC) or the time dependent failure rate can be approximated by step functions of different constant failure rates and standard PSA codes repeatedly run for these different steps.

The above approaches can be applied not only to individual component failures, but to observed times of human errors, common cause failures, and structural failures. The above approach can also be applied to times of degradations if the degradations are related to failures (for example multiplying the degradation rate by a factor failure rate conversion).

For example, changes in material properties in strutures can be proportioned to give the same ratio for the change in the structural failure rate. If the structural failure rates is expressed as an explicit function of material properties then changes in the material properties can be used to estimate the associated time dependent structural failure rate.

Finally, in cases where no detailed failure time data has yet been collected then the above models can be further simplified to the linear failure rate model to study the predicted effects of aging effects or time dependent variations. The linear aging model is also useful for sensitivity studies to initially prioritize the safety impacts of potential aging effects.

The linear failure rate model is given by

$$\lambda(t) = \lambda_o + bt \qquad (19)$$

where $\lambda(t)$ is the time dependent component failure rate, λ_o is the baseline, or constant failure rate, and b is the linear rate parameter.

When there is not failure time data, the parameter b can be grossly estimated as

$$b = 2 \frac{f}{1 - f} \frac{\lambda_o}{M}$$

where f is the fraction of failures which is associated with aging mechanisms and M is the present age of the plant (see Reference 11). The constant failure rate λ_o can be taken to be the standard PSA constant failure rate.

Table 7 summarizes the analyses, data, and application considerations involved in using the PSA to predict future plant safety performance.

TABLE 7. ANALYSES AND DATA INVOLVED IN USING THE PSA TO PREDICT FUTURE SAFETY PERFORMANCE

The basic PSA models data in Table 4 are required plus the following:

Analysis techniques to translate observed times of one or more occurrences of an initiating event into a time dependent or age dependent, predictive initiating event frequency with associated uncertainties.

Analysis techniques to translate observed times of one or more occurrences of a component downtime and its associated duration into a time dependent or age dependent, predictive component unavailability with uncertainties.

Analysis techniques to translate observed times of occurrences of human errors into a time dependent or age dependent, predictive human error rate with associated uncertainties.

Analysis techniques to translate observed times of occurences of common cause failures into a time dependent or age dependent, predictive common cause probability with uncertainties.

Analysis techniques to translate the observed times of occurrences of precursor events into a time dependent or age dependent, predictive sequence frequency contribution.

If PSA data are related to environmental and programmatic variables, then analysis techniques to estimate time dependent or age dependent, predictive variable values with associated uncertainties.

For age dependent component failures rates, test and maintenance models which reflect the effectiveness in controlling the aging failure rate.

4. SPECIFIC WAYS GIVEN PSA CRITERIA CAN BE UTILIZED FOR EACH OF THE DIFFERENT PSA APPLICATIONS

To assist in utilizing the PSA results for decision making, numerical criteria can be used to assess the acceptability of the results for each of the different PSA applications. Numerical criteria have been defined in various references to help assess the acceptability or unacceptability of calculated PSA results (see for example References 12 and 13). Table 8 gives specific criteria which are representative of the criteria values which have been presented in the various references. The rationale that is presented for the criteria in the various references is not limited to any specific PSA application, and hence the same criteria, with suitable interpretations, can

TABLE 8. REPRESENTATIVE CRITERIA VALUES FOR SPECIFIC PSA RESULTS

PSC Results	Criteria Per Year
Individual personal risk from severe accidents	$< 1x10^{-6}$
Frequency of major releases of radioactive materials	$< 1x10^{-6}$
Containment failure	$< 1x10^{-1}$ *
Core-melt frequency	$< 1x10^{-5}$
Individual accident sequence frequency	< 10% contribution

* per core melt

be used for all the different types of PSA applications which have been addressed here. Table 9 gives the interpretations which make any set of criteria values consistent and applicable when using the PSA for evaluating the plant's design and procedures, when using the PSA for monitoring the plant's performance, and when using the PSA to predict the plant's future performance. The sections below discuss these interpretations in somewhat more detail.

TABLE 9. INTERPRETATIONS OF CRITERIA FOR THE DIFFERENT PSA APPLICATIONS

EVALUATION OF THE PLANT'S DESIGN AND PROCEDURES
Use the criteria directly to assess the acceptability or unacceptability of the PSA results.
MONITORING OF PLANT PERFORMANCE
Interpret the criteria as applying to the PSA result averaged over a year. Therefore, translate the monitored PSA result to obtain the yearly average PSA contribution and compare the translated yearly average contribution to the respective criteria.
PREDICTION OF PLANT PERFORMANCE
Apply the criteria to the calculated yearly average PSA results for future times or ages. If, when considering uncertainties, the calculated results become higher than the criteria at a future time then re-evaluation at or before this time is indicated.

4.1 Interpretation of the Criteria when Evaluating the Plant's Design and Procedures

As Table 9 indicates, when the PSA is used to evaluate the plant's design and procedures (the top entry in the table) then the given criteria, such as those represented in Table 8, are applied directly to the calculated

PSA results to assess their acceptability or unacceptability. This is the usual application of the criteria and there is no need to reinterpret the criteria.

4.2 Interpretation of the Criteria when Monitoring the Plant's Performance

When the PSA is used to monitor the plant's performance (the middle entry in the table), the monitored PSA results need to be translated into yearly average results to obtain the results in the same units as standardly defined in the criteria. The yearly average results are then compared to the respective criteria values.

For example, if the monitored core melt frequency is observed to have a value of C_1 for a time period P_1 and a value C_2 for a time period P_2, where $P_1 + P_2$ is less than one year, then the yearly average core melt frequency value C is

$$C = \frac{C_1 P_1 + C_2 P_2}{T}$$

where T is the time in a year, in the same units as P_1 and P_2. The above interpretation assures that the contribution over the observed time period does not exceed the yearly contribution defined by the respective criterion value when proportioned (or prorated) by the observed time period.

4.3 Interpretation of the Criteria when Predicting Future Plant Performance

Finally, when the PSA is used to predict the future plant performance as the bottom entry in Table 9 indicates, the calculated, future yearly average results are compared directly to the criteria values. This is again consistent with the yearly average interpretation standardly given to the criteria.

5. SPECIFIC STEPS WHICH CAN BE IMPLEMENTED FOR USING PRESENTLY AVAILABLE PSA MODELS, DATA AND GIVEN CRITERIA TO ASSIST LIFE EXTENSION DECISION MAKING

Tables 10, 11, and 12 describe the specific steps that can be taken to apply presently available PSA approaches to assist life extension decision making by again:

1. Evaluating the plant's design and procedures,

2. Monitoring the plant's performance,

and

3. Predicting future plant performance.

These tables are self explanatory and require no additional discussions.

TABLE 10. PRESENT STEPS WHICH CAN BE CARRIED OUT TO APPLY A PSA TO EVALUATE THE PLANT'S DESIGN AND PROCEDURES

1. If the plant does not have a plant specific PSA, then a plant specific PSA should be performed to evaluate the safety of the plant's design and procedures. The PSA should at least evaluate the core melt frequency and include the significant accident initiators.

2. If the plant already has a plant specific PSA then the PSA should be updated to evaluate the present safety of the plant's design and procedures. The PSA should evaluate the core melt frequency and include the significant accident initiators.

3. To assist in decision making, the PSA results should be compared to given criteria to determine the acceptability of the results. If the results are above the acceptable values additional assessments should be carried out to identify the most effective means of lowering the PSA results.

4. The PSA models and data should be updated at least every two years. Whenever the models or data have changed, then the PSA needs to be requantified as described in the preceding steps.

TABLE 11. PRESENT STEPS WHICH CAN BE CARRIED OUT TO APPLY A PSA TO MONITOR THE PLANT'S PERFORMANCE

1. A data collection programme can be implemented at the plant to collect, for each PSA contributor, the times of occurrence and duration times, where relevant, of the event (the first six items in Table 6).

2. The above data should be collected on all the initiating events, major components, human errors, and common cause failures in the PSA to monitor the safety performance from these contributors.

3. To provide a baseline for life extension decision making, the data collection programme should be implemented as soon as possible before the life extension consideration, ideally at least five years before the life extension consideration.

4. Core melt frequency implications and system unavailability implications from plant configurations and from the monitored data should be evaluated to monitor the time varying safety performance of the plant.

5. The monitored PSA results should be compared to criteria and if they become unacceptable then assessments should be made as to how to correct these deviations. This monitoring process can provide a basis for helping to assure safe operation before and after the life extension consideration.

TABLE 12. PRESENT STEPS WHICH CAN BE CARRIED OUT TO APPLY A PSA TO PREDICT THE PLANT'S FUTURE PERFORMANCE

1. When there is sufficient data to identify trends, then predictive failure rates, initiating event rates, human error rates, and common causes rates should be estimated to be input into PSA predictive evaluations.

2. The predictive rates and probabilities should be updated at least every two years after the data collection programme has been implemented to update the predictive data evaluation.

3. Each of the tests and maintenances identified in the PSA models should be evaluated to determine their effects in controlling aging effects and surveillance inefficiencies.

4. The predictive data, and updated test and maintenance models, should be utilized to predict future core melt frequency and system unavailabilities, and their associate uncertainties for the next five years, or other appropriate future time period.

5. The future PSA results should be compared to respective criteria to determine their acceptability in the future time period.

6. If the PSA results, including uncertainties, are above the criteria then appropriate actions need to be taken. These can involve improving tests or maintenances, overhauling equipment, replacing equipment, and re-evaluating the PSA.

6. MODELING AND DATA RESEARCH THAT CAN BE CARRIED OUT TO EXTEND THE APPLICABILITY OF PSAs FOR ASSISTING LIFE EXTENSION DECISION MAKING

As the final section of this report, Tables 13 and 14 identify modeling and data research that can be carried out to extend the applicability of the PSA for monitoring purposes (Table 13) and for predictive purposes (Table 14). The tables also identify the new and extended applications that could be carried out if these modeling and data developments were completed. The tables are again self explanatory in terms of the research efforts which can be carried out.

TABLE 13. MODELING AND DATA RESEARCH TO EXTEND THE APPLICABILITY OF PSAs TO MONITOR PLANT PERFORMANCE

1. Extend computer codes used for status monitoring applications to be able to more efficiently handle complete fault trees and event trees, and not only a truncated set of minimal cut sets. This will provide accurate PSA results even when multiple components are down.

2. Extend the computer software algorithms used for status monitoring to be able to handle components that are known to be up and to incorporate times since last surveillance test. This can provide for more accurate, and less conservative, monitoring.

3. Develop software to automatically link the monitoring data analyses to the PSA models to provide automated outputs of PSA results.

4. Incorporate uncertainty calculations into the PSA monitoring evaluations to provide real time PSA results with their uncertainties.

5. Extend the data analysis approaches by incorporating pattern recognition approaches and fuzzy set approaches to more effectively identify pattern and trends in PSA monitoring.

6. Explicitly relate initiating event frequencies, component unavailabilities and other PSA data to more basic engineering and programmatic variables to provide faster response times and to identify causal variables.

7. Extend current probabilistic fracture mechanic approaches to explicitly relate structural failure rates to material properties, including aging effects, to allow more effective monitoring of structural components.

TABLE 14. MODELING AND DATA RESEARCH TO EXTEND THE APPLICABILITY OF PSAs TO PREDICT PLANT PERFORMANCE

1. Incorporate uncertainty evaluations into time dependent and PSA calculational approaches.

2. Incoporate sensitivity and importance evaluations into time dependent and PSA calculational approaches.

3 Develop automated and rule-based approaches for extracting trends from recorded events to produce predictive failure rates and other predictive data.

4. Extend PSA test and maintenance models to cover cases between "good as new" and "good as old" to allow more accurate evaluations of test and maintenance effectiveness in controlling aging.

5. Develop procedures and rules for translating engineering descriptions ot test and maintenance procedures into reliability models involving "good as new", "good as old", or more complex models.

6. Explicitly relate PSA input data (failure rates, etc) to basic engineering and programmatic variables to obtain predictive estimates which are related to basic engineering and programmatic variables.

7. Extend current probabilistic structural mechanic approaches to predict structural failure rates as a function of time-dependent material properties.

Appendix A

SUPPORTING DOCUMENT ON USE OF PSA FOR EXTENDING LIFETIMES OF NUCLEAR POWER PLANTS

Life Extension of Nuclear Power Plant

1. The issue of concern is the continuing safety of nuclear power plants as they approach the end of their original design lifetime. There are generally three aspects to this problem:

(a) Changes in the state of knowledge about plant behaviour with respect to safety

(b) Changes in safety philosophy and safety standards

(c) Assessment of the current state and possible degradation of plant items which have undergone deterioration with time.

2. Taking these aspects in turn, the contribution of an existing plant PSA can be discussed. It is assumed that a PSA has been performed recently for the plant under discussion.

(a) State of Knowledge

As a result of both plant operating experience and research programmes many plant safety issues have been highlighted over the last 20-30 years. In general these issues were not known at the design stage of our older nuclear power plants and therefore those designs did not specifically address those issues. The question therefore arises, were these issues adequately covered within the plant design and, if not, does it matter from a safety viewpoint?

Take for example our knowledge about material properties and their behaviour under irradiation or under various environmental conditions e.g. water chemistry. Over the last decades we have become aware of a number of material susceptibilities which were not known when some of our older plants were designed. The first task is therefore to review the plant specification to see whether these new susceptibilities are relevant. In many cases the original conservatism of the plant design will be such that even with our new knowledge there is no cause for concern.

The original conservatism often existed because of the relatively unsophisticated methods of analysis available at that time. While the use of those same methods or standards would sometimes not eliminate concern about new material susceptibilities more modern analysis methods will frequently demonstrate adequate safety margins.

In some cases it is not clear that the plant design does adequately incorporate margins against the new material susceptibilities and then the question is does it matter from a safety viewpoint? Here the PSA can provide a very useful perspective. The PSA may provide information such as:

(i) What are the safety consequences of the particular component/material failure in question?

(ii) What is the resulting frequency contribution to significant core damage accidents and how does this compare to the existing frequency of such accidents?

(iii) Can the consequences of the particular component material failure be adequatley mitigated by improvements in performance or reliability of other plant safety functions?

Where the plant PSA has been supported by the collection of data from operational experiences it may be possible to demonstrate that this specific plant performance has been better than the original safety analysis assumptions. Such improved plant performance may help to offset the detrimental effects of the new material susceptibilities now being recognised. These improvements may be in, say, inspection effectiveness leading to reduced initiating event frequencies or in a more accurate calculation of plant fatigue life due to fewer than expected operational cycles.

(b) Safety Philosophy and Standards

As the technology of safety analysis has developed and as the public awareness of safety issues has increased so there have been changes in the approach to the safety justification of nuclear power plants. Particular issues have been the consideration of accidents beyond the plant design basis, the requirement to demonstrate safety against a wider range of potential accidents including external events and the recognition of the need to analyse non-engineering aspects such as human reliability. Consideration of the life extension for a nuclear power plant often acts as a catalyst to focus attention on all these issues for a specific plant. It may therefore become a condition for continued operation that these issues are addressed and satisfactorily resolved over a relatively short period of time.

A PSA provides a uniquely appropriate framework within which to prioritise and assess these issues. The assessment may involve consideration of:

(i) A more realistic analysis of the likelihood of particular reactor events and of the plant response to such events. The original plant safety justification sometimes made unnecessarily pessimistic assumptions because there was at that time no need to be more realistic.

(ii) Incorporation into the safety analysis of plant features or systems which had not previously been considered. These may for example include components that have a higher specification than the original plant design recognised and areas where our improved knowledge allows us to claim higher integrity or improved reliability.

(iii) Evaluation of potential hardware modification or procedural changes. It may be possible to demonstrate that, by relatively minor changes to existing safety systems or by changes in the method or frequency of plant maintenance, inspection and testing, the new safety targets can be met.

(iv) Finally it may be possible to demonstrate that particular safety concerns make such a small relative contribution to plant safety that it is inappropriate to incur the costs of plant modification.

(c) Current Plant State and Potential Degradation

In the original plant safety case it would have been typical to assume that items of plant which were known to experience degradation with time or operational history had a capability or integrity appropriate to the end of the design life. Thus allowance would have been made for maximum expected corrosion, radiation embrittlement, fatigue life exhaustion etc. Life extension therefore requires an evaluation of the current state of such components based on the actual history and a justification of continued acceptable capability over the new extended life. It is frequently possible to show that the original assumptions of degradation were very pessimistic or that the safety margins in the original component design were higher than originally assumed. In both cases it may be possible to demonstrate that life extension is acceptable without component replacement or refurbishment. This process of assessment is generally a deterministic analysis which aims to demonstrate that the safety margins will be achieved.

There generally will be no connection made between this assessment of component capability and the probability of component failure. The rationale appears to be that the failure probability is unchanged provided that it can be shown that the component meets the specified design requirements after incorporating the predicted degradation effects.

In addition to the expected degradation of plant components there are also areas where specific plant deterioration has unexpectedly occured. These may frequently be situations where cracks have been discovered in particular components and therefore a specific safety analysis has been performed to demonstrate that acceptable safety margins exist despite these known cracks. As a general rule this safety analysis has been deterministic and has not been reflected in the probabilities of component failures.

As for previous considerations PSA can provide a useful perspective to assess the sensitivity of plant safety to the expected and known plant state. However the PSA probabilities do not generally reflect the degraded conditions which exist for some components or will occur over a period of time for others.

3. Possible Alternative Approaches

As noted in 2(c) PSA has in the past generally not specifically reflected expected or known degradation in component capability particularly for passive structural components. Indeed PSA has always had some difficulty in modelling the structural failure contributions to plant safety. Consider for example the plant safety issues which originate in structural issues:

(a) LOCA Intitiators

- Steam Generator Tube Rupture
- Failure of Pressure Shells - RPV, Pressurizer
- Primary Circuit Components - Pumps, Pipework, Valves
- Loose Parts from RPV Internals

(b) Transients and Safety Systems

- Control Rod Failures
- Steam Generator Shell
- Pump Valve and Pipework Failures- MSIV, AFW, Accumulators
- Seismic, Aircraft Crash, Missile Impact, Blast Response - Internal Sources of Missiles e.g. Turbine, Deaerator, Steam drums

(c) Containment

- Containment Isolation
- Containment Failure

Most of these issues are presently incorporated into PSA in a rather general way using failure rates based on generic incident information or expert judgement. In particular cases there have been more formal analysis to derive a failure probability for specific components. One example is the RPV for Sizewell, where a probabilistic fracture mechanics (PFM) model was used to incorporate the distributions of various parameters including:

o flaw distribution
o NDT failure to detect particular flaw sizes
o material property variation
o changes of material properties through life

These distributions were then combined to evaluate the probability of the vessel exceeding its design criteria. The analysis was used to demonstrate

- o the low probability of failure
- o the important activities e.g. ND examination, which have an impact on the failure probability

In principle detailed structural models could be developed for most, if not all, structural components of safety interest and failure probabilities derived. While the absolute validity of such models may be questionable such models do provide an explanation of the failure probability derivation and can be used to examine the significance and impact of any events (cracks, NDE failures etc) which occur during plant life.

In the absence of such models it has been customary to develop specific arguments to support the acceptability of particular defects which arise. These arguments may be a combination of probabilistic and deterministic features. Take as an example a problem on a prototype reactor:

> Following an incident in which a leak occured on the sodium/air heat exchanger used to remove decay heat an investigation revealed a design weakness in these air heat exchangers. The result of this weakness was that there was a fatigue mechanism which could lead to cracking and failure of the heat exchanger tubes. The safety problems therefore were:
>
> (i) Are further tube leaks going to occur?
>
> (ii) How much of the fatigue life had been exhausted?
>
> (iii) What process could be used to preclude further leaks?
>
> (iv) What now was the reliability of the heat exchangers in accident situations?
>
> A safety argument was developed along the following lines:
>
> An experimental programme tested a large population of heat exchanger tubes using a typical but accelerated fatigue cycle. As a result the fatigue life could be characterised in terms of the number of cycles and the magnitude of the cycles. This information indicated that failures were possible during the plant life. However there was no reliable record of the fatigue life so far experienced by the heat exchanger tubes.
>
> Re-analysis of the experimental data showed that crack initiation occured at the outside surface of the tubes while there was still a certain fraction of the fatigue life remaining. Therefore if

the crack could be detected, tube failure should be avoided. Since it is impossible to inspect the tubes during plant operation the following process was devised:

(i) During shutdown the tubes were all inspected and any cracked tubes removed.

(ii) All tubes were instrumented to record the thermal cycles and calculate the fatigue life exhausted since the last inspection.

(iii) The minimum value of fatigue life remaining after crack initiation was derived from the experimental results and a safety margin deducted.

(iv) During operation if any tube fatigue life exhaustion since the last inspection approached the minimum residual value the plant would be shutdown for tube inspection.

In order to establish the reliability of the heat exchangers for accident sequences the following issues were considered:

- The validity of the physical mechanism driving the tube fatigue
- The reliability of crack detection in tubes
- The variability of experimental results and differences between the experimental tubes and the actual tubes
- Mistakes in the interpretation of the tube monitoring programmes

Some of the problems would be common to each of 3 heat exchangers and some would generally be specific to individual tubes. It was therefore necessary to derive reliabilities for both individual heat exchangers and common mode failure of all 3 heat exchangers.

It was possible to provide some analysis for

- The inspection procedures and their reliability for both individual heat exchangers and common mode failures
- The variation in the experimental results
- The on-line monitoring of fatigue life exhaustion during operation.

However no meaningful analysis could be provided for two important factors:

- The validity of the physical model
- The effect of tube material properties variation from the experimental test pieces.

Thus the trigger level for plant shutdown was arbitrarily reduced to reflect the above two uncertainties and the remaining factors were assessed to generate a heat exchanger reliability. Since the heat exchanger reliability thus derived was of similar order to the probability previously assumed in the PSA it was judged that the safety case remained valid given the new operating procedures.

The foregoing argument is perhaps fairly typical of the type of safety case, involving both probabilistic and deterministic elements, which may be involved in life extension discussions of structural items.

Non-Structural Components

Apart from passive components which show a structural degradation with time there is evidence that active components also show a deterioration in reliability with time. In some cases such reliability versus time trends may not depend on the absolute age of the plant but occur at any stage in plant life as the result of specific factors such as poor maintenance, poor water chemistry control etc. In other cases reliability trends will depend on plant age, and components in this category which may be of safety significance include:

Station batteries (plate embrittlement)

Diesel generators

Component with high speed rotating parts including, pumps, fans, ventilators etc. (fatigue)

Instrumentation including thermocouples, differential pressure transducers etc (fatigue)

Pipe supports/dampers (fatigue).

The reliability of these components are difficult to model in a way which allows a theoretical analysis of deterioration and consequently reliance must be placed on data available either generically or from the specific components. Generic data can be used to give broad indications of useful component life and may suggest whether a component replacement policy is necessary. However there will be large variations in component useful life depending on the operational history of the components. Therefore component specific data should be collected wherever possible in order to provide specific evidence on the reliability trends for significant components. It may however be difficult to obtain good evidence for a specific plant unless there is a significant number of particular types of components, or components exhibit a number of different modes of degradation. Thus for example diesel generators are a small population but they may exhibit numerous degradation modes and the compilation of data from all modes could indicate a significant deteriorating trend while the data for any particular mode may not do so. By contrast degradation of electrical cable insulation due to environmental effects or fatigue of thermocouples is likely to be a clearer trend because of the large population of these components from which data can be collected.

Where data can demonstrate significant trends in component reliability this can be included directly in the PSA by amending the failure rates or unavailabilities. It is important to recognise that there may be systematic trends across a number of components and therefore failure rates should be amended on a systematic basis to reflect these correlations. If the quality and quantity of data on any particular component is appropriate it may be possible to derive empirical models to describe the component reliability in terms of component engineering parameters. For example, say, the reliability of gate valves may be related to:

o pressure and temperature of operation

o parameters of fluid contained - water, steam, void fraction, superheat etc.

o maintenance/test interval and strategy

o material of construction and packing

o method of actuation

A convenient form to test any engineering hypothese is the proportional hazards model which relates these various parameters as

$$\Lambda(t) = \Lambda(t)\, e^{-(B\,1 + \;B\,2\ldots\ldots + B\,n)}$$

Where $B_1 \ldots\ldots B_n$ are the explanatory variables (engineering characteristics) which may be continuous or more usually are divided into discrete categories. Thus for the gate valve, seat material is obviously a discrete category while steam superheat could be continuous but is probably better treated in a few discrete categories. In general data availability or quality is insufficient to prove particular relationships but the data may be adequate to give confidence in the engineering hypotheses. Thus an empirical model can be produced which is appropriate to give guidance on the relative importance of particular engineering features and may especially be useful in considering degradation issues.

The ultimate position which in principle could be achieved with sufficient data is:

(i) the PSA includes failure probabilities for all active and passive components

(ii) Empirical reliability models exist for all components relating failure probability to engineering characteristics of the components

(iii) changes in component engineering parameters due to degradation are known and can be used in the models form (ii) to calculate new failure probabilities

(iv) the PSA results can be recalculated to reflect component degradation.

Current position with respect to this ideal is

o many PSÂs do not include failure of passive components

o where passive components are included the data is rather arbitrary

o degradation in components, either expected or occuring unexpectedly, is not reflected in component failure probabilities

o few empirical component reliability models exist; in part because of a lack of good quality data.

Appendix B

SUPPORTING DOCUMENT ON USE OF PSA FOR RELICENSING OF EXTENDED LIFETIMES OF NUCLEAR POWER PLANTS

Comments on life extension of old plants

In the life of a plant we are confronted with 4 main problem areas:

1. Increasing state of knowledge
2. Changes in technical products
3. Changes in "Safety Philosophy"
4. Time dependent changes in material characteristics (degradation)

Examples are:

Problem Area 1

- Proper material for the pipe work of the secondary system and exchange of the relevant pipes
- Changes in the injection topology of the ECCS (hot leg and cold leg injection in the primary circuit)

Problem Area 2

- New designed electronic circuits in the SIMATIC serie in the FRG

Problem Area 3

- Bunkered aux-feedwater systems against external events, like airplane crashes

Problem Area 4

- Exchange of the heat exchangers in PWRs e.g. KWO, GKN in the FRG

Assuming that for the plant under consideration a plant specific PSA is available, this PSA could be used to support the decisions in these four problem areas. It should be mentioned that the potential of the PSA in supporting these different areas is different. Also the methods and tools of the PSA must be adapted in a different way to these four areas. The differences are explained in more details in the following section.

For additional information see Table 1, Figure 1 and Figure 2.

1. Increasing State of Knowledge

In this field we are confronted mainly with new advanced material compositions, surface preparation or different system topologies.

Related to the material question it should be mentioned that normally no specific reliability figures for a given component built with the new material are available. This means the benefit in e.g. risk reduction can not be evaluated quantitatively. Perhaps, operating records show the "negative record" of the old situation, if it was monitored in a proper way. After some years of recording the new situation we would be able to monitor the effect of such changes.

Differences in system topology normally can be monitored by an updated PSA. The PSA must be performed for different time intervals (e.g. 1 year) considering the plant specific changes in system topology. If only the topology was changed then the component failure rates should be the same.

2. Changes in Technical Products

The basic safety philosophy for NPPs requires products with successful operating experience in other technical fields. Especially in the electronic field, it is more and more common practices to maintain or guarantee product reliability at a given level. Therefore, the plant specific PSA can be updated with such component and/or system changes.

3. Changes in "Safety Philosophy"

Many discussions and decisions on safety issues are based on traditional deterministic engineering practices and subjective judgement. In this field it is a great potential of the PSA to support these decisions with its plant wide probabilistic system model. Thus, proposals for improvements - as an outcome of the living safety philosophy - could be validated by a PSA. In this context the PSA can show the impact of the proposed improvements either on the system level or on the core damage level. If the proposal is related to a structure and/or a material problem then today's PSAs have technical problems. The reason is the gap between the state of the art in structural reliability technique and the practiced system reliability technique.

It should be recommended to use and validate as much as possible also probabilistic structure models to monitor the effect of changes in structures or in material properties. Especially comparisons on the basis of sensitivity or importance studies are in the domain of probabilistic struture models. Benchmark studies in this field would help to increase the confidence in the model and to formulate research work.

4. Time Dependent Changes in Material Properties

The four main areas are:

- Fatigue
- Embrittlement
- Crack Growth
- Surface degradation (friction, erosion, corrosion)

All the above simply categorized effects influence the structure with respect to safety or reliability.

In the category of structures, we have to distinguish between structures without any preplanned replacement (e.g. RPV, primary pipeworks, heat exchangers) and strutures with preplanned or scheduled replacements (e.g. control rods/finger tubes, fuel elements, batteries, fuses, impellers).

For both types of structures the PSA could help to support decisions for life cycle extension.

In the first category of structures only one life cycle is considered. The end of a life cycle must be decided. In the second category the life cycle is one or some years. A proper end of this cycle must also be decided.

Looking back at the four main time dependent effects on structures, we can observe that advanced probabilistic structure models (see e.g. SMIRT or ICOSSAR conferences) take under consideration fatigue, embrittlement, crack growth and some of them also corrosion phenomina.

Time dependent effects on stucture are normally identified by engineering practices and therefore very well monitored (e.g. periodic ultrasonic inspection, eddy current inspection). A typical product is the so called 'crack map' of class 1 structures in the primary circuit of a PWR. Especially the wall thickness of heat exchanger tubes are extensively monitored. Based on this information deterministic models and expert opinion are normally used in the decision making process related to life cycle questions.

It should be mentioned that a probabilistic model which considers based on the deterministic states of knowledge - as an example - the success probability to monitor a given crack, the initial crack distribution, the crack growth rate and in a realistic way the other random or distributed parameters can show much better the reliability impact as the different uncorrelated deterministic models.

Analytical models have a great potential to show not only the actual impact from time dependent parameters but also to predict the future trends measured or expressed in decreasing reliability. Such models bring together all the information which are needed from fabrication, operation, periodic inspection, and structure engineering. The potential is the wide range information processing in an integrated fashion.

In the categorie of active components normally the identification of time dependencies in failure rates are sufficient indicators of degradation. If such time dependent failure rates are introduced in the PSA then the results reflect the time dependent safety performance of the plant.

In table B1 some components that are sensitive to degradation or time dependent changes in material characteristics are listed.

TABLE B1. Typical Components which degrade

Restored Components		Unrestored Components
active or parts inactive components	passive or parts inpassive components	
. seals . bearings . control rod fingers.tubes . pump and van impellers . diesels . switches . relays . pilot valves . turbine blades	. batteries . fuse . diesel head . elastic pipe . connectors . dampers . pump casings (size dependent) . heat exchangers . condenser tubes . electronic cards	. primary pressure boundary . steam generator heat tube bundle . pump casings (size dependent) . pressure vessels (size dependent) cables

In figure B1 the different uses of PSA for different decision making processes are shown.

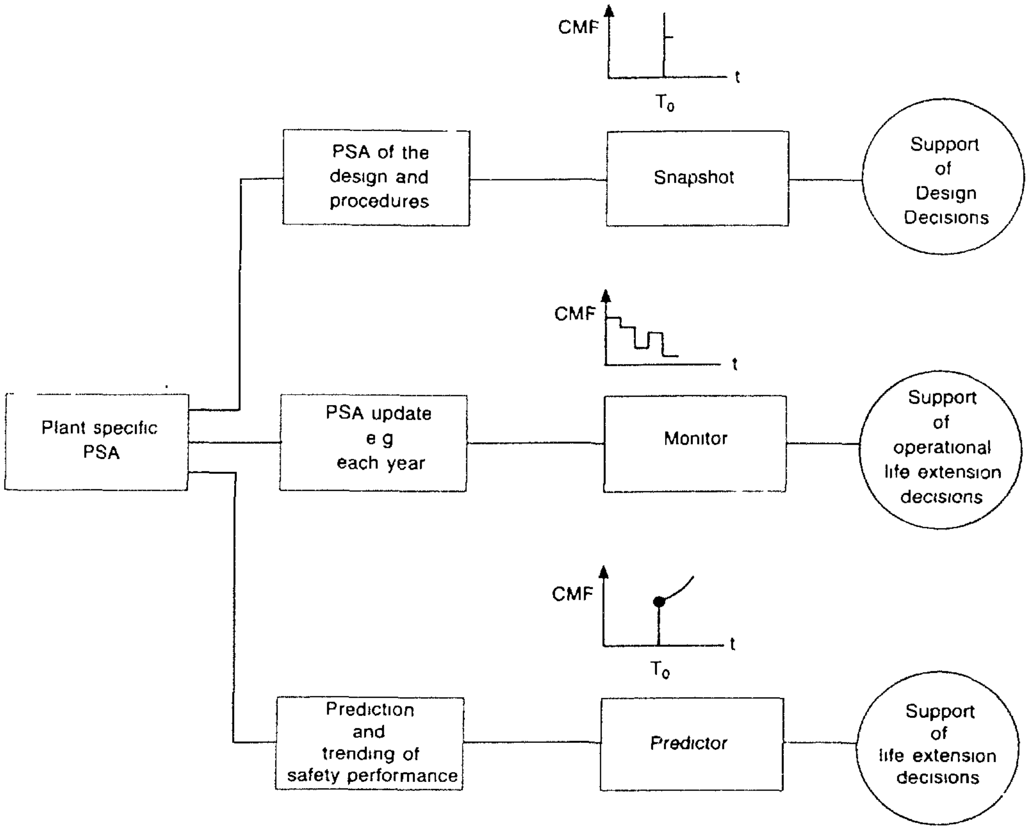
CMF
t
T0
PSA of the design and procedures
Snapshot
Support of Design Decisions
CMF
t
Plant specific PSA
PSA update e g each year
Monitor
Support of operational life extension decisions
CMF
t
T0
Prediction and trending of safety performance
Predictor
Support of life extension decisions

FIG.B1. Different uses of PSA for different decisions.

The main steps in the use of PSA for life extension are shown in Figure B2.

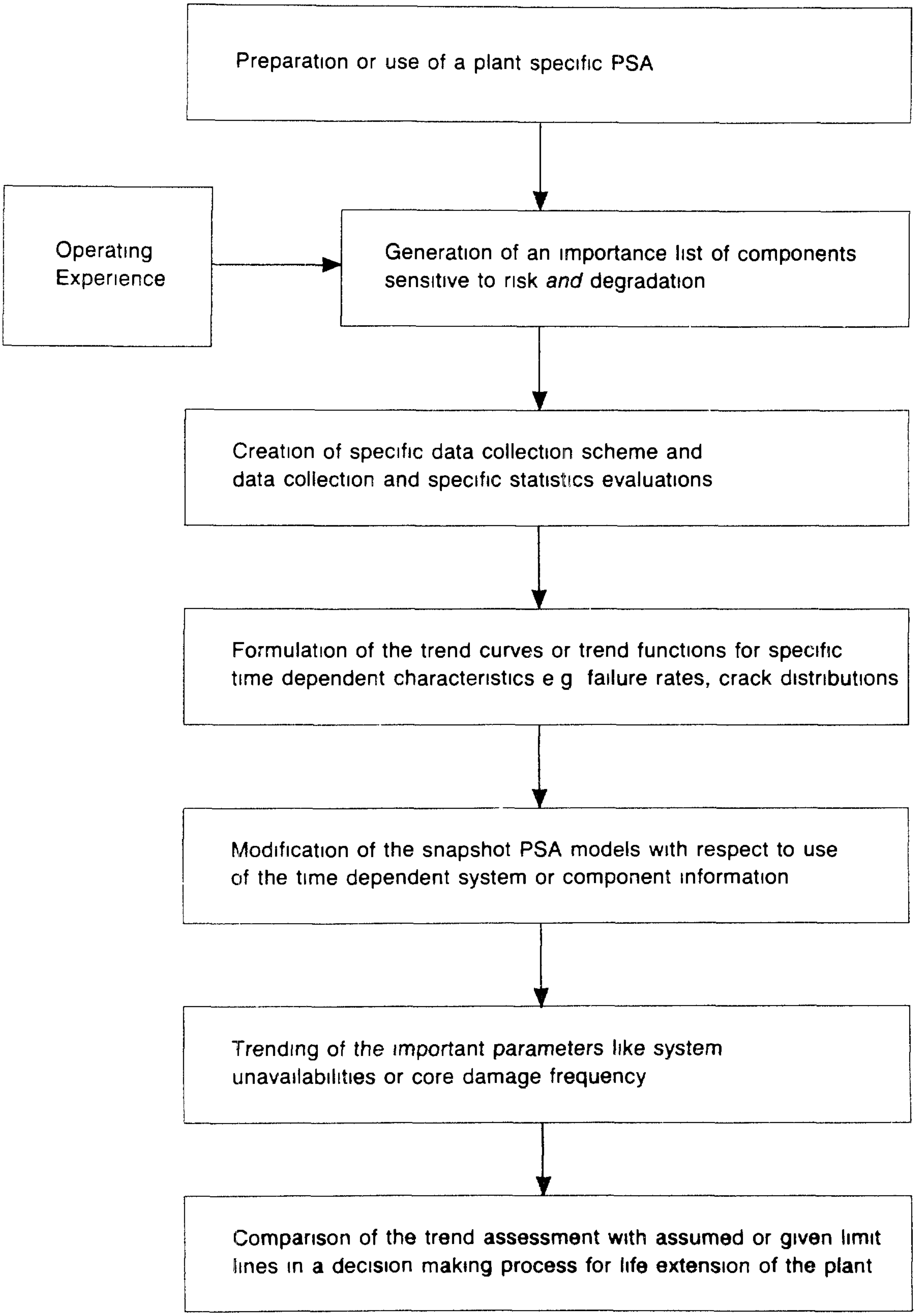
Preparation or use of a plant specific PSA
Operating Experience
Generation of an importance list of components sensitive to risk *and* degradation
Creation of specific data collection scheme and data collection and specific statistics evaluations
Formulation of the trend curves or trend functions for specific time dependent characteristics e g failure rates, crack distributions
Modification of the snapshot PSA models with respect to use of the time dependent system or component information
Trending of the important parameters like system unavailabilities or core damage frequency
Comparison of the trend assessment with assumed or given limit lines in a decision making process for life extension of the plant

FIG B2 Main steps in the use of PSA for the life extension

Conclusion

- In the decision making process for life extension of NPPs PSA can be used as an indicator or monitor of begining problems and as a predictor for trending the future safety performance.

- As a first indicator for the safety performance a special statistic evaluation of low level information (e.g. component or train maintenance and repair records) with respect to unavailabilities is sufficient.

- To monitor additionally interactions between systems and/or the plant personnel fullscope models (e.g. level 1 PSA) are necessary otherwise the different pieces of uncorrelated information can stimulate wrong decisions.

- From the monitoring of material characteristics (e.g. cracks or wall thickness) adequate probabilistic structure models should be evaluated. Such a well structured information processing system model makes it possible to identify correlated trends.

- Degradation is normally a systematic process on similar (redundant) components. Therefore the PSA model needs an adaption on these circumstances.

- To predict the future trend in safety performance PSA-type models integrated high level information (e.g. core damage frequency) should be used for an adequate handling of system interactions and parameters correlations.

- In the decisions making process for life time extension limits for the parameters of interest (e.g. core damage frequency) must be given. These limits can be based on official safety goals or safety assessment guidelines.

- Different from the risk monitor discussed above is a risk monitor system (e.g. PRISIM, ESSM) installed in a plant for fast optimization of operating and maintenance/repair regimes.

In such a risk monitor system it is necessary to input the actual plant/system status (e.g. components out of order) and then the system evaluates the actual risk level at this time and e.g. a prioritization list of the repair work with respect to minimum risk. The basis of such a system is a plant specific PSA modelled in an adequate way on a computer. The advantage is that the plant personnel is able to optimize in an interactive way with the help of the monitor system the operating and/or the maintenance/repair work under the actual system status conditions with respect to a minimum risk level (expressed e.g. as core damage frequency).

Appendix C

THE INTERNAL INITIATING EVENTS GENERALLY CONSIDERED FOR A BWR AND A PWR*

BWR EVENTS

T1 Transient caused by Loss of Offsite Power (LOSP)

T2 Transient without Power Conversion System (PCS) and offsite power initially available

T2A* Transient without PCS and Feedwater (FW) lost

T2B* Transients caused by an inadvertent open relief valve in the primary system

T3 Transient with PCS available and offsite power initially available

T3A* Transients of the T3 group other than T3B

T3B* Transient involving loss of feedwater, but with the steam side of PCS initially available

TAC/x Transient with loss of AC bus "x"

TDC/x Transient with loss of DC bus "x"

A Large LOCA

S1 Intermediate LOCA

S2 Small LOCA

S3 Small Pump Seal LOCA

V Interfacing LOCA

LOSP Loss of site power

* Taken from Reference 2.

PCS	Power conversion system
LOCA	Loss of coolant initiator

PWR EVENTS

T1	Transient caused by LOSP
T2	Transient without PCS available (and offsite power initially available)
T3	Transient with PCS available (and offsite power initially available)
T6	Transient caused by loss of cooling water
TAC/x	Transient with loss of AC bus "x"
TDC/x	Transient with loss of DC bus "x"
A	Large LOCA
S1	Intermediate LOCA
S2	Small LOCA
S3	Small Seal LOCA
V	Interfacing LOCA

Appendix D

SAFETY FUNCTIONS WHICH ARE GENERALLY INCLUDED IN BWR AND PWR EVENT TREES*

BWR - LOSS OF COOLANT INITIATORS

- Reactor subcriticality
- Emergency core cooling
- Early containment overpressure protection
- Late containment overpressure protection
- Post-accident radioactivity removal

BWRs - TRANSIENTS

- Reactor subcriticality
- RCS overpressure protection
- Emergency core cooling
- Residual heat removal

PWRs - LOSS OF COOLANT INITIATORS AND TRANSIENTS

- Reactor subcriticality
- Core heat removal, early
- RCS integrity
- Containment pressure suppression
- Core heat removal, late
- Containment atmosphere heat removal

* Taken from Reference 2.

Appendix E

SYSTEMS WHICH ARE GENERALLY ANALYSED FOR A BWR AND A PWR*

BWR SYSTEMS

Front Line:

High Pressure Core Spray
High Pressure Coolant Injection
Reactor Core Isolation Cooling
Automatic Depressurization System
Safety Relief Valve
Low Pressure Core Spray
Low Pressure Coolant Injection
Residual Heat Removal/ Suppression Pool Cooling
Residual Heat Removal/ Containment Spray
Residual Heat Removal/ Shutdown Cooling
Control Rod Drive
Suppression Pool Makeup
Reactor Protection System
Alternate Rod Insertion
Standby Liquid Control
Power Conversion System
Alternate Injection System

Support:

Electric Power
Actuation
Instrument Air
Heating Ventilation and Air Conditioning
Service Water

PWR SYSTEMS

Front Line:

High Pressure Injection
High Pressure Recirculation
Power Operated Relief Valve
Low Pressure Injection
Low Pressure Recirculation
Accumulators
Power Conversion System
Auxiliary Feedwater
Containment Spray Injection
Containment Spray Recirculation System
Reactor Protection System
Alternate Injection System

Support:

Electric Power
Actuation
Instrument Air
Heating Ventilation and Air Conditioning
Service Water

* Taken from Reference 2.

Appendix F

CASE STUDY OF CONSTRUCTING INDICATORS TO MONITOR THE UNAVAILABILITY PERFORMANCE

Introduction

This appendix presents a case study of how indicators can be constructed to monitor the unavailability of safety systems. The analyses are described in detail in Reference 14. The construction of indicators to monitor plant safety performance can be a critical element in a programme to provide guidance in the relicensing of extended lifetimes of the plant. Indicators can give the time variations in the safety performance of the plant in terms of the safety system unavailability performance, the core melt frequency performance, and other measures of safety performance.

The following benefits are obtained from constructing and applying performance indicators:

1. The safety performance of the plant is objectively measured in terms of safety system unavailability performances, core melt frequency performance, and other risk performance measures,

2. The time variations in the safety performance of the plant can significantly deviate from the calculated static PSA values, and safety indicators are a principal way of measuring the dynamic changes in the plant safety performance,

3. Aging trends and other deteriorating trends can be signaled by the indicators, and the causes for the trends can be corrected before actual accidents occur,

4. By using PSA models, the safety performance indicators can integrate different data behaviors to show their resulting safety impacts, and can conversely also show the basic causes of core melt frequency and safety performance behaviors,

5. The indicators can measure the effects of plant design changes and plant procedure changes in terms of their impacts on safety performance,

Appendix F

CASE STUDY OF CONSTRUCTING INDICATORS TO MONITOR THE UNAVAILABILITY PERFORMANCE

Introduction

This appendix presents a case study of how indicators can be constructed to monitor the unavailability of safety systems. The analyses are described in detail in Reference 14. The construction of indicators to monitor plant safety performance can be a critical element in a programme to provide guidance in the relicensing of extended lifetimes of the plant. Indicators can give the time variations in the safety performance of the plant in terms of the safety system unavailability performance, the core melt frequency performance, and other measures of safety performance.

The following benefits are obtained from constructing and applying performance indicators:

1. The safety performance of the plant is objectively measured in terms of safety system unavailability performances, core melt frequency performance, and other risk performance measures,

2. The time variations in the safety performance of the plant can significantly deviate from the calculated static PSA values, and safety indicators are a principal way of measuring the dynamic changes in the plant safety performance,

3. Aging trends and other deteriorating trends can be signaled by the indicators, and the causes for the trends can be corrected before actual accidents occur,

4. By using PSA models, the safety performance indicators can integrate different data behaviors to show their resulting safety impacts, and can conversely also show the basic causes of core melt frequency and safety performance behaviors,

5. The indicators can measure the effects of plant design changes and plant procedure changes in terms of their impacts on safety performance,

and

6. The indicators can provide an objective record of the safety performance of the plant, which can be used in assessing whether to grant the plant a life extension.

We shall focus here on unavailability indicators as a class of performance indicators. The first step in constructing unavailability indicators is to use component failure and downtime data to construct component and train unavailability indicators which are combined to form system unavailability indicators. The following sections describe how unavailability indicators can be constructed and can be implemented. The specific indicators which are discussed in the next section are calculated on a quarterly bases (i.e. are calculated every three months), although any other time period can be used if the data are available.

Once the system unavailability indicators are calculated, they can be input into a PSA plant model to obtain the core melt frequency indicator and other plant safety indicators. We will not describe the determination of the core melt frequency indicator from the system unavailability indicators since they involve standard PSA manipulations utilizing fault trees and event trees. Even without the full PSA plant model, the system unavailability indicators themselves can provide useful and important information on the plant safety performance.

SPECIFIC CASE STUDY APPROACHES

There are various ways that system unavailability indicators can be constructed. For the specific case study which will be reported upon here, the following specific approach was used:

1. The system was defined in terms of the trains constituting the system.

2. For each train of the system, the downtime which occurred in each quarter (in each three month preiod) were recorded and the plant critical hours were recorded (i.e. the hours the plant was online)

3. The recorded downtime information for each train consisted of the duration of the downtime, whether the downtime was due to failure or to maintenance, and whether the train was functional during the downtime.

4. The total downtime per quarter for a train was determined by adding the detected downtime plus the undetected downtime. The detected downtime consisted of the repair downtime duration (associated with failures) plus the maintenance downtime duration in which the train was not functional. The undetected downtime consisted of the time interval from the time of failure occurrence to the time at which the failure was detected. When the time of failure occurrence was not recorded then the undetected downtime was estimated as one half the surveillance test interval.

The actual construction of the system unavailability indicators consisted of the following steps:

1. The average train downtime per quarter was determined by taking the total downtime per train divided by the number of trains.

2. If regulations (technical specifications) did not allow both trains to be down for maintenance then the average maintenance downtime per train was also calculated. The average maintenance downtime per train was calculated in the same way as the total downtime per train except that only repair time durations and maintenance time durations were used (the undetected downtime was not considered)..

3. The smoothed train unavailability per quarter was obtained by using a 3 downtime smoothing. The 3 downtime smoothing, or 3-D smoothing for short, consisted of averaging the past quarters such that there are three quarters of non-zero downtimes. Consider the following example.

$$\begin{array}{ccccc} D_1 & 0 & D_3 & 0 & D_5 \\ L_1 & L_2 & L_3 & L_4 & L_5 \end{array}$$

Where D_i denotes the downtime per quarter i and L_i denote the critical hours per quarter. Assume that D_1 and L_1 represent the data for the present quarter. The 3-D smoothed unavailability indicator q.

$$\bar{q} = \frac{D_1 + D_3 + D_5}{L_1 + L_2 + L_3 + L_4 + L_5}$$

Thus the 3-D smoothed indicator is a type of running average where past history is included such as to cover three quarters of downtimes.

4. The 3-D indicator is updated at quarters with non-zero downtime. If at a given quarter in which there is a non-zero downtime, there are fewer than two additional quarters of non-zero downtimes in past history (to give the 3-D indicator) then all of the past history is used. This procedure serves to initialize the 3-D indicator.

5. The 3-D smoothing is restarted after each shutdown period (thus treating the data after a shutdown as new history) to evaluate unavailability behavior before and after end shutdown.

6. Where there are no technical specifications limiting multiple trains being down, the smoothed system unavailability indicator is calculated by raising the 3-D train indicator to the power which represents the number of trains in the system. For example if q_2 represents the 3-D smoothed indicator for a two train system and q represents the 3-D average train unavailability then

$$\bar{q}_2 = (\bar{q})^2$$

7. For more complex systems, the 3-D system unavailability is calculated from the Boolean formulas for the system. Furthermore if the separate trains were diverse and consisted of different components then the train downtimes would not be aggregated. Statistical tests can be performed to test the hypothesis of similar downtime behavior.

8 When technical specifications do not allow multiple trains to be down for repair or maintenance then the 3-D system unavailability is adjusted by subtractingthe appropriate maintenance condtributions using the 3-D maintenance downtime unavailability per train. The 3-D maintenance unavailability per train is calculated in the same way as the 3-D total unavailability per train except that maintenance and repair downtime per quarter is only used.

9. A warning limit or tolerance limit can also be defined indicating abnormal behaviors. For the auxiliary feedwater system which is presented here, the 95% tolerance limit is assigned to be 0.05 per train.

10. Finally, statistical trends in the indicators can be determined by using standard statistical tests. Kendall's tau test was used here. Kendall's tau test basically looks at all the permutations of data which

can occur and determines the fraction which produces trends as great or greater than these observed. A trend is taken to be significant if its significant level (fraction) is less than 0.05 (giving confidences greater than 95%)

RESULTS FOR THE SPECIFIC CASE STUDY

On the following pages, using plant recorded data, the 3-D system unavailability indicator is calculated for the aux-feed system. The results are presented in the following format:

1. A table (spreadsheet) of the raw data and calculated unavailabilities is first given,
2. A plot of the 3-D average train unavailability indicator per quarter showing 95% significant time trends and a 95% warning limit is then given,
3. A plot of the 3-D system unavailability per quarter indicating 95% significant time trends and showing a 95% warning limit is finally given.

The tables on the next page define the labels that are used in the spreadsheet which gives the calculated results. The tables and plots on the following pages (with a "Plant 1" label) present the actual plots. In the first spreadsheet table for the aux-feed system, the downtime hours per train (DWNA, DWNB, DWNC) include the detected plus undetected downtime hours. Undetected downtime hours occur only when a failure (loss of function) of the train is discovered; the undetected downtime hours are the hours the failure remains undetected until the test and are calculated as one-half the interval between consecutive tests (or demands) of the train.

The aggregated train unavailability (summed over the 3 trains) and the average train unavailability for the aux-feed system are shown on the same plot with the label "3-TRAIN AGGREGATE". The same plot can be used for either the aggregate or average train unavailability, reading the left or right scale, respectively. The aux-feed system unavailability plot is calculated as the cube of the average train unavailability. The dotted lines in the figures connect behaviors before and after plant shutdown periods.

The aux-feed results provide a great deal of information and show significant time trends and show significant departures from the 95% warning limit. The aux-feed system unavailability exhibits a significant increasing time trend before an actual shutdown which occurred from 86-2 to 87-2. The plant shutdown was in fact partly due to problems with the aux-feed system and other mechanical components. Consequently, the indicator forewarned of this problem. After the 86-2 to 87-2 shutdown, the unavailability decreased (as compared to the value immediately before the shutdown) and continued on a significant decreasing trend. The indicator plot thus shows that the maintenance and personnel changes that were instituted during the shutdown had significant beneficial effects on the unavailability.

DEFINITIONS OF LABELS USED IN THE TRAIN AND SYSTEM UNAVAILABILITY TABLES

Label Name	Label Description
3 AVERAGE	3-Cycle Running Average for the 3-train or 2-Train aggregate
3 AVG./TRAIN	3-Cycle Running Average per train for the 3-train or 2-train aggregate
(PER TRAIN)^3	The cube of the 3 AVG./TRAIN
A&B 3 AVG.	3-Cycle Running Average for the 2-train aggregate
A&B 3 AVG./TRAIN	3-Cycle Running Average per train for the 2-train aggregate
A&B DOWN TOTAL	Number of hours trains A&B were down
A&B (PER TRAIN)^2	The square of A&B 3 AVG./TRAIN
A&B(PER TRAIN)^2 * T	The product of A&B (PER TRAIN)^2 with T 3 AVG.
CRITICAL HOURS	Hours of plant operation for the current quarter
CUMM. CRIT. HRS.	Total number of hours of plant operation to date
DOWN TOTAL	Number of hours all trains were down
DWNA, DWNB, DWNC, DWNT, DWN1, DWN2	Number of hours trains A, B, C, T, 1, & 2 were down
T 3 AVG.	3-Cycle Running Average for train T

PLANT 1:   AUX-FEED

YEAR	QUARTER	CRITICAL HOURS	CUMM. CRIT. HRS.	DWNA	DWNB	DWNC	DOWN TOTAL	3 AVERAGE	3 AVG. / TRAIN
83	83-1	2141	2141	0.00	0.00	0.00	0.00	NA	NA
	83-2	2164	4305	0.00	0.00	912.00	912.00	0.21	0.07
	83-3	978	5283	0.00	0.00	978.00	978.00	0.36	0.12
	83-4	0	5283	0.00	0.00	0.00	0.00	NA	NA
84	84-1	0	5283	0.00	0.00	0.00	0.00	NA	NA
	84-2	0	5283	0.00	0.00	0.00	0.00	NA	NA
	84-3	568	5851	0.00	0.00	0.00	0.00	NA	NA
	84-4	983	6834	0.00	0.00	0.00	0.00	NA	NA
85	85-1	2160	8994	0.00	571.23	0.00	571.23	0.15	0.05
	85-2	2183	11177	58.50	0.00	0.00	58.50	0.11	0.04
8	85-3	1784	12961	926.50	0.00	0.00	926.50	0.25	0.08
	85-4	1363	14324	0.00	240.00	0.00	240.00	0.23	0.08
86	86-1	327	14651	0.00	0.00	0.00	0.00	NA	NA
	86-2	1163	15814	0.00	256.00	0.00	256.00	0.31	0.10
	86-3	0	15814	0.00	0.00	0.00	0.00	NA	NA
	86-4	0	15814	0.00	0.00	0.00	0.00	NA	NA
87	87-1	0	15814	0.00	0.00	0.00	0.00	NA	NA
	87-2	1937	17751	0.00	58.00	364.00	422.00	0.22	0.07
	87-3	1762	19513	11.62	38.00	293.00	342.62	0.21	0.07
	87-4	528	20041	0.00	0.00	0.00	0.00	NA	NA
88	88-1	1574	21615	0.00	48.00	0.00	48.00	0.14	0.05
	88-2	2043	23658	0.37	1.40	59.00	60.77	0.08	0.03

PLANT 1:   AUX-FEED : TABLE CONTINUED

YEAR	QUARTER	(PER TRAIN)^3
83	83-1	NA
	83-2	3.43E-04
	83-3	1.73E-03
	83-4	NA
84	84-1	NA
	84-2	NA
	84-3	NA
	84-4	NA
85	85-1	1.25E-04
	85-2	4.93E-05
	85-3	5.79E-04
	85-4	4.51E-04
86	86-1	NA
	86-2	1.10E-03
	86-3	NA
	86-4	NA
87	87-1	NA
	87-2	3.94E-04
	87-3	3.43E-04
	87-4	NA
88	88-1	1.02E-04
	88-2	1.90E-05

REFERENCES

1. INTERNATIONAL ATOMIC ENERGY AGENCY, Guidelines for Conducting Probabilistic Safety Assessment for Nuclear Power Plants, IAEA, Vienna 1989. (to be published as a Safety Series Report)

2. DROUIN, M.T., HARPER, F.T., CAMP, A.L., Analysis of Core Damage Frequency from Interval Events: Methodology Guidelines, NUREG/CR-4550, Volume 1, September 1987.

3. AMERICAN NUCLEAR SOCIETY AND THE INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, PRA Procedures Guide, NUREG/GR-2300, January 1983.

4. VESELY, W.E., The Development of Maintenance Programmatic Indicators and Their Trending, Brookhaven National Laboratory Technical Report A-3295 4-27-88, July 1988.

5. MINARICK, J.W., et al, Precursors to Potential Severe Core Damage Accidents: 1985 A Status Report, NUREG/CR-4674, November 1986.

6. CAMPBELL, D.J., et al, Risk Assessment Application to NRC Inspection; Progress Report, NUREG/CR-4560, June 1986.

7. VESELY, W.E., VORA, J.P., "Integration of Engineering Information and Risk Information for Aging Assessments", Proceedings of the International Nuclear Power Plant Aging Symposium, August 1988.

8. SMITH, A.L., Reliability of Engineering Material, Butterworths Publishing, Boston, 1984.

9. FRANTIC ABC, GINZBURG, T., POWERS, J., FRANTIC II - A Computer code for Time Dependent Unavailability Analysis, NUREG/CR-1924, October 1981.

10. GINZBURG, T., BOCCIO, J.L., HALL, R.E., FRANTIC II - Applications to Standy Safety Systems, NUREG/CR-3627, December 1983.

11. VESELY, W.E., Risk Evaluations of Aging Phenomena: The Linear Aging Model and Its extensions, NUREG/CR-4769, April 1987.

12. USNRC, Risk Criteria for Nuclear Reactors, NUREG-0880, March 1981.

13. SOLOMON,K.A., et al, An Evaluation of Alternatives Safety Criteria for Nuclear Power Plants Risk Analysis Vol. 5, No.4, September 1985, pp.209-216.

14. VESELY, W.E., BURLILE, G.A., Train and System Unavailability Indicators Applied to the Past Histories of Five Plants, Brookhaven National Laboratory Technical Report A-3295 1-11-89, January 1989.

CONTRIBUTORS TO DRAFTING AND REVIEW

Consultants' Meeting on "The Use of Probabilistic Safety Assessment in the Relicensing of Nuclear Power Plants for Extended Lifetimes", 13 June - 1 July, 1988, Vienna.

UNION OF SOVIET
SOCIALIST REPUBLICS

E.K. Shubeiko

Science and Engineering Centre
Taganskage Street 34
109147 Moscow

UNITED STATES
OF AMERICA

W.E. Vesely

Science Applications Int'l Inc.
2929 Kenny Road
Suite 245, Columbus
Ohio 43221

IAEA

M. Cullingford — Scientific Secretary
S.M. Shah

Consultants' Meeting on "The Use of PSA for Relicensing of extended lifetimes of nuclear power plants", 5 - 9 December 1988, Vienna.

GERMANY, FEDERAL REPUBLIC OF

P. Kafka

Gesellschaft f. Reaktorsicherheit
(GRS) mbh
Forschungsglände, 8046
Garching

UNITED KINGDOM

G.M. Ballard

UKAEA, SRD
Wigshaw Lane, Culcheth
Warrington, Chershire WA3 ENE

UNITED STATES
OF AMERICA

W.E. Vesely

Science Applications Int'l Inc.
2929 Kenny Road
Suite 245, Columbus
Ohio 43221

IAEA

M. Cullingford

Scientific Secretary

S.M. Shah

HOW TO ORDER IAEA PUBLICATIONS

An exclusive sales agent for IAEA publications, to whom all orders and inquiries should be addressed, has been appointed in the following country:

UNITED STATES OF AMERICA	UNIPUB, 4611-F Assembly Drive, Lanham, MD 20706-4391

In the following countries IAEA publications may be purchased from the sales agents or booksellers listed or through major local booksellers. Payment can be made in local currency or with UNESCO coupons.

ARGENTINA	Comisión Nacional de Energía Atómica, Avenida del Libertador 8250, RA-1429 Buenos Aires
AUSTRALIA	Hunter Publications, 58 A Gipps Street, Collingwood, Victoria 3066
BELGIUM	Service Courrier UNESCO, 202, Avenue du Roi, B-1060 Brussels
CHILE	Comisión Chilena de Energia Nuclear, Venta de Publicaciones, Amunategui 95, Casilla 188-D, Santiago
CHINA	IAEA Publications in Chinese China Nuclear Energy Industry Corporation, Translation Section, P.O. Box 2103, Beijing IAEA Publications other than in Chinese China National Publications Import & Export Corporation, Deutsche Abteilung, P.O. Box 88, Beijing
CZECHOSLOVAKIA	S.N.T.L., Mikulandska 4, CS-116 86 Prague 1 Alfa, Publishers, Hurbanovo námestie 3, CS-815 89 Bratislava
FRANCE	Office International de Documentation et Librairie, 48, rue Gay-Lussac, F-75240 Paris Cedex 05
HUNGARY	Kultura, Hungarian Foreign Trading Company, P.O. Box 149, H-1389 Budapest 62
INDIA	Oxford Book and Stationery Co., 17, Park Street, Calcutta-700 016 Oxford Book and Stationery Co., Scindia House, New Delhi-110 001
ISRAEL	Heiliger & Co. Ltd 23 Keren Hayesod Street, Jerusalem 94188
ITALY	Libreria Scientifica, Dott. Lucio de Biasio "aeiou", Via Meravigli 16, I-20123 Milan
JAPAN	Maruzen Company, Ltd, P.O. Box 5050, 100-31 Tokyo International
PAKISTAN	Mirza Book Agency, 65, Shahrah Quaid-e-Azam, P.O Box 729, Lahore 3
POLAND	Ars Polona-Ruch, Centrala Handlu Zagranicznego, Krakowskie Przedmiescie 7, PL-00-068 Warsaw
ROMANIA	Ilexim, P O. Box 136-137, Bucharest
SOUTH AFRICA	Van Schaik Bookstore (Pty) Ltd, P.O Box 724, Pretoria 0001
SPAIN	Díaz de Santos, Lagasca 95, E-28006 Madrid Díaz de Santos, Balmes 417, E-08022 Barcelona
SWEDEN	AB Fritzes Kungl. Hovbokhandel, Fredsgatan 2, P.O. Box 16356, S-103 27 Stockholm
UNITED KINGDOM	Her Majesty's Stationery Office, Publications Centre, Agency Section, 51 Nine Elms Lane, London SW8 5DR
USSR	Mezhdunarodnaya Kniga, Smolenskaya-Sennaya 32-34, Moscow G-200
YUGOSLAVIA	Jugoslovenska Knjiga, Terazije 27, P O. Box 36, YU-11001 Belgrade

Orders from countries where sales agents have not yet been appointed and requests for information should be addressed directly to:

Division of Publications
International Atomic Energy Agency
Wagramerstrasse 5, P.O. Box 100, A-1400 Vienna, Austria