IAEA-TECDOC-669

Case study on the use of PSA methods:

Assessment of technical specifications for the reactor protection system instrumentation

INTERNATIONAL ATOMIC ENERGY AGENCY

IAEA

October 1992

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

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

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

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

CASE STUDY ON THE USE OF PSA METHODS:
ASSESSMENT OF TECHNICAL SPECIFICATIONS FOR
THE REACTOR PROTECTION SYSTEM INSTRUMENTATION
IAEA, VIENNA, 1992
IAEA-TECDOC-669
ISSN 1011–4289

Printed by the IAEA in Austria
October 1992

FOREWORD

Probabilistic Safety Assessment (PSA) is increasingly being used to complement the deterministic approach to nuclear safety. From the traditional discipline of reliability engineering, PSA developed as a structured method to identify potential accident sequences from a broad range of initiating events and to quantify their frequency of occurrence.

PSAs use inductive (event tree) and deductive (fault tree) logic and plant specific as well as generic component failure rates and frequencies of initiating events. Plant specific test and maintenance schedules, human errors and common cause failures are also considered in the probabilistic models.

PSA is nowadays a fundamental tool that provides guidance to safety related decision-making. By its very nature PSA recognizes the uncertainties associated with the logic models used to represent reality and quantifies the variability in the data of the parameters in the models.

The IAEA is promoting the conduct of PSA studies through standardization of the methodology, co-ordination of research, assistance through its Technical Co-operation Programme, and development of PSA software (PSAPACK). In addition it offers International Peer Review Services (IPERS) to review PSAs at various stages of completeness.

Emphasis at present is concentrated on "level-1" PSAs which quantify accident sequences up to estimates of core-damage probability. Level-2 (releases of radioactivity) and level-3 (off-site impacts) will be addressed at a later stage.

The work described above on the conduct of PSA is complemented by a programme on how to use the results of PSA in nuclear safety. For this purpose a series of CASE STUDIES has been prepared. The objective is to provide those who have performed PSAs with practical examples on how PSA results have been used. Those authorities and utilities still reluctant to request or perform PSAs will find convincing evidence on the benefits of such studies for nuclear safety.

With these objectives in mind, the IAEA requested a number of internationally recognized experts to document, in a uniform and suitable format, actual experience with the use of PSA for safety decisions. The documents were peer reviewed by an Oversight Committee for quality and completeness.

It is hoped that this series of CASE STUDIES will significantly contribute to the use of PSA to improve nuclear safety.

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.

PREFACE

A series of CASE STUDIES has been prepared to summarize practical examples on how the results of PSA studies have been used in nuclear safety. They draw from the experience of major studies and, to the extent possible, use a similar format to guide the reader. The studies illustrate the range of applications in a specific topical area. It is the objective to take examples which are using level-1 PSAs rather than individual accident sequences or systems reliability. Emphasis is given to a logical step-by-step description of the analysis and documentation of calculational procedures and data. The interpretation of the results explicitly addresses the problem of uncertainties and limitations of the studies, and includes the results of Peer Reviews.

This case study presents a methodology for the probabilistic evaluation of alternative plant technical specifications regarding system surveillance frequencies and out-of-service times. The methodology is applied to the reactor protection system of a 4 loop PWR-RESAR-3S type nuclear power plant. The effect of the statistical characteristics of the system on the relative comparison of various sets of technical specifications is examined through sensitivity studies and an uncertainty analysis.

The purpose of this CASE STUDY is thus to provide a good example on the use of probabilistic evaluation of alternative plant Technical Specifications regarding system surveillance frequencies and out-of-service times.

The following additional Case Study documents are available:

IAEA-TECDOC-522	A Probabilistic Safety Assessment Peer Review: Case Study on the Use of Probabilistic Safety Assessment for Safety Decisions (1989)
IAEA-TECDOC-543	Procedures for Conducting Independent Peer Reviews of Probabilistic Safety Assessment (1990)
IAEA-TECDOC-547	The Use of Probabilistic Safety Assessment in the Relicensing of Nuclear Power Plants for Extended Lifetimes (1990)
IAEA-TECDOC-590	Case Study on the Use of PSA Methods: Determining Safety Importance of Systems and Components at Nuclear Power Plants (1991)
IAEA-TECDOC-591	Case Study on the Use of PSA Methods: Backfitting Decisions (1991)
IAEA-TECDOC-592	Case Study on the Use of PSA Methods: Human Reliability Analysis (1991)
IAEA-TECDOC-593	Case Study on the Use of PSA Methods: Station Blackout Risk at Millstone Unit 3 (1991)

CONTENTS

1. PROBLEM DEFINITION

1.1. TECHNICAL SPECIFICATIONS OF NUCLEAR POWER PLANTS

Technical specifications of nuclear power plants are design and procedural limits that entail explicit restrictions on the operation of the plants and on the maintenance of safety related systems in normal conditions. Technical specifications generally define how a plant may be operated in order to stay within the bounds of the analysis of the FSAR.

Technical specifications (TS) of interest to this case study are those that determine the set of conditions under which a particular system should operate. In particular, technical specifications regarding testing policies for systems whose availabilities are not constantly revealed (e.g. because they are in a standby mode) determine: what components should be maintained; with what frequency should these components be tested; and how long they are allowed to be out of service before the plant is required to take actions outside its normal operation envelope.

Surveillance testing (ST) (scheme and frequency) aims at increasing the assurance that the system in question will be available to perform its function when called upon.

Often the performance of a test requires that the tested component, and sometimes a greater part of the system, be put out of service. This means that the part of the system under test is unavailable to perform its intended function if it is called to do so during the test. Similarly, if the component is found failed and it is put under repair it is unavailable until the repair is completed and the component is put back to service. When a safety related system, or a part of it, is unavailable the safety margin under which the nuclear power plant operates is reduced.

Allowable out-of-service time (AOT) for a component is the time for which the plant can operate with the particular component out of service and, hence, the time for which the plant can operate under the associated reduced safety margin.

High frequencies of surveillance testing tend, on the one hand, to increase the degree of assurance that the corresponding system or component will be available if called upon, but on the other hand, the associated increase of the out-of-service time (owing to tests) has the opposite effect.

Short allowable out-of-service times (AOTs) assure that the plant will not operate for too long under a reduced safety margin. Yet short AOTs mean frequent plant shutdowns and decreased plant availability.

Technical specifications decision making regarding system surveillance frequencies and allowable out-of-service times requires, therefore, careful consideration and balancing of the desirable and undesirable impacts on the operation of the plant. Decisions cannot be made, ad hoc, but require a logical and systematic framework.

Probabilistic safety assessment (PSA) provides such a logical and systematic framework for making decisions about the technical specifications of systems in nuclear power plants since PSA generates quantitative estimates of the relative likelihood of occurrence of certain undesirable consequences as well as the mechanisms (accidents) that can lead to these consequences. Furthermore, TS are explicitly included in the associated models and hence their impact on the results of the PSA can be established. Consequently PSA provides a natural framework for decision making in any of the following topics:

(i) Determination of acceptable values of TS: this includes both the determination of specific values for the TS that satisfy certain risk-based criteria or the evaluation of a specific change to an existing set of TS.

(ii) Granting of one-time AOT extension or ST exemption: in several instances plants request from their regulatory bodies one-time extensions of the AOT and/or ST exemptions requiring corresponding decisions from the regulatory body.

(iii) Establishing the types of tests to be performed: this includes establishing the most significant failure modes that should be tested as well as the types of tests to be performed to simulate the demand experienced in the important accident scenarios.

(iv) Establishing which TS are important: this includes understanding which TS are risk significant and which are not; the latter might not require as much regulatory-body control. (In the case of USNRC this means transfer to supplemental specifications).

This case study provides a methodological framework for making decisions of type (i) above about the TS of the reactor protection system in a pressurized water reactor (PWR) and in addition presents the results of a realistic application of this methodology.

1.2. TECHNICAL SPECIFICATIONS OF THE REACTOR PROTECTION SYSTEM OF A PWR

The reactor protection system (RPS) of a nuclear reactor keeps the reactor operating within a safe region. If one or more physical parameters enter an unacceptable range of values, a trip signal will be produced that will cause the insertion of the control rods into the core and ensure an orderly shutdown of the nuclear chain reaction. In a pressurized water reactor the trip signal will de-energize the electromagnetic holding power of the control rod drive mechanisms and the control rods will drop into the core because of gravity.

The part of the RPS that senses the need for and sends a trip signal for the rods to insert, is called the electrical part of the RPS. A detailed description of the electrical part of the RPS of Westinghouse designed PWR is given in Section 4.1 of this case study. For the purposes of this discussion it suffices to observe that the electrical part of the RPS consists of: (a) **analog channels** that sense and monitor the

various physical parameters and send a trip signal if any of the parameters exceeds its predetermined range; and (b) **logic trains** that receive the outputs of the analog channels and decide on the basis of a voting scheme if enough channels are sending trip signals to require sending a trip signal to the mechanical subsystem of the RPS to insert the control rods.

To ensure their proper function both analog channels and logic trains are tested at predetermined time intervals. The frequency of testing (surveillance frequency) is one of the TS for the RPS. During testing both the analog channels and the logic trains are bypassed and hence, they are unavailable for their intended function in the RPS. Consequently during this time the safety margin built into the RPS is reduced. The time for which an analog channel or a logic train can remain bypassed - the allowable bypass time - is the second TS for the RPS. If the allowable bypass time is exceeded then the analog channel or the logic train is tripped; that is, it is put in a mode as if that particular channel or logic train was giving a signal for the reactor shutdown. Thus, high surveillance frequency and short allowable bypass times tend to increase the availability of the RPS. On the other hand, however, such TS tend to invoke too many inadvertent reactor trips, and as a result, cause unnecessary transients and challenges to other safety systems and increase unavailability (down time) of the plant. Furthermore, according to the Westinghouse Owner's Group [3], operating staff must devote significant amount of time and effort which would otherwise be redirected to other tasks, to comply with the requirements of performing, reviewing and documenting the various activities related to the surveillance and testing.

It follows that decisions about determining specific technical specifications require careful consideration of the advantages and the disadvantages of a particular set of TS. Until recently, however, TS for RPS were established on the basis of engineering judgment on the part of the regulatory bodies. Such ad-hoc determinations of technical specifications were not, however, necessarily optimum from either the safety point of view or the plant-availability point of view. As a result, in recent years there has been a growing interest in reviewing the TS of the RPS (as well as those for other systems) using PSA techniques that allow for the quantification of most of the impacts (positive and negative) of a specific set of TS.

1.3. BENEFITS AND COSTS ASSOCIATED WITH THE TS OF THE REACTOR PROTECTION SYSTEM

The first step in a formal decision making approach is the identification of those areas of concern that are affected by the various alternative courses of action and that produce the "benefits" and the "costs" associated with each possible decision.

The second step consists in defining attributes or measures of effectiveness that provide a quantitative measure of the identified costs and benefits.

The third step determines the possible value ranges and the associated uncertainties for all the attributes that are implied by each and every alternative course of action.

Finally, in the fourth step the alternatives are compared on the basis of their "scores" in the attributes and the most preferred is chosen.

The alternatives in a decision problem about the TS of the RPS are simply the possible values of the surveillance frequencies and the allowable times in the bypass mode of the various components. As mentioned above, in order to be able to compare any two sets of TS we must first define the areas of concern affected by the TS, and the attributes that measure the impact of each particular TS in these areas.

There are four general areas of concern that are affected by changes in the TS for the electrical part of the RPS:

(i) Unavailability of the RPS to sense the need for and signal a reactor scram.

(ii) Unnecessary plant transients and challenges to the protection system.

(iii) Human factors considerations.

(iv) Plant and manpower availability.

The first area has to do with the availability of the RPS and the likelihood of an anticipated transient without scram (ATWS). A decrease in the surveillance frequency of the components and an increase in the allowable out-of-service times tends to increase the unavailability of the RPS. This in turn means an increase in the probability of core damage following a failure to scram along with possible offsite consequences. The benefits and the costs incurred by a change in the TS in this area have to do with decreases and increases in the RPS availability.

The second area (i.e. reduction of unnecessary plant transients) has to do with the spurious trips and resulting scrams that are associated with test and maintenance activities. There are two sources for these scrams.

(a) During the test and maintenance, an analog channel (after the initial allowable bypass time) is tripped. This changes the logic of the channels from 2-out-of-4 to 1-out-of-3. A spurious trip in one of the remaining channels results in a spurious scram. An increase in the maximum allowable time in a "bypass" mode, therefore, decreases the probability of spurious scrams.

(b) Spurious scrams can also be generated during test and maintenance of any part of the RPS because of human errors. A decrease in the frequency of testing decreases the probability of spurious scrams.

Spurious scrams (like regular scrams) represent a challenge to the decay heat removal and other safety systems of the plant and have the potential of leading to core damage. A decrease in the surveillance frequency and an increase in the allowable out-of-service times tends to decrease the frequency of spurious scrams and hence the probability of core damage. Another effect of the reduction of the spurious scrams is a related reduction in the number of the actual scrams. This is due to the fact that a large number of scrams in PWRs occur during the start-up phase because of steam generator and feedwater system instabilities. Every time the plant scrams, because of a spurious signal, there is a chance for an additional scram on the way back to power.

The third area (i.e. human factor considerations) actually includes a number of benefits. One such benefit can be derived from the fact that shift supervisor and control room operators will have to spend less time in authorizing and overseeing the tests, attending and being aware of the causes and alarms and false instrument readings, and hence spend more time in monitoring other plant functions pertaining to normal plant operations and other safety aspects of the plant. Another human factors benefit is that with less testing and false alarms the operators might be more sensitized to plant alarms and abnormal indications. The quantification of these two benefits is indeed difficult and it could be done only if a complete PSA, for the plant in question, is available. But in principle it is possible. Another effect of increasing the allowable out-of-service times and pertaining to human factors is the potential for a decrease in the probability of human error during test and maintenance. Given the reluctance of the plant management to put analog channels in a tripped mode, as well as the potential significance of exceeding the plant technical specifications (forced shutdown) the test and maintenance personnel are under pressure to complete the repair within the (short) time allowed by the technical specifications. The probability of human error under these circumstances is higher than if more time were available.

The fourth area is economic in nature. By reducing the spurious scrams and the actual scrams that are associated with the corresponding comebacks to power, the plant availability increases and this of course implies significant economic benefits. The decrease in the manpower necessary to perform these tests also implies an economic benefit.

Given these four areas of concern and the associated costs and benefits, attributes could be defined that measure the effect of a particular set of TS in each and every of the identified costs and benefits. Decisions on the basis of such quantitative results would not be so straightforward, however, since one would have to compare a decrease in the availability of the RPS with a decrease in the number of the spurious scrams and maybe a decrease in the probability of a human error during testing. Instead three more general groups of attributes can be identified. Each group suggests a different basis for decision making.

(i) **Single Risk-Attribute:** This approach quantifies all the safety related "benefits" and "costs" of the alternative policies in terms of their effect on a single risk attribute or index; e.g. the frequency of core damage. This includes the effect of any change in the test frequencies on the unavailability of the RPS (and consequently on the frequency of core damage as a result of an ATWS), on the

probability of human error and through that on the RPS unavailability, and on the probability of spurious and actual scrams (and consequently on the probability of core damage that could occur as a result of these transients). The various TS policies are then evaluated only on the basis of their effect on this single attribute.

(ii) **Risk Value-Impact-Multiple Attributes:** This approach is similar to (i) but it goes one step further by calculating the effect of the alternative policies on several risk indices (i.e., core damage frequency, acute fatalities, and latent fatalities). Usually the tradeoffs between various TS policies involve a change in the ATWS frequency and an opposite change in the frequency of core damage from spurious or actual scrams. Since the consequences (health effects) of core melt scenarios resulting from an ATWS are usually different than those resulting from scrams, this approach introduces additional dimensions into the decision making process. Actually this approach weighs differently a change in the ATWS-induced core damage frequency than a similar change in the scram-induced core damage frequency. As a result, a policy favored by approach (i) above could be rejected by approach (ii). This increased dimensionality poses two problems: first, the calculation of the effect on the acute and latent fatalities requires plant-specific and site-specific considerations and second the existence of a level-3 PSA.

Probabilistic Safety Assessment models and techniques provide the necessary quantification of the effects of an TS policy on any of the attribute groups mentioned above. The PSA model can be a single system reliability model that provides the unavailability of the system, a level-1 PSA assessing the frequency of core damage, or a level-3 PSA providing estimates for the ultimate health consequences. As the level of completeness in the PSA models increases so does their complexity, the required information, and the level of effort to generate and quantify them. Thus, while a single system model requires information only about the system design, a level-1 PSA requires information about the whole plant, and the level-3 PSA requires information about the specific site of the plant.

Finally, the last step of the decision making procedure would be to compare the alternative TS policies on the basis of their "score" in the chosen group of attributes. If a single attribute is used, this comparison is straightforward since either more or less of the attribute would be preferable. If, however, several attributes are chosen then the comparison between two alternatives requires, in general, some sort of preference assessments or value tradeoffs, in order to make possible the comparison among attributes that are measuring different concepts.

2. OBJECTIVES AND SCOPE OF THE STUDY

2.1. OBJECTIVES

The objectives of the work reported here are the following:

Present a methodological framework for making decisions about the TS for systems in nuclear power plants.

Develop a methodology for decision making about the TS of the Reactor Protection System, as well as any other system for which the allowable outage times are short compared to the mean times to failure and repair. This methodology should include a model for the system that would allow the quantification of as many effects as possible of the TS on the safety and the economics of the nuclear power plant.

Specialize the decision making methodology so that a single attribute measures all the safety related concerns and another single attribute measures the non-accident related economic effects. In particular, use the probability of core damage per year of reactor operation as the single risk index and the expected downtime per year of reactor operation as the single (non-accident related) economic index.

Demonstrate the methodology by a full scope application on the TS for the RPS of a nuclear power plant.

2.2. SCOPE

The methodology developed in this study covers decisions on the surveillance frequencies or surveillance test intervals (STIs) and the allowable outage times (AOTs) for components of systems that are standby, tested and if needed repaired. The standby operation is meant in the sense that a real need for the system does not exist constantly but it arises randomly by corresponding demands. Furthermore, the developed methodology covers decisions for the STIs and the allowable bypass times (ABTs) for the components of the instrumentation of the RPS.

The developed model for the RPS includes the effects of STI and ABT on the probability of core damage per year of reactor operation and on the availability of the plant for electricity generation. These effects include all the areas of concern discussed in Section 1.3.

A full scale application of the developed methodology was performed on the RPS of a Westinghouse RESAR-3S PWR [1]. The application contains two parts.

(1) A comparison of two specific TS policies: the one in force at the time of the analysis [2]; and an alternative proposed by the Westinghouse Owners Group (WOG) to the United States Nuclear

Regulatory Commission (USNRC) [3]. In the WOG request all the concerns discussed in Section 1.3 are mentioned but in the supporting analysis only the effect on the RPS unavailability is quantified. The model developed in this study can quantify all these aspects. Details of the model capabilities are given in Section 4.2. The effects of changing TS on the probability of human errors are not, however, included in the numerical application owing to the lack of relevant data. The two policies are compared on the basis of the corresponding core damage probability and reactor unavailability.

Use of generic data was made in the quantification of the model along with results of plant specific PSAs. A sensitivity analysis of the results on key parameters of the model was performed.

Finally an uncertainty analysis was performed to investigate how the comparison of the two policies is affected by the uncertainty in the inputs and parameters of the model.

(2) Determination of the "optimum" TS policy: a study of the effects on the attributes of changing the TS over a range of possible values and under several assumptions (sensitivities) was also performed. The TS policy that "minimizes" the adverse effects on the attributes would be the preferred one.

3. OVERVIEW OF THE ANALYSIS

3.1. OVERVIEW OF THE METHODOLOGICAL FRAMEWORK

The basic steps in the overall methodology for evaluating alternative technical specifications are depicted in Figure 1.

The first step consists in determining the technical specifications to be evaluated. This includes the system and/or the procedures they refer to, the technical specifications currently in place and the basis for their establishment. Next, the alternative sets of technical specifications or policies to be evaluated are determined. A single specific alternative could be compared against the current practice, or a range of alternatives could be considered among which the "best" is to be chosen.

The second step consists in establishing the "areas of concern", that is, the characteristics of the nuclear power plant that are affected by the technical specifications under review. These usually include safety and economics although reliability of electricity supply might also be an issue. Furthermore, this step establishes the specific ways in which the general areas of concern are affected by a change in the technical specifications, e.g. by affecting the availability of a safety system.

In the third step attributes or indices of performance are established that measure the extent to which a specific area of concern is affected. In the probabilistic safety assessment (PSA) approach risk indices are used to measure the impact on safety, and expected plant availability can be used to measure both economic impacts (accident and non-accident related) and reliability of electricity supply.

The fourth step of the analysis is performed interactively with the second and third steps. In this step PSA models are established that quantify the impact of the technical specifications on the areas of concern through their effect on the chosen attributes. The PSA models can be viewed as functions that map the space of the possible alternatives of technical specifications to the space defined by the attributes. If the probability of core damage per reactor year is used as an attribute then, in general, elements and results of a level-1 PSA are required. If health consequences are included in the set of attributes then results of level-3 PSA are required. As a general rule, detailed models are required only for the systems that are directly affected by the technical specifications under review, while summary results - as conditional probabilities and importance measures - of the rest of the PSA are sufficient. In some approaches the whole analysis can be performed on the basis of importance measures that have been calculated for the technical specifications.

In the fifth step, the PSA models are quantified and the numerical values of the attributes corresponding to each alternative technical specification policy are assessed.

The sixth step is performed only if two or more attributes have been chosen. In this case a preference assessment, that is a value trade off among the attributes, must be established before a

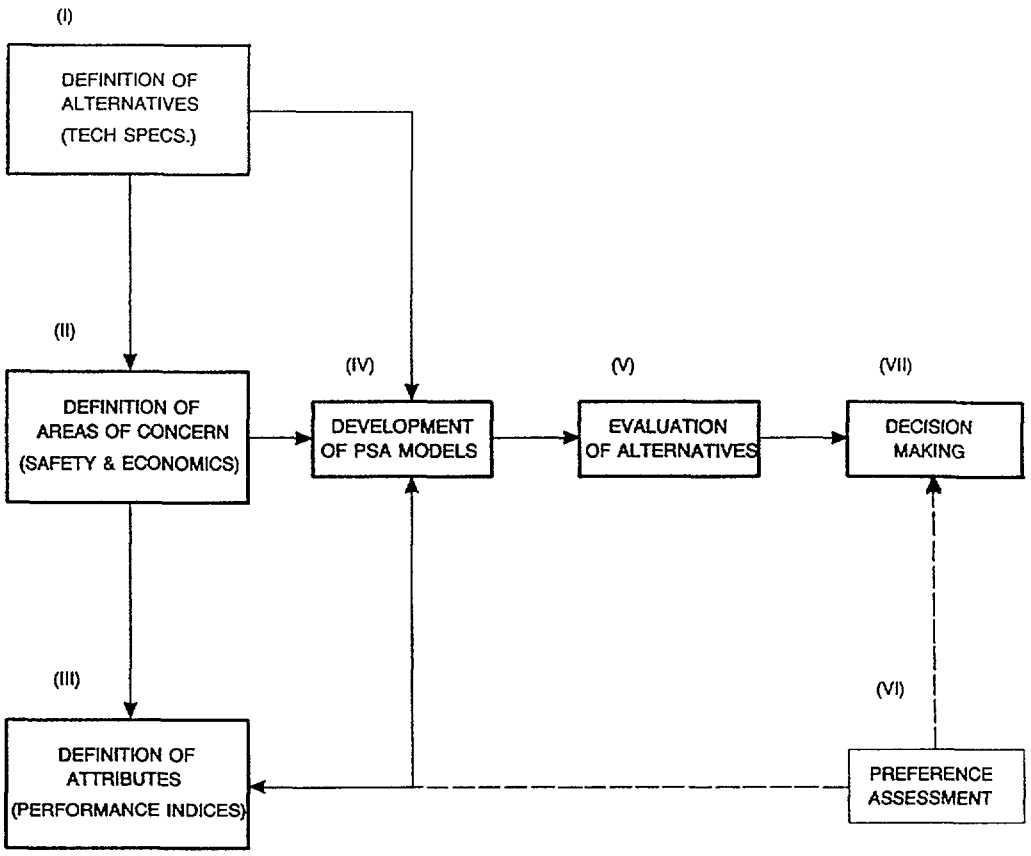


FIG. 1. Overview of methodological framework for technical specification evaluation.

comparison of the effects of two different alternatives can be made. This is a very important and at the same time difficult task because it is not mathematical or calculational in nature but rather it involves the assessment and the quantification of value judgments. This means that probability of core damage must be valued against health consequences and all these against economic impacts. Often this step is ignored, although any type of decision making implicitly (if not explicitly) makes such value judgments.

The seventh and final step of the analysis involves the actual decision making, that is, the comparison of the various alternatives through their impact on the attributes. If only one attribute has been chosen, such as system unavailability or probability of core damage per year of reactor operation, the comparison is straightforward. Usually, in those cases the fifth and seventh steps are combined into one "optimization" procedure in which the technical specification that minimizes the single attribute is established. In that case step six is of course not necessary.

The sixth step might not be necessary for the performance of the seventh step in some special cases of "dominance" even if two or more attributes are used. If, for example, a specific technical specification results in better values in all the attributes than another, then value tradeoffs among the attributes are not necessary since the comparison is straightforward.

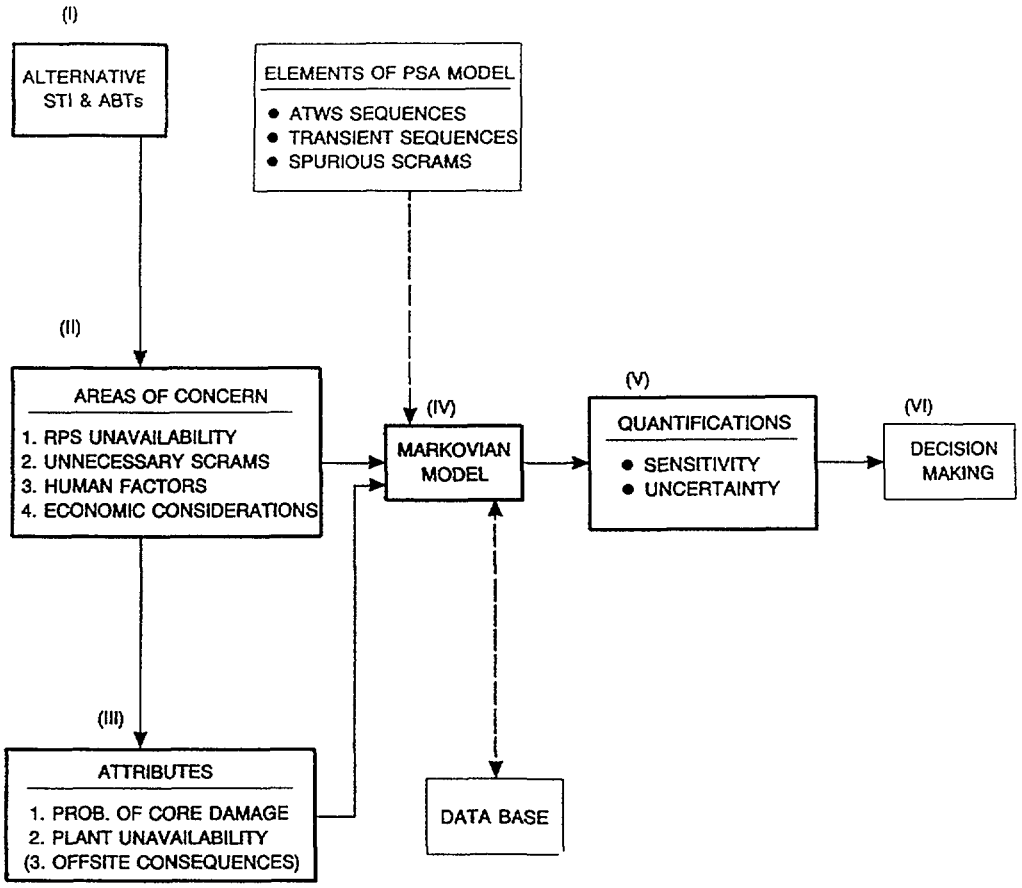


FIG. 2. Overview of the methodology for the evaluation of alternative STIs and ABTs for the reactor protection instrumentation system.

3.2. OVERVIEW OF THE METHODOLOGY FOR THE REACTOR PROTECTION SYSTEM

The basic steps of the methodology followed for the evaluation of technical specifications of the reactor protection instrumentation system (RPIS) and the specific applications are depicted in Figure 2.

In the first step the technical specifications to be evaluated are determined. For the RPIS these are: the frequency of surveillance (SF) of the analog channels and the logic trains; and the times for which they are allowed to remain in the bypass mode (ABT) while tested and/or repaired before they are tripped. In this study two distinct cases have been analyzed. In the first, two specific sets of SFs and AOTs, one in place at the time of the analysis [2] and a second proposed by the WOG [3] are to be compared. In the second, a range of SFs for the logic trains is to be evaluated for different values of ABTs.

In the second step, safety and economics were chosen as the areas of concern affected by changes in the RPIS technical specifications. The TS affect the availability of the RPS, the frequency of transient initiators - through spurious scrams, the availability of the plant, and the probability of human errors during testing and/or repair. All these have an impact on both plant safety and economics.

The attributes that measure the extent to which plant safety and plant economics are affected are established in the third step. These are: (1) probability of core damage per year of reactor operation; (2) plant availability for electricity production. It is felt that the probability of core damage per reactor year is an adequate measure of the level of safety that characterizes a particular power plant. The results of this analysis can be readily extended to include the effect on offsite consequences as it is explained later in this section. Plant availability has been chosen as an economic attribute since it affects the amount of electricity produced by the plant. Any non-accident related economic impacts are directly related to the amount of electricity produced which is the only quantity that can be affected by a change in the TS of the RPIS.

To quantify the effect of TS on the chosen attributes, a Markovian Reliability Model has been developed in the fourth step. This model simulates the stochastic behavior of the nuclear reactor as a function of time. Only the RPS instrumentation is modeled explicitly (at the component level) while the remaining elements (e.g. decay heat removal systems) are modeled through summary results from other PSA models. These summary results include the conditional probability of core damage given an ATWS and the conditional probability of core damage given a successful real scram. The model calculates the probabilities of various plant damage states the sum of which provides the probability of core damage. Each plant damage state can result in offsite consequences with different probabilities which, however, depend only on the containment performance and on the site characteristics. Consequently, if these latter probabilities are available the results of this analysis can be expanded to include the effect of TS changes on offsite consequences.

The Markovian model developed in this study has several advantages over the traditional combinations of event and fault trees. These advantages are fully discussed in the appropriate part of Section 4.2. Here it suffices to mention that it allows for the quantification of TS impacts on the probability of core damage that are not directly or indirectly due to the RPS unavailability, such as the impact of spurious scrams, and the TS impact on the reactor availability.

In the fifth step the values of the model parameters are assessed using generic data bases, as well as plant specific PSAs, and the model is quantified. A combination of two computer codes (STAGEN and MARELA) has been used for the building and the quantification of the model. These codes are described in Ref. [25]. The quantification of the model provides as output the probability of core damage per year of reactor operation (along with its constituents, plant damage state probabilities) and the expected reactor downtime per year of reactor operation.

Finally in the sixth step the results are displayed and discussed but no attempt is being made to provide value tradeoffs of core damage and expected reactor downtime. The latter are left to appropriate decision makers.

4. CALCULATIONAL PROCEDURES AND METHODS

4.1. TESTING PROCEDURES FOR THE REACTOR PROTECTION SYSTEM INSTRUMENTATION

4.1.1. System description

The reactor protection system (RPS) keeps the reactor operating within a safe region. If one or more physical parameters enter an unacceptable range of values, a trip signal will be produced to de-energize the electromagnetic holding power of the control rod drive mechanisms so that the control rod drop because of gravity ensures an orderly shutdown of the nuclear chain reaction. Typical plant parameters which are monitored and used as inputs to the RPS are the following [1]:

- Power range neutron flux
- Power range neutron flux-high positive rate
- Power range neutron flux-high negative rate
- Intermediate range neutron flux
- Source range neutron flux
- Overtemperature ΔT
- Overpower ΔT
- Pressurizer pressure - low
- Pressurizer pressure - high
- Pressurizer water level - high
- Loss of reactor coolant system flow
- Steam generator water level - low low
- Steam/feedwater flow mismatch and steam generator water level - low
- Undervoltage - reactor coolant pumps
- Underfrequency - reactor coolant pumps
- Turbine trip - low fluid oil pressure
- Turbine trip - turbine stop valve closure
- Safety injection signal
- Reactor coolant pump breaker position

The electrical portion of a typical RPS of Westinghouse-designed pressurized water reactors consists of analog channels, logic trains and trip breakers. The specific design details may differ depending on the vintage of the reactors. The particular hardware configuration which is the subject of this study is that of a 4 loop RESAR-3S PWR [1] type reactor with solid state combinational logic units. References [1,3] describe the RPS in greater detail.

Analog Channels

The analog channels sense the plant parameters and provide binary (on-off) signals to the logic trains. A typical analog channel is composed of a sensor/transmitter, a loop power supply, signal conditioning circuits and a signal comparator (bistable). The bistable compares the incoming signal to a setpoint and turns its output off if the input voltage exceeds the setpoint. Each bistable feeds two separate input relays, one associated with reactor trip logic train A and the other associated with reactor trip logic train B. Each plant parameter listed above has, in general, its own analog channels with varying degree of redundancy depending on the parameter (e.g. 2-out-of-4 for the power range neutron flux and 2-out-of-3 for the pressurizer water level-high). However, some plant parameters share the sensors and transmitters. For example, the same sensors and transmitters are used for the pressurizer low pressure trip and for the high pressure trip. The signal is evaluated by two separate bistables with different setpoints.

Logic Trains and Trip Breakers

There are two logic trains and each logic train receives signals from the analog channels through input relays. The input signals are then applied to universal boards which are the basic circuits of the protection system. They contain 1-out-of-2, 2-out-of-3, 2-out-of-4 coincidence logic circuits depending on the plant parameters and the corresponding analog channels, as mentioned earlier. The trip signals generated in the universal boards are sent to undervoltage (UV) output boards or engineered safeguard output boards. The UV board in each logic train has two UV coils, one for the reactor trip breaker and another for the bypass breaker which is racked out in normal operation of the plant. A trip signal from the UV board will de-energize the UV coils by removing the 48 volt output of the UV board. This will open the reactor trip breaker or the bypass breaker (if closed as in the case of test and maintenance of the corresponding trip breaker) removing power supply holding the control rods.

4.1.2. Testing procedures

The RPS is designed to allow periodic testing during power operation without initiating a protective action unless a trip condition actually exists. An overlapping testing scheme, where only parts of the system are tested at any one time, is used. Typical RPS testing involves verification of proper channel response to known inputs, proper bistable settings and proper operation of the coincidence logic and the associated trip breakers. Detailed testing procedures including testing frequency and allowable bypass times are described in Refs. [2] and [3].

Analog Channel Testing

The analog channel testing is to verify that the analog channel is functioning properly and that bistable settings are at the desired setpoint. During test, the test switch disconnects the sensor/transmitter

from the channel and the circuit is capable of receiving a test signal through test jacks. The input signal to the test jacks is then adjusted to check operability and setpoints of the bistable. The analog channel under test is allowed to be bypassed for a duration specified by the technical specifications and put in a trip mode if the allowable bypass time is exceeded.

Logic Train and Trip Breaker Testing

This portion of the RPS testing encompasses three stages: (1) testing of input relays places each channel bistable in a trip mode causing one input relay in logic train A and another in logic train B to de-energize. Each input relay operation will light the status lamp and annunciator. This stage of the testing provides overlap between the analog channel and logic train positions of the test procedure: (2) testing of logic trains involves one train at a time. The semi-automatic test device checks through the solid state logic to the UV coil of the reactor trip breaker. The logic train under test is also allowed to be bypassed for the specific duration and the plant must be shut down if the allowable bypass time is exceeded; (3) testing of the trip breaker requires manual trip and operability verification of the bypass breaker and then manual trip test of the trip breaker through the logic train.

4.2. MARKOVIAN MODEL OF THE REACTOR PROTECTION SYSTEM

The basic principles of Markovian reliability analysis are discussed in References [6-11] and briefly presented in the Appendix. This section describes the Markov model developed for the electrical portion of the reactor protection system (RPS).

The model developed for this study does not include the mechanical portion (control rod drive mechanisms and control rods) and the operator manual actions to scram the plant by pushing the buttons in the control room or by locally opening trip breakers or output breakers on the rod drive motor-generator sets. The effects of these can nevertheless be included parametrically in the conditional probabilities of core damage given the electrical part of RPS is unavailable and available, respectively.

A typical four-channel parameter was considered to evaluate the effects of changes in the test procedures on unavailability and risk measures, e.g., increments in unavailability or core damage frequency.

The RPS is represented in a functional block configuration in Figure 3. There are four blocks for analog channels (one for each channel) and two blocks for logic trains (one for each logic train and the associated trip breaker).

Each functional block is considered as a supercomponent composed of several basic components in series. Hence, the failure rate of a block is simply the sum of the failure rates of the composing components.

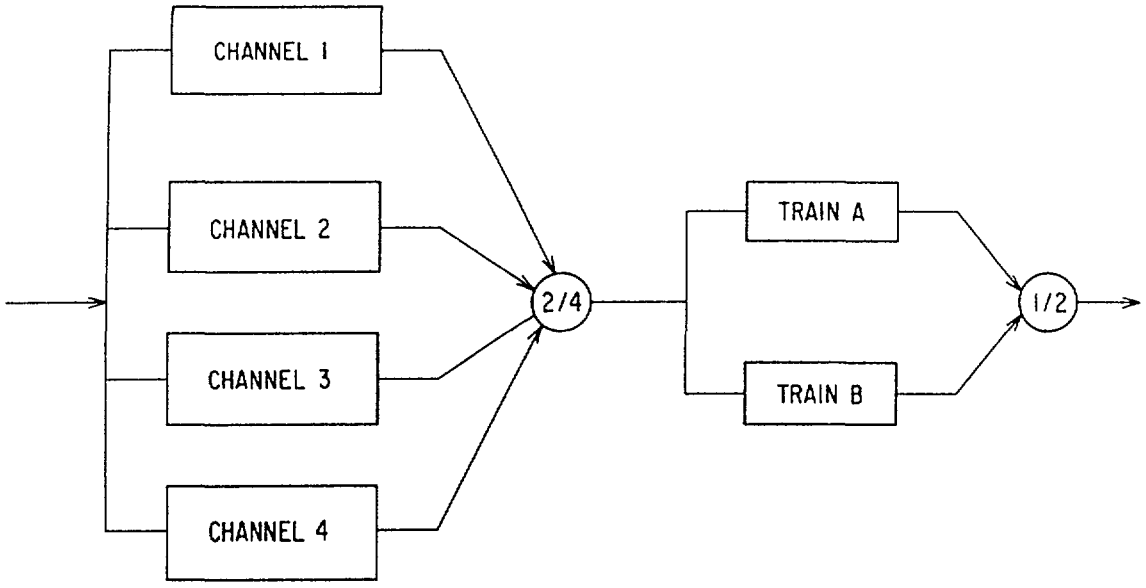


FIG. 3. Reactor protection system instrumentation functional block diagram.

The block for an analog channel consists of the following components:

- a sensor/transmitter
- loop power supply (120V AC)
- signal conditioning circuits
- a bistable
- an input relay

It is noted that each bistable feeds two input relays, one for each logic train. To avoid complexity of the model, however, it is assumed that each bistable feeds only one input relay. This is a slightly conservative assumption.

The block for a logic train consists of the following components:

- solid state combinational logic circuits
- DC power for the logic circuits (15V DC)
- undervoltage coils
- DC power for the undervoltage coils (48V DC)
- a trip breaker

The state transition diagram for an analog channel is given in Figure 4. An analog channel is represented by a five-state component:

State 1: is the operating state.

State 2: is the failed state. In this state the component is failed, the failure can be detected in the next test and the component will be put under repair.

State 3: is the tripped state. In this state the channel generates a trip signal and it may undergo repair.

State 4: is the bypass state related to state 1. To perform a test the channel can be bypassed for a prespecified period of time: allowable bypass time (τ). At the end of this period the component transits instantaneously to state 3.

State 5: is the bypass state related to state 2. If the channel is failed the testing and repairing can be performed while in a bypass mode, provided that the allowable bypass time (τ) is not exceeded.

If the analog channel is in state 1, it may transit (see Figure 4):

(a) to state 2 with a failure rate λ;

(b) to state 3 when any one of the internal components gives a spurious trip signal or if it fails in a detectable way and the operator immediately trips the channel with transition rate "λ_s"; and

(c) to state 4 following a test, which takes place every T hours.

Thus the transition rate is represented by a delta function $\delta(t-kT)$, $k=1,2,...$

If the analog channel is in state 2 it transits to state 5 following a test.

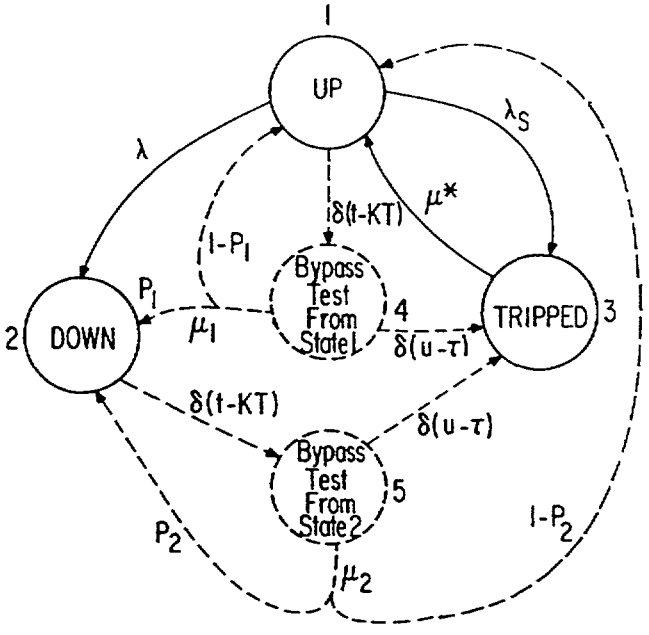


FIG. 4. State transition diagram for analog channel: "Non-Markovian" model.

If the analog channel is in state 3 it transits back to state 1 once the repair is completed, with transition rate μ^*.

If the analog channel is in state 4 it may transit to:

(a) state 3 if the testing is not completed within the ABT (τ) [instantaneous transition symbolized by the delta function $\delta(\mu\text{-t})$ where μ is the time spent in state 4];

(b) state 1 if the test is completed within the ABT (τ) and there is no human error in restoring the channel in its operating state [transition rate $\mu_1(1\text{-}P_1)$];

(c) state 2 if the test is completed within the ABT (τ) and there is a human error that leaves the channel failed (transition rate $\mu_1 P_1$);

If the analog channel is in state 5 it may transit to:

(a) state 3 if the test/repair is not completed within the ABT (τ) [instantaneous transition symbolized by the delta function $\delta(\mu\text{-t})$];

(b) state 1 if the test/repair is completed within the ABT (τ) and no human error is committed in restoring the channel into its operating state [transition rate $\mu_2(1\text{-}P_2)$];

(c) state 2 if the test is completed within the ABT (τ) and there is a human error that leaves the channel failed (transition rate $\mu_2 P_2$).

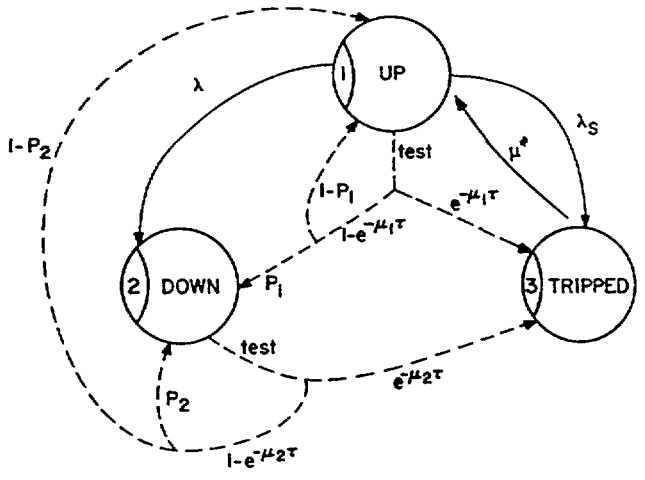


FIG. 5. State transition diagram for analog channel: "equivalent" Markovian model.

Whenever the allowable bypass time is small compared to the mean time of channel failure, the two test states (4 and 5) can be omitted by assuming that the transitions in and out states 4 and 5 occur instantaneously at the time of testing and with the following probabilities (see Figure 5):

(i) from state 1 to state 3 with probability $\exp[-\mu_1\tau]$, i.e. probability that the test will last for more than τ units of time;

(ii) from state 1 to state 2 with probability $P_1(1-\exp[-\mu_1\tau])$; i.e. probability of completing the repair in less than τ units of time and that of a human error will occur;

(iii) from state 2 to state 3 and state 1 with probabilities $\exp[-\mu_2\tau])$ and $(1-P_2)(1-\exp[-\mu_2\tau])$, respectively.

In this study, exponentially distributed times to test completion were used. This assumption is not, however, a requirement of the model. Any distribution of testing times can be used. Only the cumulative probabilities are needed in the model.

The state transition diagram for the logic train and trip breaker is similar to the one for the analog channel and it is presented in Figure 6. The mean time to complete the test (μ_1) can be different for the logic train than that of the analog channel.

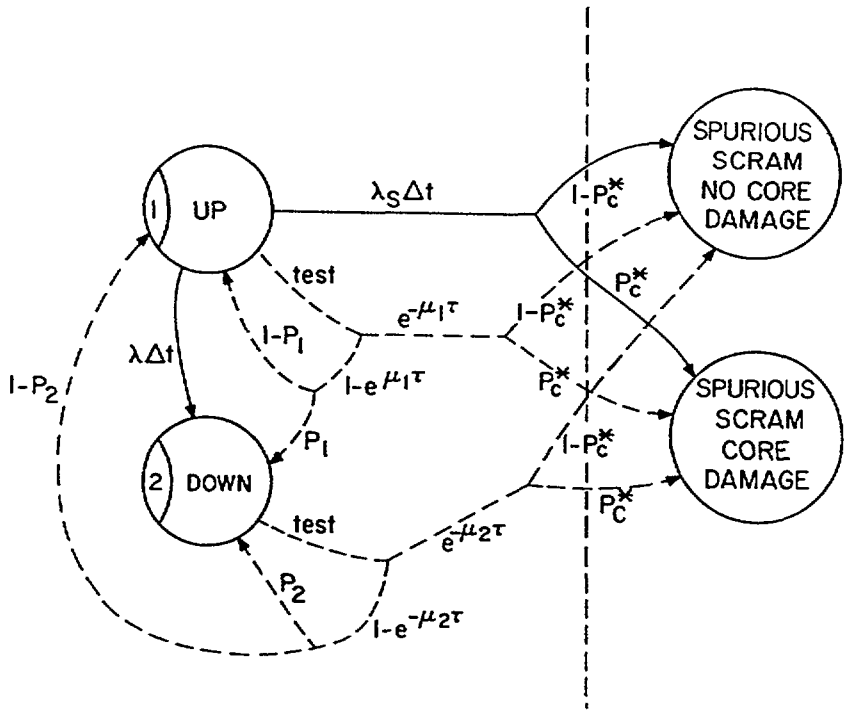


FIG. 6. State transition diagram for logic train: "equivalent" Markovian model.

The six components (4 analog channels and 2 logic trains) form a system that can be in 729 ($=3^6$) states. The system states are generated by the computer code STAGEN (see [25]) but not all of them are necessary for the solution of the model. The system states have been regrouped into 198 states. The major grouping involves states that imply a spurious scram. If two analog channels are in the trip state or if one logic train is in the trip state a spurious scram signal is generated because of the 2-out-of-4 and 1-out-of-2 logic, respectively. The scram signal will cause a reactor shutdown that will result in a successful shutdown or in a core damaged state depending on the availability of the decay heat removal function. All the system states with two tripped analog channels or one tripped logic train were merged into two global system states.

The 198 system states can be further grouped into the following nine groups:

(1) **RPS Available With No Tripped Analog Channel:** this group contains all system states with at least two analog channels and one logic train operable. If the RPIS is in one of these states it can sense the need and send a signal for a reactor scram.

(2) **RPS Available With One Tripped Analog Channel:** this group contains all system states with one analog channel tripped and at least one more analog channel and one logic train operable. If the RPIS is in one of these states it can sense the need and send a signal for a reactor scram. A spurious scram signal from one of the operating analog channels generates a spurious reactor scram.

(3) **RPS Unavailable**: this group contains all the states that imply system unavailability (two logic trains or three analog channels failed).

(4) **"Real" Scram-No Core Damage**: this group contains all the states of the system that imply an available RPS and the successful reactor shutdown following a "real" scram signal. Real signal means a signal generated by the RPS by properly responding to abnormal conditions of the plant.

(5) **"Real" Scram-Core Damage:** this group contains all the system states that imply an available RPS and the reactor in core-damaged state. The RPS successfully responded to the "real" challenge but the decay heat removal function failed.

(6) **"Spurious" Scram-No Core Damage:** this corresponds to Group No. 4 with the scram signal spuriously generated internally to the RPS.

(7) **"Spurious" Scram-Core Damage:** this corresponds to Group No. 5 with a spurious scram initiator.

(8) **ATWS-No core Damage:** this group contains all the system states that imply an unavailable RPS coupled with a real challenge (Anticipated Transient Without Scram-ATWS) but with successful mitigation of the event.

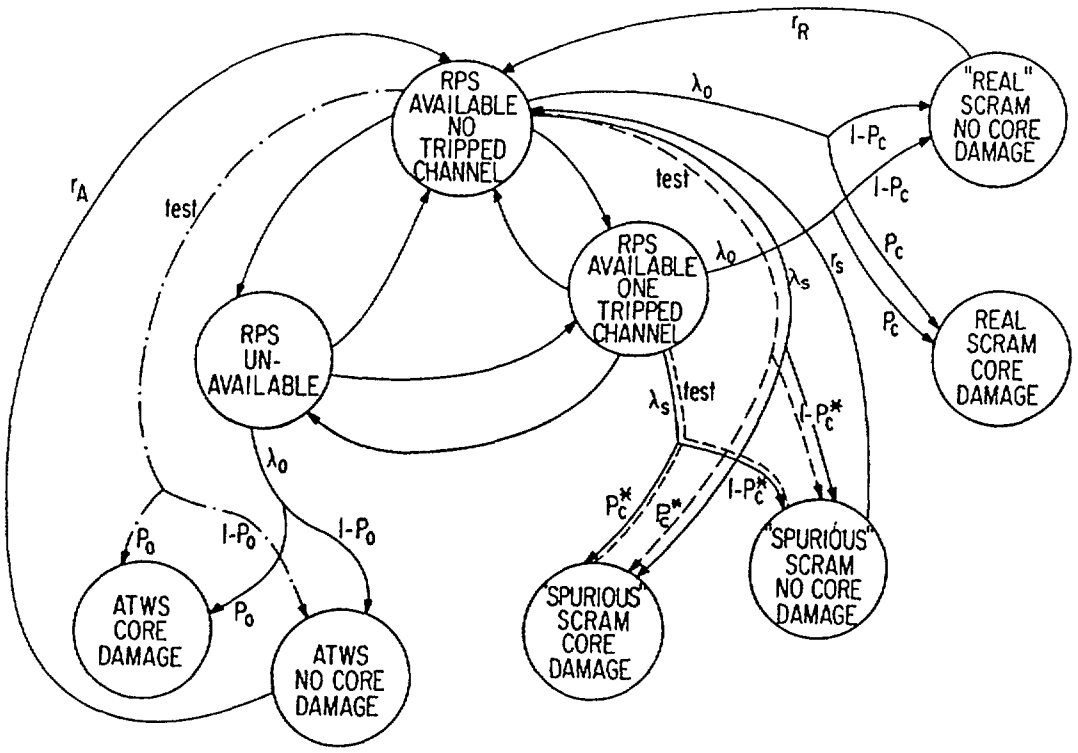


FIG. 7. Generalized state diagram.

(9) **ATWS-Core Damage:** this group contains all the system states that imply unavailable RPS coupled with a real challenge (ATWS) that results in core damage.

The system transitions are graphically depicted, in summary form, in the state transition diagram in Figure 7. If the system is in a state of group 1 it can transit to another state in the same group, or a state in group 3 if a component fails. The system transits from a state of group 1 to a state of group 2 if an analog channel trips. Transitions from groups 2 and 3 back to group 1 occur whenever a component is repaired. Similar transitions (involving failures and repairs of components) can occur within groups 2 and 3 as well as between groups 2 and 3.

If the system is in a state of group 1 or 2 (available), a real challenge assumed to occur according to a Poisson random process with intensity λ_0 will generate a scram which in turn will result in core damage with probability P_c or in a safe shutdown with probability $1-P_c$ (see Figure 7). The "real scram-core damage" state is an absorbing state, that is, the system can not leave this state. Following a successful scram, however, the reactor is brought back on line after spending some time (random variable) in the shutdown mode. This transition, back to the operating state, is depicted in Figure 7 by the transition rate r_R. It is further assumed that following a successful scram all existing failures in the RPS are detected and repaired.

Spurious scrams are modeled by transitions from either group 1 or group 2 to the "spurious scram-no core damage" states (group 6) and "spurious scram-core damage" state (group 7). From a state

in group 1, a spurious scram can occur if a spurious signal is generated (randomly with time) in a component of the logic train and trip breaker or if the allowable bypass time (ABT) is exceeded while testing and/or repairing such a component. The same transitions are possible from a state in group 2. Additional spurious scrams are possible from states in group 2, however, if a spurious scram signal is generated by an analog channel (one channel is already tripped) or if the allowable bypass time for testing/repairing an analog channel is exceeded. The conditional probability of core damage given a spurious scram is now denoted by P_c^* (see Figure 7). From a safe shutdown state following a spurious scram the system is brought back to the operating state (renewed) with rate r_s (see Figure 7).

ATWS events can occur from some states in groups 1 or 2 and all states in group 3. If the system is in a state of group 3, it is unavailable to detect the need for shutdown and a challenge will bring the system to an "ATWS-No Core Damage" (group 8) or "ATWS-Core Damage" (group 9) state with probability $1\text{-}P_o$ and P_o, respectively. ATWS transitions can occur from states in groups 1 and 2 during tests. If the system has two analog channels and/or one logic train failed undetected then a test of a "good" component (channel or logic train) will put this component in a bypass mode and it will render the system unavailable for the duration of the test. If a challenge occurs during this time an ATWS will occur. The system then transits to "ATWS-Core Damage" and "ATWS-No Core Damage" states with probabilities P_o and $1\text{-}P_o$, respectively. From the ATWS-No Core Damage state the system returns to the operating state (renewed) with rate r_A (see Figure 7). The transitions to the "ATWS-Core Damage" states are among the most safety significant transitions because of the severe offsite consequences they imply. Additional features of the model are staggered testing and inclusion of common-cause failure modes. Uniform staggered testing [4] has been assumed for the analog channels and logic trains. Multiple dependent component failures because of a miscalibration of sensors during the annual refueling outage have been included in the model. Externally (to the system) generated common cause failures are also included in the model using the ß factor approach [12].

4.3. SPECIAL FEATURES OF THE MARKOVIAN MODEL

The Markov model for the RPS described in the previous subsection includes several characteristics of the stochastic behavior of the system that cannot be adequately modeled by the current state-of-the-art PSA techniques. In present PSA techniques, the system is modeled by a fault tree or an equivalent logic model which in turn is quantified by inputting the average unavailabilities of the components. The average (over time) component unavailabilities are estimated by considering each component independently of the other components or of the system. Thus, the current PSA techniques do not consider the effects of the time dependence of the system characteristics and the effects of dependence of the stochastic behavior of the component on the state of other components and/or the system (see Appendix). It is almost always possible to apply the current PSA techniques with assumptions that will provide "conservative" answers in the sense that they will overestimate the various unreliability parameters of the system. It is not, however, obvious that such overestimations are desirable or that they can provide useful

insights in cases where operating policy is to be decided at least partly on the basis of the results of a probabilistic assessment. The specific areas that the model presented in this paper improves over current PSA techniques are the following:

(i) Modeling of Multiple States: A component can be in any number of discrete states. In particular, the Markov model allows for the modeling of bypass and trip states for the analog channels and the logic trains. A current PSA technique (e.g. fault tree) would assume only one failed state (component unavailable) and it would assume that the component is unavailable every time it is tested and for a period of time equal to the mean time of the maintenance activity (see [3]). This approach creates three problems:

(a) It introduces a conservatism in the calculation by over-estimating the unavailability of the system. This is because when a channel is in a trip mode it takes three additional failures for the system to be unavailable. Assuming that the channel is unavailable, however, requires only two additional failures to fail the system;

(b) It introduces a nonconservatism by underestimating the probability of spurious scrams. When a channel is in a trip mode an additional spurious trip in anyone of the remaining channels will cause a spurious reactor scram;

(c) It introduces a difficulty in estimating the real effect of a TS policy change. It is conceivable that two alternative TS policies are characterized by the same mean time to test and repair a channel (which is a component characteristic after all) and different allowable times in bypass.

(ii) State Dependence: The stochastic behavior of the system might depend on its state. For example, the allowable bypass time for an analog channel should depend on whether another channel is already tripped or not. The repair rate of an analog channel might depend on whether another channel is under repair or on whether the reactor is shutdown or on line. Exceeding the allowable bypass time in an analog channel will generate a scram signal depending on whether another channel is tripped or not and on whether the reactor is on line or note.

(iii) Renewal Effect of Challenges: A successful challenge to the system will reveal any existing failures which will be subsequently repaired. Thus, the challenges to the system usually have the same effect as randomly occurring tests. However, whether a challenge will have the equivalent effect of a test on a component will depend on whether the system is available at the time of the challenge.

(iv) Inclusion of the "NO CORE DAMAGE" and "CORE DAMAGE" States: The inclusion of no core damage states is important because they allow for the estimation of the expected reactor

TABLE I FAILURE DATA

Component	Failure Mode	Failure Probability	Source (Ref.)
Analog Channel Block			
Input Relay	Fails to open	5.09(-7)/demand	[16]
	Operates spuriously	3.60(-8)/h	[16]
Loop Power Supply(120V AC)	Inoperable[1]	5.40(-7)/h	[17]
	Reduced Capability[1]	9.10(-8)/h	[17]
Signal Conditioning Module	Inoperable[2]	2.60(-6)/h	[17]
	Reduced Capability[2]	1.55(-6)/h	[17]
Comparator (Bistable)	Inoperable	6.50(-7)/h	[17]
	Reduced Capability	8.40(-7)/h	[17]
Sensor/Transmitter			
Neutron Flux	Inoperable	3.40(-6)/h	[17]
	Reduced Capability	8.50(-7)/h	[17]
Pressure	Inoperable	2.60(-7)/h	[17]
	Reduced Capability	3.10(-6)/h	[17]
Total			
Flux Channel	Fails to operate	6.65(-6)/h	
	Operates spuriously	3.91(-6)/h	
Pressure Channel	Fails to operate	3.51(-6)/h	
	Operates spuriously	3.91(-6)/h	
Logic Train and Trip Breaker Block			
Trip Breaker	Fails to open	2.27(-4)/demand	[16]
	Operates spuriously	4.30(-8)/h	[16]
UV Coils	Fails to open	5.09(-7)/demand	[16]
	Operates spuriously	3.60(-8)/h	[16]
DC Power (48V) for UV Coils	Inoperable	5.40(-7)/h	[17]
	Reduced Capability	9.10(-8)/h	[17]

[1] Both failure modes of power supply are considered to produce spurious signals

[2] In Ref. [17] "Inoperable" is defined as failure events involving actual failure and "Reduced Capability" as instrument drift, out-of-calibration, intermittent (spurious) events The condition of reduced capability is considered to produce spurious signals

TABLE I. (cont.)

Component	Failure Mode	Failure Probability	Source (Ref.)
Solid State Logic Circuits	Fails to operate Operates spuriously	1.73(-6)/h 2.48(-6)/h	[16] [16]
DC Power (15V) for Solid State Logic Circuits	Inoperable Reduced Capability	5.40(-7)/h 9.10(-8)/h	[17] [17]
Total Logic Train and Trip Breaker Block	Fails to operate Operates spuriously	2.52(-6)/h 3.28(-6)/h	

downtime that is directly related to the RPS. This quantity is an important attribute of any TS policy. In addition, the inclusion of the no core damage and core damage states permits a more accurate estimation of the system unavailability and failure probability. This is due to the fact that the system spends a finite amount of time in the "no core damage states". The time the system spends in states of groups 1 to 3 is then reduced accordingly and thus some double counting is avoided in the estimation of the systems unavailability and failure probability.

The Markov model calculates the effect of these characteristics by considering their impact dynamically, that is, as a function of time.

4.4. DATABASE

The failure rates of the components comprising the analog channels and the logic trains are given in Table I. The numerical values of other parameters required in the model are given in Table II.

The human error probability P_1 of failing a channel or a logic train following a test (see Figures 4, 6) was set at 10^{-2} following the WASH-1400 suggestion. The same value of 10^{-2} was used for the probability of failing to detect a failure (P_2) where it was assumed that all failures are detectable during test. Sensors in the analog channels are not, however, directly testable. It is assumed that failures of a single channel can be detected by comparing with indications of other channels. Common mode failures owing to sensors miscalibration committed during the annual refueling outage are not therefore detectable. The probability of four sensor miscalibrations was set equal to 10^{-3} ($10^{-2} \times 10^{-1} \times 1.0 \times 1.0$) again according to WASH-1400. To accommodate this common mode failure the probability P_2 was increased to 2×10^{-2}.

TABLE II. DATA FOR THE MODEL PARAMETERS

Parameter	Data	Source (Ref.)	Comments
μ_1^{TR}	1 h^{-1}	[3]	
μ_2^{TR}	1/7 h^{-1}	[3]	
μ_1^{CH}	1 h^{-1}	[3]	
μ_2^{CH}	1/7 h^{-1}	[3]	
μ_{31}^{CH}	1/16 h^{-1}	[3]	
λ_o	9.71 a^{-1}	[13]	Challenge rate on RPS (Frequency of Transients)
$r_s = r_R$	25.6 h	[3]	
P_c	1.43(-5)/demand	[14]	Indian Point-3 PRA revised by Sandia (internal transient initiators)
P_c^*	5.21(-7)/demand	[14]	

Common cause failures among the analog channels and among the logic trains have been treated by the ß-factor method [12].

The ß factor model assumes that components connected in parallel can fail in one of two modes:

(a) independently with failure rate $(1-ß)\lambda$; and

(b) because of a common cause that fails all the redundant components with failure rate $ß\lambda$.

Thus the total failure rate of the component is $(1-\beta)\lambda + \beta\lambda = \lambda$.

Viewed in a slightly different way the ß-factor model asserts that a component (redundant) fails with failure rate λ; from these failures a fraction ß will be due to common causes that fail all the redundant components.

The value of the parameter ß has been assumed the same for analog channels and logic trains and is treated parametrically as discussed in Section 5.2.

5. PRESENTATION AND INTERPRETATION OF RESULTS

The Markov model described in Section 4.2 was quantified using the data base given in Section 4.4. and the computer code MARELA (see [25]). The quantification of the model provides numerical values for two attributes of interest in the evaluation of the TS policies:

(1) the probability of core damage per year of reactor operation and
(2) the average reactor downtime per year of reactor operation.

The quantification of the Markov model provides the probabilities that the system will occupy each of the possible states as a function of time. The probability of core damage per year of reactor operation is given by the probability that the system will occupy any of the states in groups 5, 7 and 9 (see Section 4.2 and Figure 7) at the end of the one year period. Since core damage is a catastrophic failure from which no recovery is possible, each of the states in these groups is an absorbing state. The probability of finding the system in one of these states at time t is then equal to the cumulative probability that the time of core damage will be less or equal to t.

The probability that the reactor will be shutdown at time t is equal to the probability that the system occupies a state in groups 4, 6 or 8 (see Section 4.2 and Figure 7). Since the reactor is brought back to power from such a state, the probability of being in a state of groups 4, 6 or 8 is equal to the pointwise unavailability of the nuclear power plant [4]. The average unavailability of the reactor ($\overline{D}$) is obtained if the pointwise unavailability is integrated over the period of interest and divided by that period

$$\overline{D} = \frac{1}{T}\int_0^T D(t)dt$$

The average reactor downtime for the period T is then simply equal to $\overline{D}\ T$.

5.1. COMPARISON OF TWO TS POLICIES

5.1.1. General features of results

To demonstrate the methodology we report the results of the model for two specific TS policies. Policy 1 is the TS currently in place. Policy 2 is a proposed alternative to policy 1. A TS policy consists of the period of testing of analog channels (T^{CH}), the period of testing logic trains (T^{TR}), the allowable time in "bypass" for an analog channel if no other channel is tripped (τ_0), the allowable time in "bypass" for an analog channel if another channel is tripped (τ_1), and the allowable time in "bypass" for a logic train (τ). An uniformly staggered testing scheme [4] of the analog channels and the logic trains has been assumed for both policies and it is shown schematically in Figure 8. The values of the parameters are given in Table III. In summary, policy 2 extends both the testing periods and the allowable bypass times.

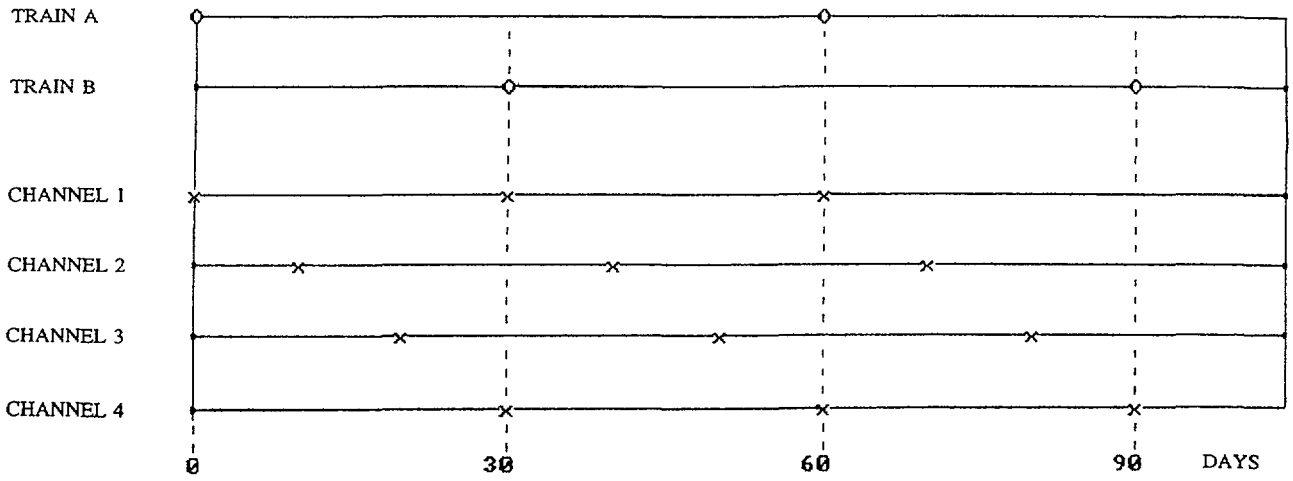


FIG. 8. Uniformly staggered testing schedule. Testing period for analog channels: 30 days. Testing period for logic trains: 60 days.

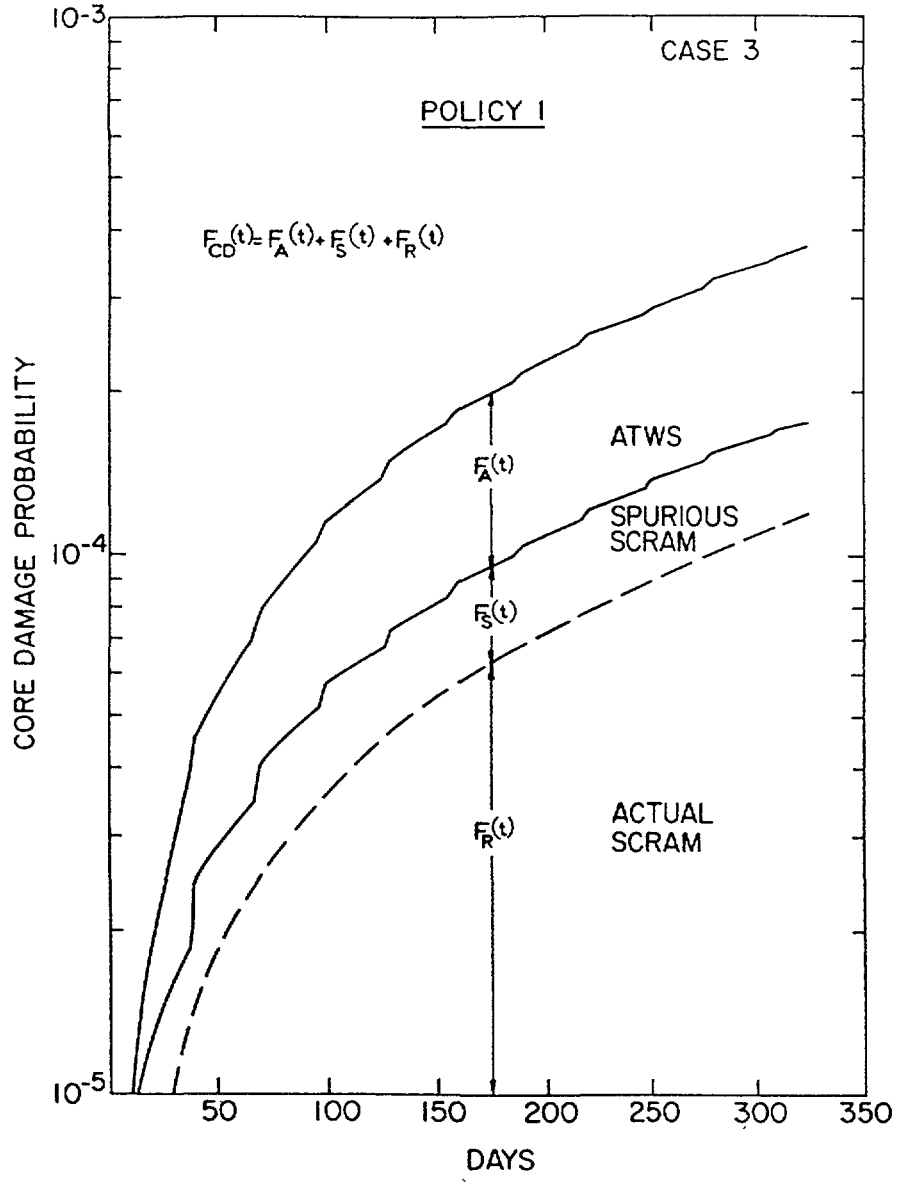


FIG. 9. Probability of core damage as a function of time.

TABLE III. TESTING SCHEDULES (Limiting Conditions of Operation)

Policy	T^{CH} (d)	T^{TR} (d)	τ_0 (h)	τ_1 (h)	τ (h)
1	30	60	1	2	1
2	90	180	6	4	4

T^{CH}, T^{TR}: Test intervals for channels and logic trains, respectively.

τ_0 Allowable bypass time for an analog channel test.

τ_1 Allowable bypass time for an additional analog channel test if one is already tripped.

τ Allowable bypass time for a logic train test.

The core damage probability as a function of time for policy 1 is given in Figure 9. Time t = 0 is the time of startup after a refueling when RPIS has been checked and all components are assumed to be "as new". As mentioned before, the core damage probability $[F_{CD}(t)]$ - that is the probability that core damage will happen any time during the time period t (see Section A.8 in Appendix) - consists of three contributors:

(i) Probability of core damage as a result of a real scram and the subsequent failure of the decay heat removal safety function $[F_R(t)]$. This is the probability that the system will occupy a state in group 5 (see Figure 7). It is equivalent to the contribution of the transient initiators to the probability of core damage calculated in PSAs.

(ii) Probability of core damage as a result of a spurious scram and subsequent failure of the decay heat removal safety function $[F_S(t)]$. This probability is the probability that the system will occupy a state in group 7 (see Figure 7). It corresponds to the contribution of the spurious scrams initiators to the probability of core damage in PSAs.

(iii) Probability of core damage as a result of an ATWS and subsequent failure to mitigate it $[F_A(t)]$. This probability is the probability that the system will occupy a state in group 9 (see Figure 7). It is equivalent to the ATWS contribution in PSAs.

The stiff increases in the probability of core damage as a result of a spurious scram occur at the time of the tests where the chance for tripping a channel or a logic train after exceeding the ABT is substantial.

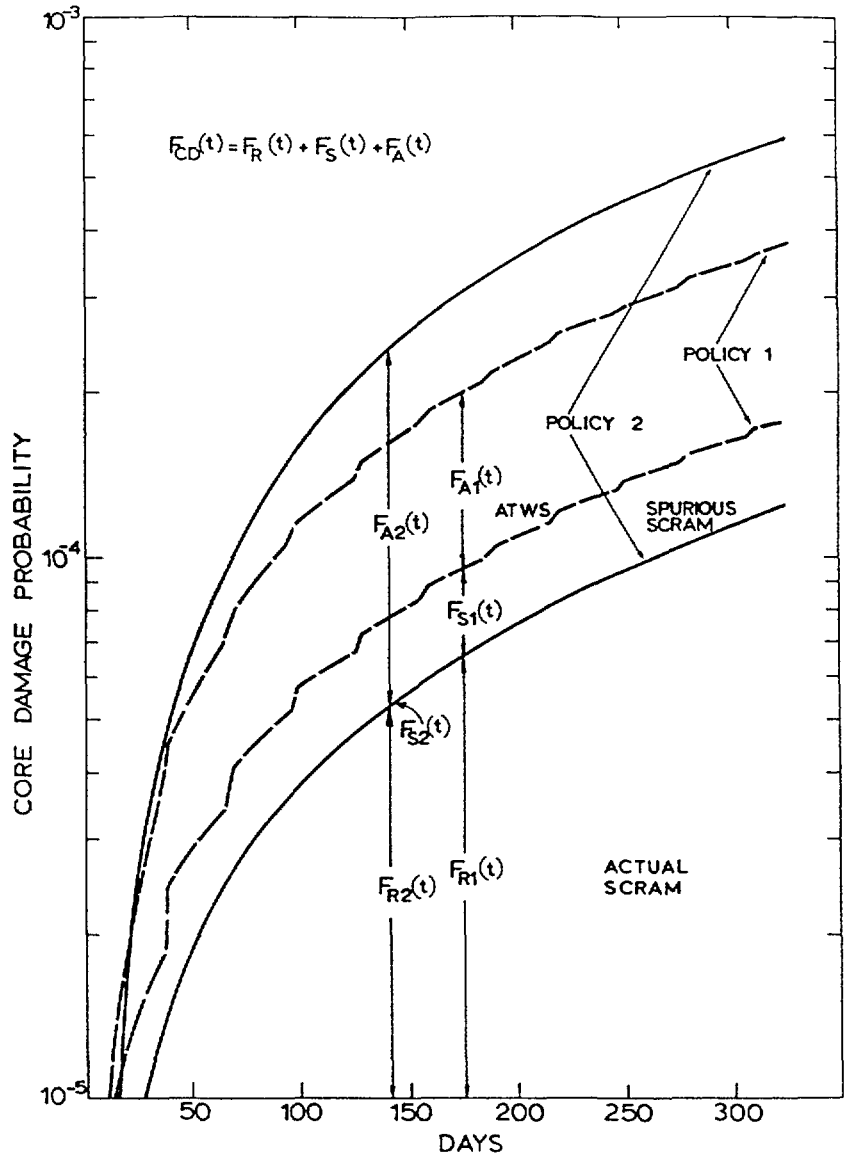


FIG. 10. Probability of core damage and its constituents as a function of time for two TS policies.

The core damage probability as a function of time for policy 2 is given in Figure 10 along with that for policy 1. The probability of core damage as a result of a real scram [$F_R(t)$] is practically the same for the two policies. This is due to the fact that almost all the contribution to this probability comes from transients occurring while the system is in a state of group 1 (see Figure 7). This latter probability is very close to unity for both policies. The probability of core damage as a result of a spurious scram for policy 1 [$F_{S1}(t)$] is small compared to $F_{R1}(t)$ mainly because the conditional probability of core damage given a spurious scram ($P_c^* = 5.2 \times 10^{-7}$) is much smaller than the conditional probability of core damage given a real scram ($P_c = 1.43 \times 10^{-5}$). Policy 2 increases the allowable bypass times and decreases the frequency of testing for both the logic trains and the analog channels. As a result, the probability of spurious scrams and consequently the probability of core damage from spurious scrams becomes negligibly small. This decrease

in core damage probability achieved by policy 2 is, however, more than offset by the increase in the core damage probability as a result of an ATWS [$F_{A2}(t)$]. This latter probability increases for policy 2 because the probability of ATWS increases owing to the increase in the RPS unavailability. It is noteworthy that in this calculation it was assumed that the probability of core damage given an ATWS is equal to unity ($P_0=1$). If $P_0 \neq 1$ the results shown in Figure 10 would be very different as it is extensively discussed later.

Furthermore, the beta factor was set equal to 0.02 for both the channels and the logic trains.

The probability of core damage per year of reactor operation is the probability of core damage at the end of the duty cycle which for the purposes of this report was taken equal to eleven months (330 days).

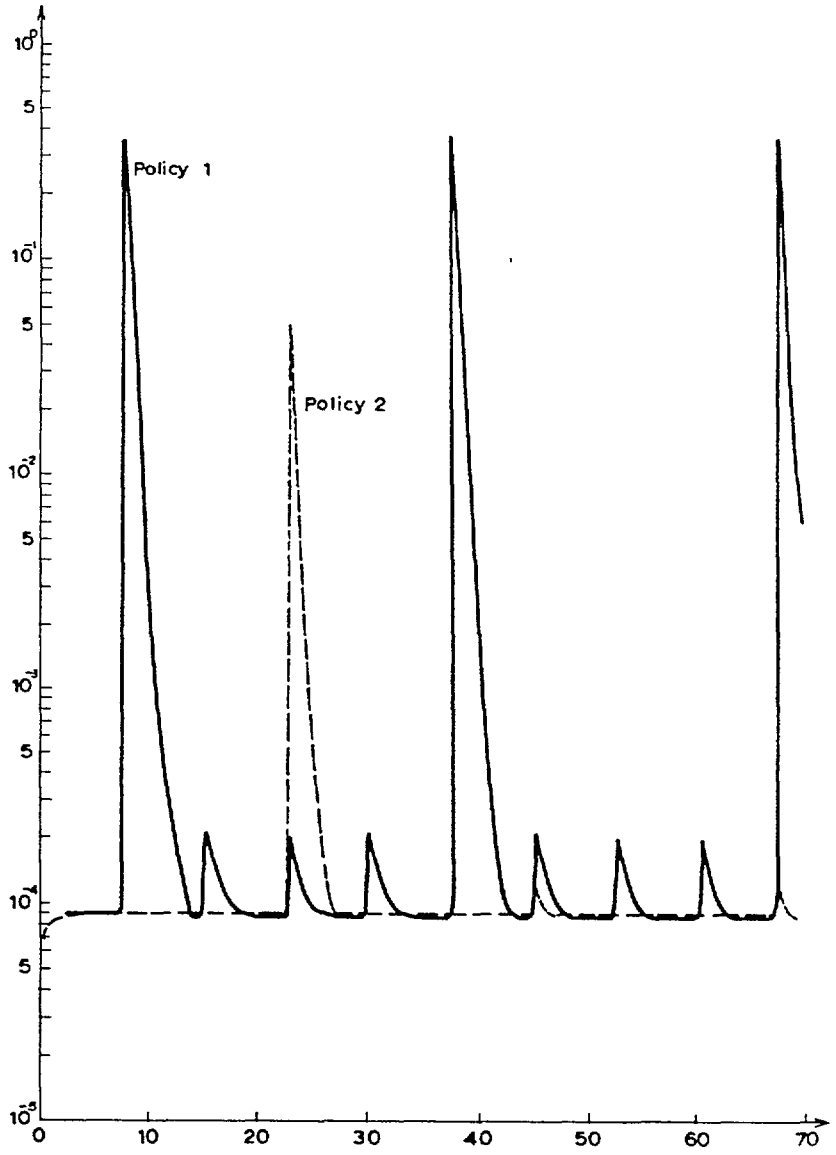


FIG. 11. Probability of the reactor being shut down after a successful response to a spurious scram, as a function of time.

If the total probability of core damage is the only criterion for evaluating the two policies, the one that results in lower core damage probability is the preferred policy. Thus, given the data in section 4.4 and the value of the beta factor and of the conditional probability of core damage given an ATWS (P_o) mentioned above, it follows that policy 1 is preferred to policy 2.

If the alternative policies are also to be evaluated with regard to the resulting reactor downtime, the average reactor downtime for each policy (over the reliability duty cycle) must be evaluated. The probability of the reactor being shutdown as a result of transient (real or spurious) is the probability of the systems being in a state of groups 4, 6 or 8 (see Figure 7). As an example, the time dependent probability of being in a state of group 6 is given in Figure 11. The spikes correspond to the probability of shutdown because of violation of allowable bypass times (ABTs) and are much less pronounced for policy 2 which has greater ABTs. The high spikes for both policies correspond to the testing of logic trains.

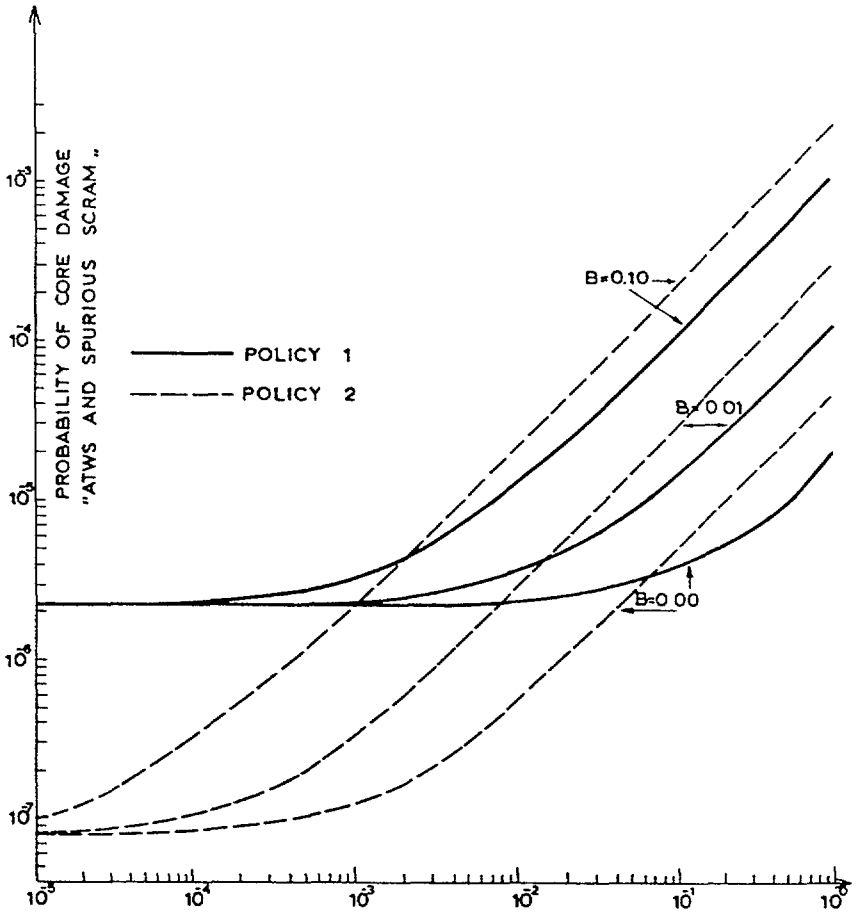


FIG. 12. Contribution of ATWS and spurious scrams to the probability of core damage as a function of P_o (conditional probability of core damage given ATWS) and for different values of the ß-factor.

5.1.2. Sensitivity analysis

Everything else being equal, the policy that results in lower core damage probability depends on the values of the parameters ß and P_o, i.e. on the degree of dependence among the analog channels and among the logic trains and on the conditional probability of core damage given an ATWS. The higher the ß-factor, the higher the contribution of testing in revealing failures and reducing the system unavailability. Hence, we expect policy 2 to be better for lower values of the ß-factors and worse for higher ß-factors. Similarly, since a decrease in testing frequency and an increase in the allowable bypass times increase the unavailability of the system and the probability of an ATWS, the effects of such policy changes are sensitive to the conditional probability of core damage given an ATWS (P_o).

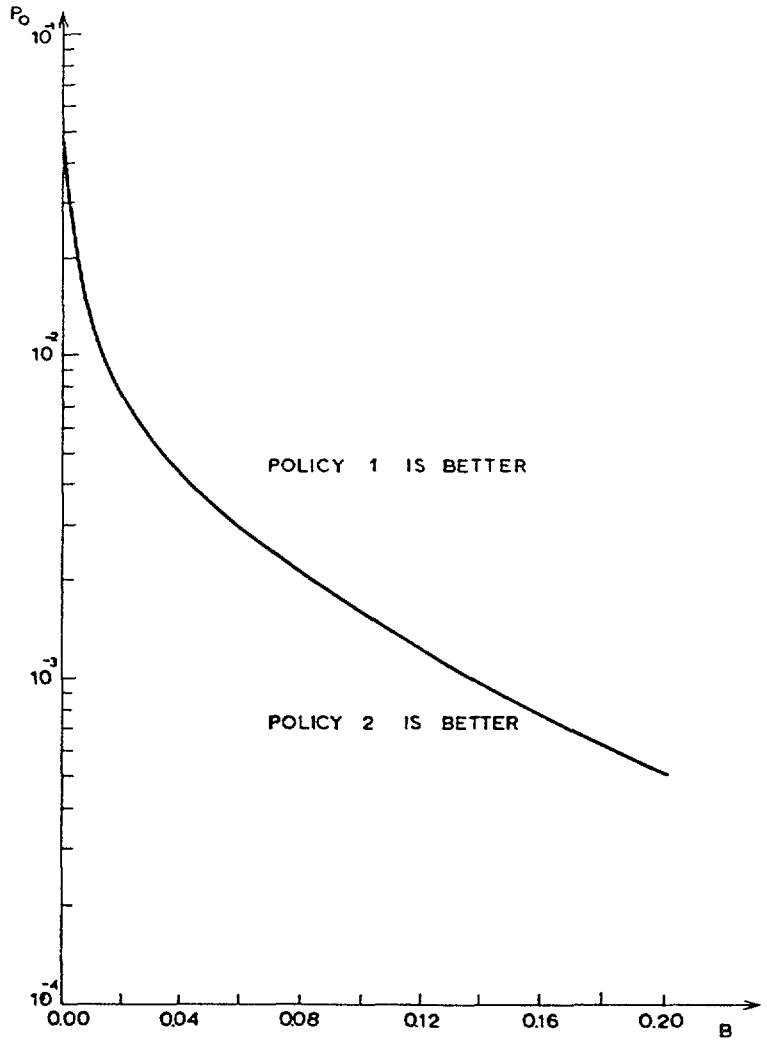


FIG. 13. Definition of better TS policy as a function of the ß-factor and the conditional probability of core damage following an ATWS (P_o).

The effects of the degree of dependence (ß-factor) and the conditional probability of core damage given an ATWS (P_o) on the total probability of core damage for the two policies have been studied in a sensitivity analysis and the results are depicted in Figures 12 and 13. Figure 12 gives the sum of the probability of core damage owing to ATWS and to spurious scrams as a function of the conditional probability of core damage given ATWS (P_o) and for several values of the parameter ß. The "y-axis" in this Figure shows the sum of the ATWS and spurious scram core damage probabilities to achieve better resolution. The probability of core damage from real scrams is practically the same for the two policies and hence, if the above mentioned sum is larger for a given policy the total probability of core damage for that policy is also larger.

Fig. 12 indicates, for example that if ß = 0 (no dependence) policy 2 results in lower core damage probability if P_o is lower than about 10^{-1}. This "cross-over" value of P_o decreases as the value of the ß-factor increases. This fact is also depicted in Figure 13 where the "cross-over" values of P_o have been plotted as a function of the ß-factor. Fig. 13 gives the line that divides the (ß,P_o) plane into two subspaces. Subspace I consists of (ß,P_o) points that imply a lower core damage probability for policy 1 while subspace II consists of (ß,P_o) points that imply the opposite. This division of the (ß,P_o) space depends, of course, on the rest of the parameters of the model given in section 4.4.

Thus, if the conditional probability of core damage given an ATWS is 10^{-2}, then policy 2 is preferred to policy 1 only if the ß-factor is less than 0.01. Otherwise policy 1 is preferred.

5.1.3. Uncertainty analysis

The model presented in Section 4.2 can be also used to quantify the effect of uncertainties that are present because of either population variability or lack of knowledge. The uncertainty calculations were performed by a modified version of the code MARELA.

The parameters of the model were considered random variables distributed according to lognormal probability density functions with the characteristics given in Table IV. It is noteworthy that "state of knowledge" dependence [24] was incorporated in the analysis. That is, components of the same type, at the same plant, are assumed to have the same failure rate. The probability density functions and the cumulative distribution functions of the various quantities of interest have been calculated for the two policies under consideration. The results are tabulated in Table V and plotted in Figs. 14-17.

The main conclusions of the point calculations are supported by the uncertainty calculations. Policy 2 results in a higher contribution to the core damage probability from an ATWS and a lower contribution from spurious scrams than policy 1. The increase in the contribution from the ATWS, however, more than outweighs the decrease from the spurious scrams. In particular, policy 1 stochastically dominates policy 2 on the probability of an ATWS. Stochastic dominance means that the likelihood that the probability of an ATWS will be less than a given value X for policy 1 is always higher than the corresponding likelihood for

TABLE IV. INPUT DATA FOR UNCERTAINTY ANALYSIS

Variable	Mean	Median	EF[1]	Source
X(1) β^{TP}	0.05	1.8772(-2)	10	Ref. [20]
X(2) β^{CH}	0.05	1.8772(-2)	10	Ref. [20]
X(3) λ^{TR}	2.52(-6)/h	1.5615(-6)	5	Refs [16,17,29]
X(4) λ^{CH}	3.51(-6)/h	2.1749(-6)	5	"
X(5) λ_s^{TR}	3.28(-6)/h	2.0324(-6)	5	"
X(6) λ_s^{CH}	6.16(-6)/h	3.8170(-6)	5	"
X(7) $1/r_A$	27.8 h	19.4907	4	Private comm. with Jansen of [3]
X(8) $1/r_R$	13.7 h	9.6051	4	"
X(9) P_c	1.43(-5)	5.3688(-6)	10	Refs [14,18,20]
X(10) P_c*	5.21(-7)	1.9561(-7)	10	"
X(11) P_o	6.42(-2)	1.6560(-2)	15	"
X(12) λ_o	7.78/year	7.1191/year [8.1382(-4)/h]	2	Refs [13,19,20]
X(13) $1/\mu_{31}^{CH}$	16 h	12.8017	3	Ref. [3,20]
X(14) $1/\mu_1^{TR}$	2 h	1.2393	5	"
X(15) $1/\mu_2^{TR}$	8 h	4.9571	5	"
X(16) $1/\mu_1^{CH}$	2 h	1.2393	5	"
X(17) $1/\mu_2^{CH}$	8 h	4.9571	5	"
X(18) P_1^{TR}	7.99(-3)	3.00(-3)	10	Refs [20, 21,22,23]
X(19) P_2^{TR}	7.99(-3)	3.00(-3)	10	"
X(20) P_1^{CH}	7.99(-3)	3.00(-3)	10	"
X(21) P_2^{CH}	1.82(-2)	6.84(-3)	10	"

[1] EF stands for error factor in lognormal distributions and is defined by the ratio 95th percentile/50th percentile.

TABLE V. CUMULATIVE DISTRIBUTIONS FOR: CORE DAMAGE PROBABILITY *PER REACTOR YEAR OWING TO REAL SCRAMS, SPURIOUS SCRAMS,* PROBABILITY OF ATWS, TOTAL CORE DAMAGE PROBABILITY AND REACTOR UNAVAILABILITY

Policy	5th Percentile	Median	95th Percentile	Mean
1.	**Core Damage Probability Owing to Real Scrams (per reactor year)**			
1	3.24(-6)	3.22(-5)	4.37(-4)	1.04(-4)
2	3.42(-6)	3.35(-5)	4.42(-4)	1.06(-4)
2.	**Core Damage Probability Owing to Spurious Scrams (per reactor year)**			
1	2.85(-8)	7.05(-7)	9.75(-6)	2.39(-6)
2	1.41(-9)	4.69(-8)	1.07(-6)	2.83(-7)
3.	**Probability of ATWS (per reactor year)[1]**			
1	2.40(-4)	1.96(-4)	1.54(-3)	4.29(-4)
2	5.66(-5)	4.67(-4)	3.53(-3)	9.94(-4)
4.	**Total Core Damage Probability (per reactor year)**			
1	6.68(-6)	4.86(-5)	4.95(-4)	1.31(-4)
2	7.20(-6)	5.93(-5)	6.06(-4)	1.67(-4)
5.	**Reactor Unavailability (per reactor year)**			
1.	1.01(-2)	2.75(-2)	8.17(-2)	3.50(-2)
2.	9.04(-3)	2.40(-2)	7.68(-2)	3.11(-2)

[1]To obtain the contribution of ATWS to the probability of core damage, the ATWS probability must be multiplied by the conditional probability of core damage given ATWS (P_0).

policy 2 - that is, for all possible values of X (see Fig. 15). Policy 2 stochastically dominates policy 1 on the contribution to the core damage probability from spurious scrams (see Fig. 14). Policy 1 stochastically dominates policy 2 on the total probability of core damage per year of reactor operation (see Fig. 16). If core damage probability is the only attribute of performance, policy 1 is preferred to policy 2.

The results of the uncertainty analysis for the average reactor shutdown time are tabulated in Table V and depicted in Figure 17. Policy 2 stochastically dominates (although not by much) policy 1 on the average reactor downtime per year of reactor operation.

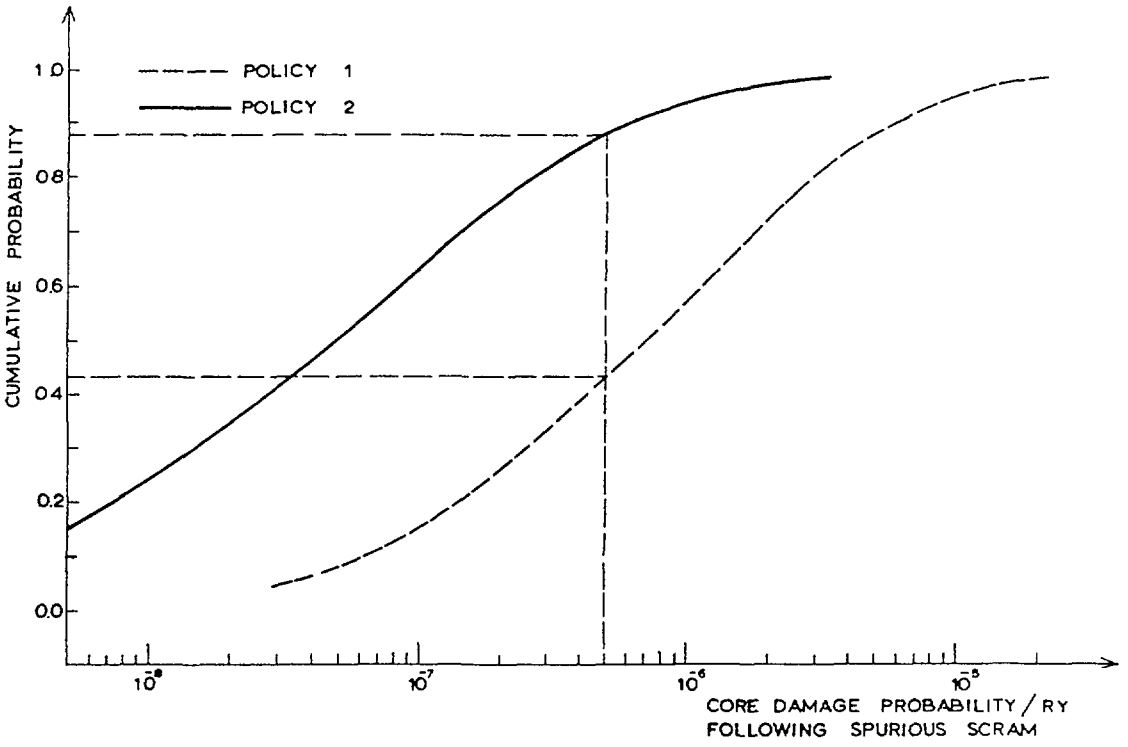


FIG. 14. Cumulative distribution functions for the probability of core damage following a spurious scram per year of reactor operation.

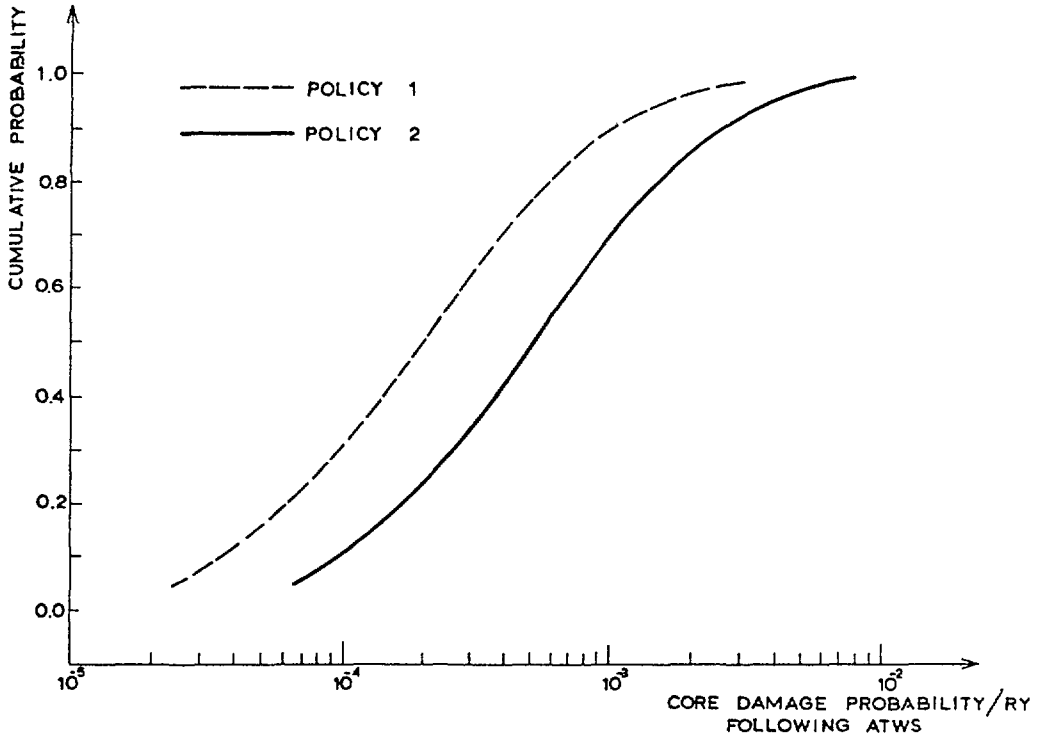


FIG. 15. Cumulative distribution functions for the probability of ATWS per year of reactor operation.

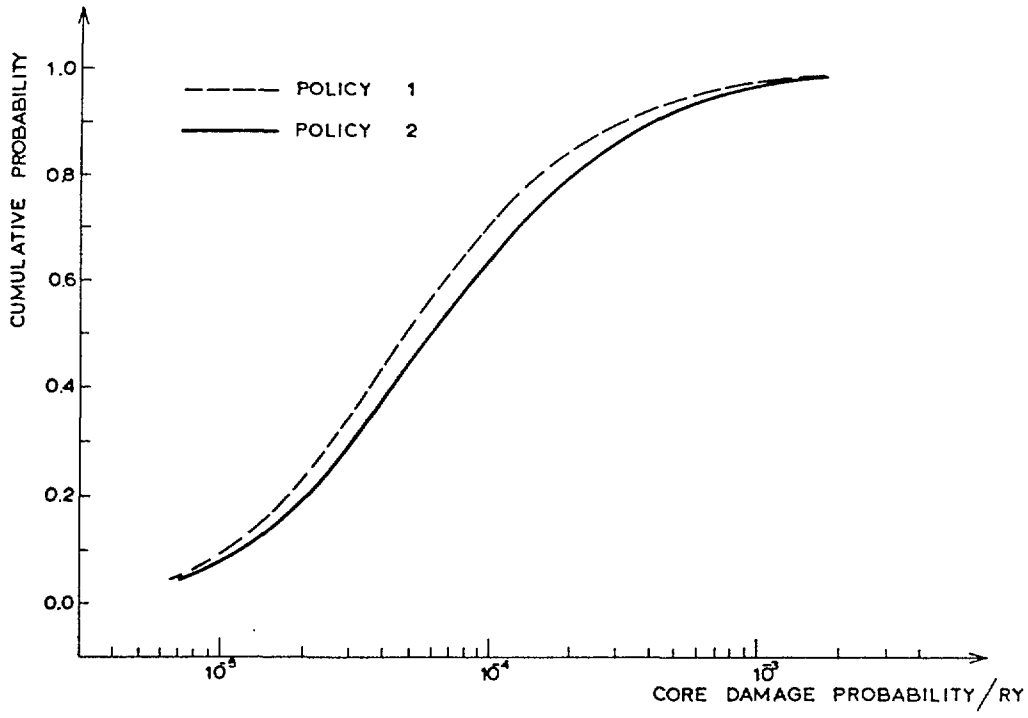


FIG. 16. Cumulative distribution functions for total core damage probability per year of reactor operation.

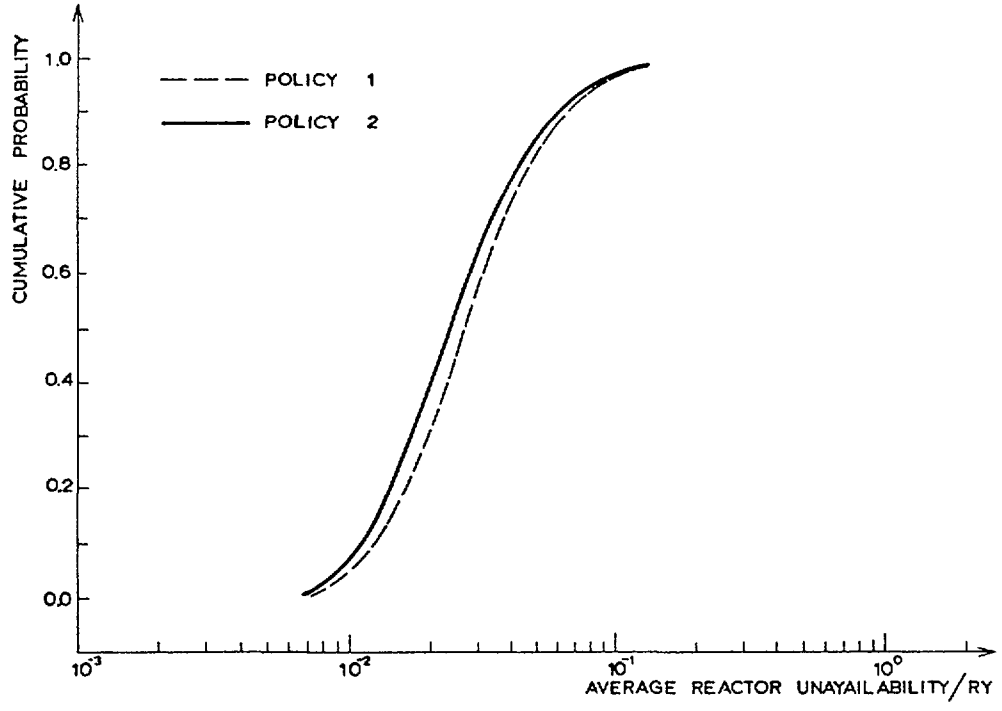


FIG. 17. Cumulative distribution functions for reactor unavailability (averaged per year of reactor operation).

5.2. COMPARISON OF SEVERAL TS POLICIES

As mentioned in earlier sections, an TS policy consists of the period of testing of analog channels (T^{CH}), the period of testing logic trains (T^{TR}), the allowable time in "bypass" for an analog channel if no other channel is tripped (τ_0), the allowable time in "bypass" for an analog channel if another channel is tripped (τ_1), and the allowable time in "bypass" for a logic train (τ). An uniformly staggered testing scheme [4] of the analog channels and the logic trains has been assumed for both policies. In general, one would like to determine the five values of these parameters that optimize the chosen risk and/or economic attributes. Such a general analysis is, however, outside the scope of this work. Instead, the main characteristics of the dependence of the attributes on the parameters of the TS policy are demonstrated by means of a sensitivity study.

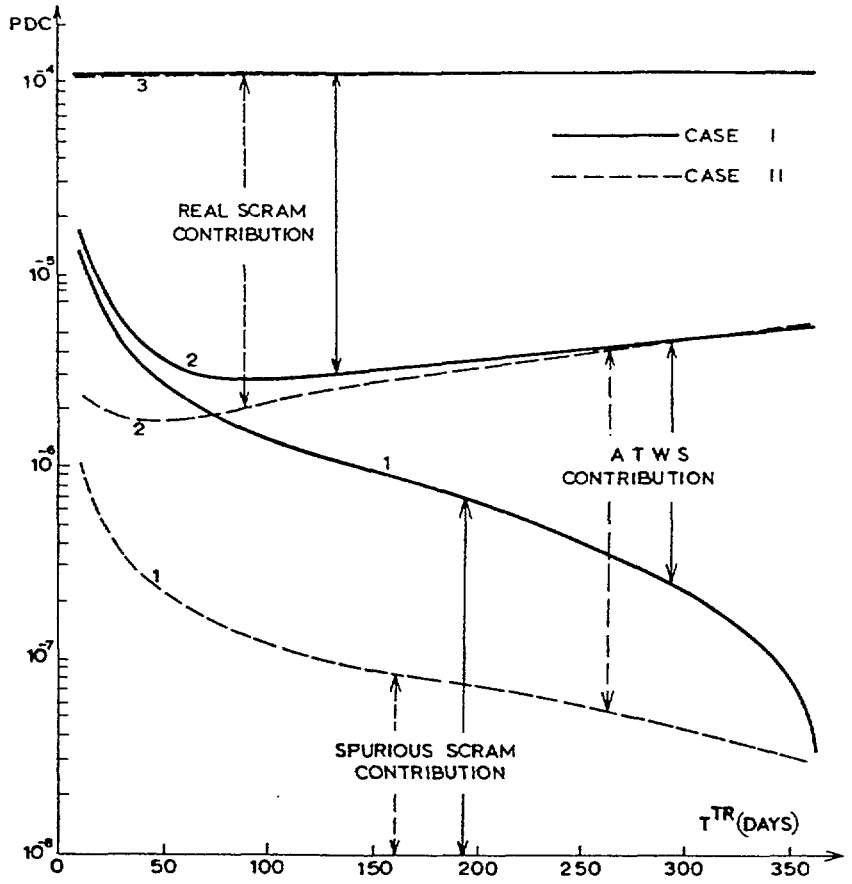


FIG. 18. Total core damage probability as a function of the logic train testing period. $\beta^{TR} = \beta^{CH} = 0$, T^{CH}=30 d, $P_o = 6.42 \times 10^{-2}$.

CASE I: τ = 1 h, τ_0 = 1 h, τ_1 = 2 h

CASE II: τ = 4 h, τ_0 = 6 h, τ_1 = 4 h

Two attributes have been chosen for evaluating the various TS policies: the probability of reactor core damage per year of operation and the expected down time of the reactor. The sensitivity studies were performed for two limiting cases of dependence, namely, no dependence ($\beta^{CH} = \beta^{TR} = 0$) and high dependence ($\beta^{CH} = \beta^{TR} = 0.10$). In the case of no dependence the system behavior is dominated by the two logic trains since the analog channels exhibit a high degree of redundancy (2-out-of-4). In the case of high dependence the role of the analog channels becomes important. The results of the sensitivity studies are shown in Figs. 18 through 21.

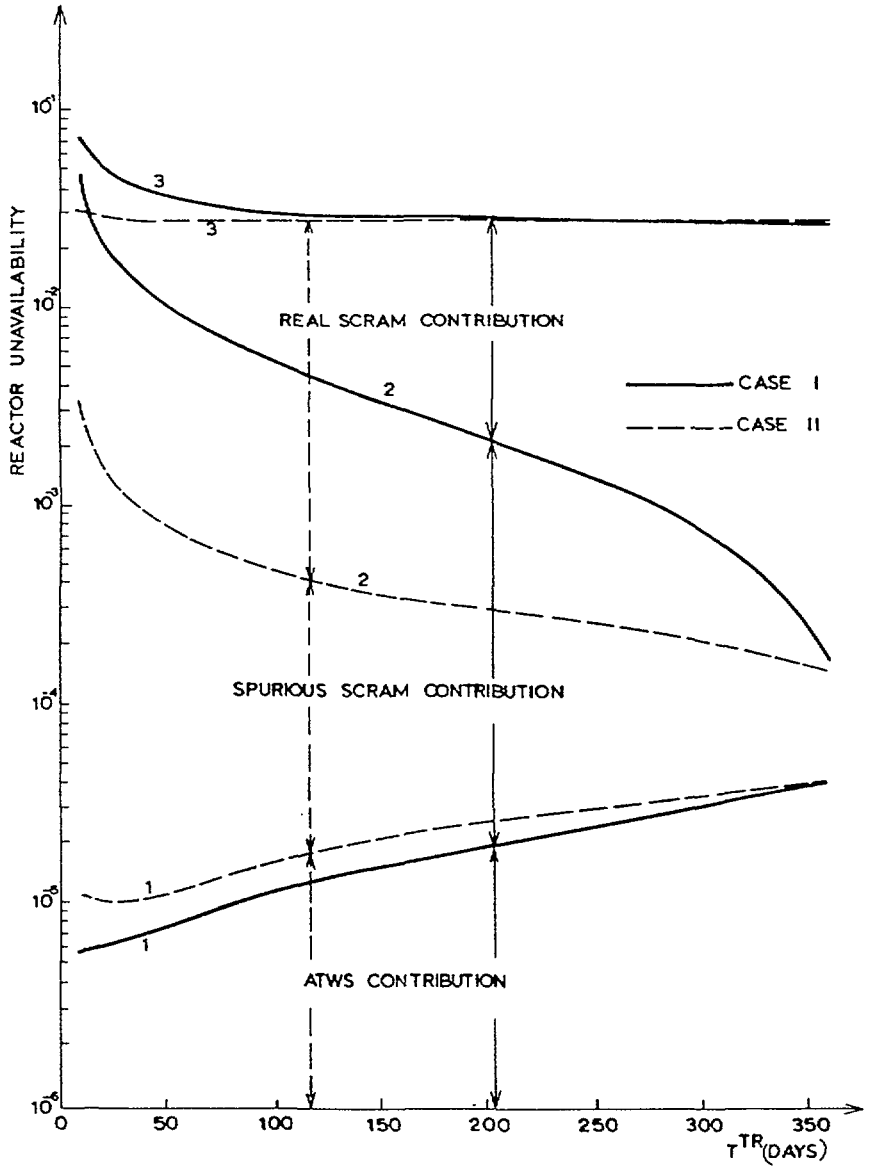


FIG. 19. Reactor unavailability as a function of the logic train testing period. $\beta^{TR} = \beta^{CH} = 0$, T^{CH}=30 d, $P_o = 6.42 \times 10^{-2}$.

CASE I: $\tau = 1$ h, $\tau_0 = 1$ h, $\tau_1 = 2$ h

CASE II: $\tau = 4$ h, $\tau_0 = 6$ h, $\tau_1 = 4$ h

Fig. 18 presents the probability of core damage per year of reactor operation (PCD) and its three constituents (i.e., core damage from spurious scram, from ATWS, and from real scram initiators) as a function of the period of testing the logic trains, when there is no dependence between trains or channels ($\beta^{CH} = \beta^{TR} = 0$). Two cases are shown: case I for short ABTs (i.e. $\tau = 1$ h, $\tau_0 = 1$ h, and $\tau_1 = 2$ h); case II for long ABT's (i.e. $\tau = 4$ h, $\tau_0 = 6$ h, $\tau_1 = 4$ h). The curves labeled I in Fig. 18 show the variation of the probability of core damage as a result of spurious scrams. This contribution decreases as the testing period for the logic trains increases. Spurious scrams are almost totally due to the exceeding of ABT for the logic train testing (τ). As T^{TR} increases, fewer tests are performed on the logic trains and the probability of spurious scrams decreases with a corresponding decrease of the probability of core damage from such spurious scrams. As expected the spurious scram contribution is smaller for case II (large ABTs).

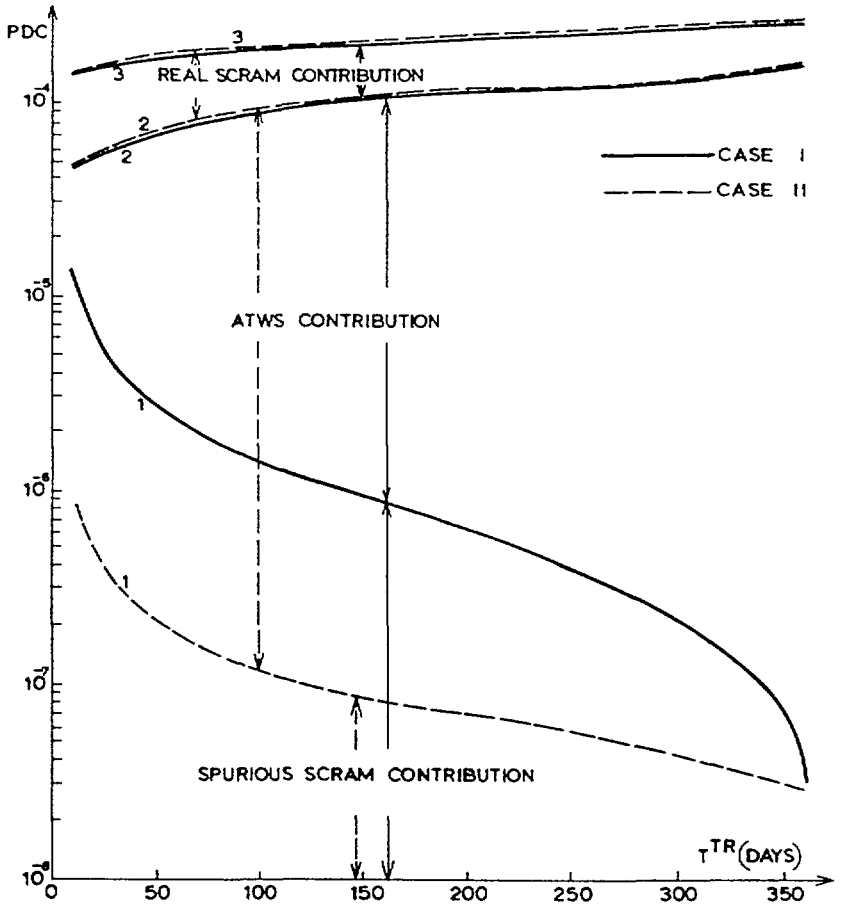


FIG. 20. Total core damage probability as a function of the logic train testing period. $\beta^{TR} = \beta^{CH} = 0.10$, $T^{CH} = 30$ d, $P_o = 6.42 \times 10^{-2}$.

CASE I: $\tau = 1$ h, $\tau_0 = 1$ h, $\tau_1 = 2$ h

CASE II: $\tau = 4$ h, $\tau_0 = 6$ h, $\tau_1 = 4$ h

The ATWS probability and hence the corresponding contribution to the probability of core damage increases with T^{TR}, since higher logic train testing period means higher RPS unavailability. The combined effect of the spurious scram and ATWS contributions on the PCD is given by the curves labeled 2 in Fig. 18. Thus, the contribution to the PCD from spurious scram and ATWS initially decreases with T^{TR} but then it increases again. The ATWS contribution is larger for case II. When the contribution of the "real scram" core damage probability is added to the other two contributions, the total probability of core damage remains practically constant for all values of T^{TR} as it is shown by the curves labeled 3 in Fig. 18. The probability of core damage from a real scram depends on the time the reactor is up and operating and hence susceptible

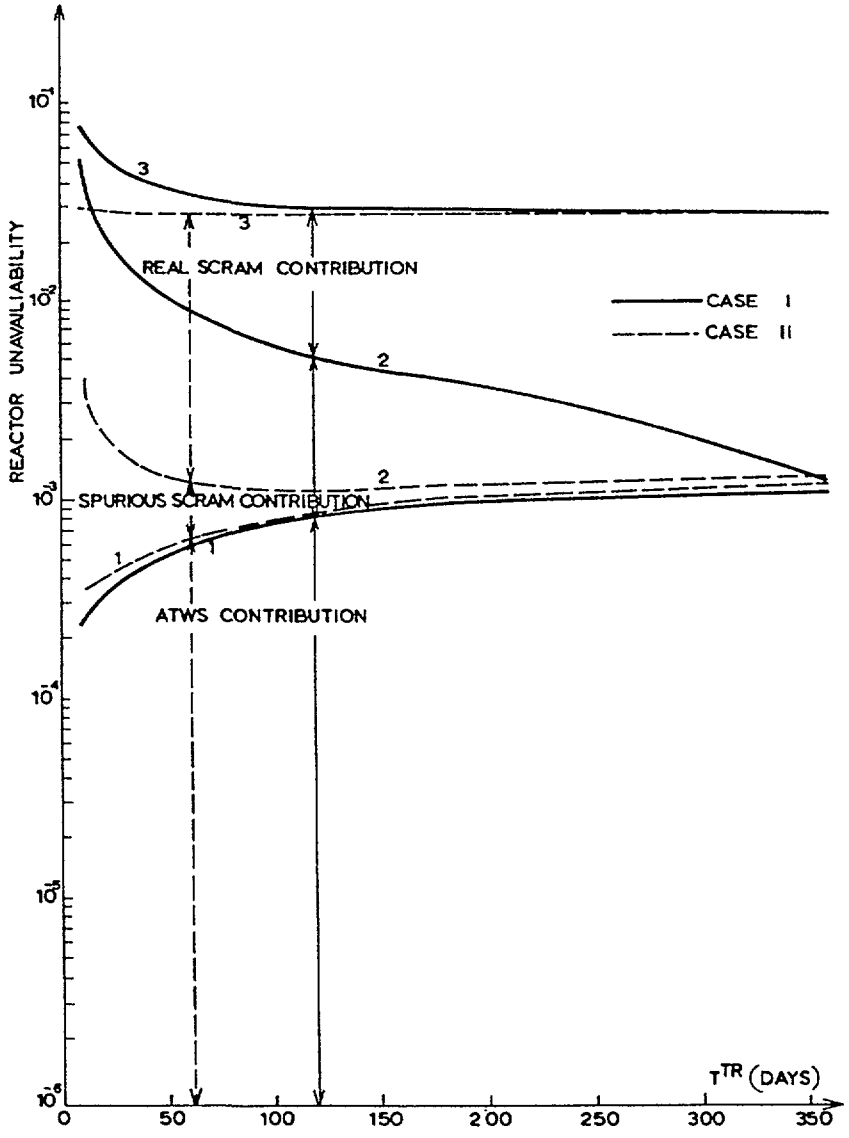


FIG. 21. Reactor unavailability as a function of the logic trains testing period. $\beta^{TR} = \beta^{CH} = 0.10$, T^{CH}=30 d, $P_o = 6.42 \times 10^{-2}$.

CASE I: $\tau = 1$ h, $\tau_0 = 1$ h, $\tau_1 = 2$ h

CASE II: $\tau = 4$ h, $\tau_0 = 6$ h, $\tau_1 = 4$ h

to a real challenge. This time increases as T^{TR} increases since the probability of spurious scrams and the associated reactor shutdown time decrease. The initial increase of the reactor-up time results in an increase of the probability of real scram and of the corresponding contribution to the PCD (see Fig. 18). As T^{TR} continues to increase the probability of an ATWS increases. This increase in ATWS probability compensates for the decrease of the spurious scram contribution both to the PCD and the reactor shutdown time. As a result, the reactor-up time decreases along with the probability of a real scram and the associated contribution to the PCD.

The variation of the reactor unavailability (per year of reactor operation) and its three constituents (i.e., downtime following a successful response to real scram, ATWS, and spurious scram) as a function of T^{TR} is given in Fig. 19. The unavailability decreases with T^{TR} because of the dominating effect of the corresponding decrease of the down-time from spurious scrams. The same qualitative behavior is observed for both small ABTs (case I) and larger ABTs (case II). The total unavailability for case II is, however, lower, because of the substantial decrease of the spurious scram contribution.

The results of the sensitivity analysis for the case of no dependence ($\beta^{TR} = \beta^{CH} = 0$) depicted in Figs. 18 and 19 indicate that if total PCD and reactor unavailability were the only criteria for assessing the ABTs and the period of testing for logic trains, then large ABTs and testing periods are favored since they do not affect the PCD while they do decrease the reactor unavailability. It should be noted, however, that this conclusion might not hold if other risk criteria are considered (e.g. offsite health effects). In this case an increase in the period of testing or in the ABTs while it does not change the total PCD it does affect the relative contribution of various accident sequences. An ATWS core melt accident sequence, for example, could be more severe than an equally probable spurious-scram core melt sequence, in terms of offsite consequences.

Figs. 20 and 21 correspond to Figs. 18 and 19, respectively, when there is dependence among the logic trains and among the analog channels ($\beta^{TR} = \beta^{CH} = 0.10$). The total PCD does increase with T^{TR} and the ATWS contribution dominates the PCD changes (see Fig. 20). This was expected since the incorporation of dependence among the logic trains increases the RPS unavailability and hence renders the ATWS probability much more sensitive to the frequency of the logic train testing. The reactor unavailability (per year of reactor operation) on the other hand takes practically the same values as for the case of no dependence. This is due to the fact that the incorporation of dependence affects mainly the reactor shutdown following a successful response of an ATWS. The latter, however, represents only a small contribution to the total unavailability.

5.3. SUMMARY AND CONCLUSIONS

The purpose of this case study has been to present a methodology and its application for the probabilistic evaluation of alternative plant technical specifications regarding system surveillance and

out-of-service times. The methodology was based on a Markov model and applied to the reactor protection system of a 4 loop RESAR-3S PWR type nuclear power plant.

The two attributes used in the evaluation of alternate sets of technical specifications for the RPS are the probability of core damage per year of reactor operation (PCD) and the expected reactor unavailability. A Markov model was employed that allows for the modeling of state dependence and other dynamic effects like the renewal of the system after each successful challenge. These modeling capabilities result in greater realism in the calculation of the two attributes mentioned above. Furthermore, the model includes multiple components and system states that permit the calculation of the three contributors to the PCD: i.e., probability of core damage following a real scram, probability of core damage following a spurious scram, and probability of core damage following a failure of the RPS to scram the reactor. Each technical specification affects a different contributor to the PCD and thus, the proposed model offers, in addition to the greater realism in the calculation of the PCD, a better insight into the effects of specific changes in the technical specifications.

The general trends identified in the calculations performed in this study are as follows:

(i) The probability of core damage is mainly affected by the unavailability of the RPS and consequently by the probability of an ATWS. The reactor unavailability, however, is mainly affected by the probability of spurious scrams. This behavior is due to the fact that the conditional probability of core damage given an ATWS is much higher than the conditional probability of core damage given a spurious scram.

(ii) The Allowable Bypass Times (ABTs) for the analog channels and the logic trains affect mainly the probability of spurious scrams. In general, an increase in the ABTs results in a decrease in the probability of a spurious scram and in a much smaller increase in the probability of an ATWS. The conditional probability of core damage given a spurious scram is, however, much smaller than the conditional probability of core damage given an ATWS. Consequently, an increase of the ABTs results in either no increase or small net increase of the probability of core damage, depending on the level of dependence among analog channels and among logic trains. On the other hand, the significant decrease in the probability of spurious scrams corresponds to a significant decrease in the reactor down time. Given the very small increase in the PCD and the significant decrease in the expected reactor down time obtained in this study, an increase in the ABTs might be justified if these two are the only attributes used to evaluate the effect of changing TS.

(iii) The frequency of testing of the analog channel and the logic trains affects the probability of core damage more than it affects the expected reactor downtime and in a way that depends on the level of dependence among the analog channels and among the logic trains (dependent failures). At low levels of dependence low frequencies of testing are justified, while at high levels of dependence high frequencies result in lower probabilities of core damage.

6. PEER REVIEW

Most of the results presented in this case study were generated as part of work performed by the group of Risk Evaluation of the Department of Nuclear Energy at Brookhaven National Laboratory for the US Nuclear Regulatory Commission under contract FIN A-3729.

The risk evaluation group was providing technical support to the Reliability and Risk Assessment Branch of the Office of Nuclear Reactor Regulations to be used as an input on the USNRC response to a request by the Westinghouse Owner's Group to revise the Technical Specifications. Consequently, the methods and results of this work have been subject to the BNL internal quality assurance procedures, reviewed and commented upon by USNRC project managers and Westinghouse analysts. Furthermore, Westinghouse requested and received a copy of the computer code used in this work for further use. Some of the results have been also presented at the International Meeting on Probabilistic Safety Methods and Applications, in San Francisco, California, February 1985.

Appendix

ELEMENTS OF MARKOVIAN RELIABILITY ANALYSIS

A.1. INTRODUCTION

This Appendix is based on Ref. [11] and presents the basic principles of Markovian reliability analysis and an annotated literature review.

Reliability analyses begin with the establishment of logic diagrams such as event trees, fault trees and cause-consequence graphs. These diagrams are essential for understanding qualitatively the operating and failure modes of the system and for identifying the operating and failed states.

When the stochastic characteristics of the components of the system depend on the state of the system, the logic diagrams must be complemented by special techniques for the quantitative evaluation of the various reliability measures. In particular, when these characteristics depend only on each pair of initial and final states of the system, the technique best suited for evaluation of reliability is Markovian analysis.

Examples of particular circumstances that generate dependence on the state of the system are:

System with repairable components. Repair of a component may be possible only if the system is in an operating state and not if it is in a failed state.

System with different repair policies. Repair may depend on the number of repairmen available, or repair of certain components may not be possible while others are operating. In addition, several repair policies may be possible, such as repair all failed components before resuming operation or repair only those components that are necessary to resume operation.

Operability of standby systems. Response to a challenge may depend on the state of the standby system. For example, for some states the standby system may respond to some challenges but not to others. Furthermore, a successful response to a challenge may reveal partial failures which if repaired could make a positive contribution to reliability.

Standby redundancy. Standby failure and repair rates are in most cases different than the corresponding online rates.

Common extreme environment. The failure and repair rates of components change significantly under extreme environments.

Components sharing common loads. If a load is shared by several components, the failure rates of the components depend on the number of the components sharing the load.

Common cause or common mode failures. Two or more components of a system may fail together because of an existing commonality. Furthermore, the failure of one component might cause that of others.

The capabilities of Markovian models in reliability analyses have been recognized and extensively used. A brief review of Markovian processes and simple numerical examples of Markovian reliability analysis are given in sections two through eight. A survey of the relevant literature is given in Section A.9.

A.2. MARKOVIAN RELIABILITY ANALYSIS

A.2.1. Markov processes - Definitions

A discrete-state, continuous-time random process describes the stochastic behaviour of a system that can be in any of a finite number (z) of discrete states and that changes its state randomly as a function of time. A change of state - state transition - can occur at any instant of time.

A discrete-state, continuous-time Markov process is a random process such that the probability that the system will perform a state transition from state i to state j at any time depends only on the initial state i and the final state j of the transition.

If $\pi_i(t)$ denotes the probability that the system is in state i at time t, and $\underline{\pi}(t)$ the $1 \times z$ row vector with elements $\pi_i(t)$, for i = 1,2,...z, namely

$$\underline{\pi}(t) = [\pi_1(t),...,\pi_i(t),...,\pi_z(t)], \tag{2.1}$$

then it can be shown that $\underline{\pi}(t)$ satisfies the state evolution equation given by the relation [7]

$$\dot{\underline{\pi}} \equiv \frac{d\,\underline{\pi}(t)}{dt} = \underline{\pi}(t) \cdot \underline{A} \tag{2.2}$$

where $\underline{A}$ is a $z \times z$ matrix with elements a_{ij} such that:

$a_{ij}dt$ = the probability that the system will transit to state j during the interval between t and t+dt given that it is in state i at time t.

Vector $\underline{\pi}(t)$ is called the state-probability vector with elements the state probabilities $\pi_i(t)$'s. Matrix $\underline{A}$ is called the transition-rate matrix with elements the transition rates a_{ij}'s.

Each non-transition rate a_{ij}, for i=1,2,...,z, satisfies the relation

$$a_{ii} = -\sum_{\substack{j=1 \\ j\neq i}}^{z} a_{ij} \quad or \quad \sum_{j=1}^{z} a_{ij} = 0 \tag{2.3}$$

Indeed, the sum of the state probabilities

$$\sum_{i=1}^{z} \pi_i(t) = 1 \tag{2.4}$$

for all values of the $\pi_i(t)$'s and, therefore,

$$\frac{d}{dt} \sum_{i=1}^{z} \pi_i(t) = 0 \tag{2.5}$$

Using Eq. 2.2 in Eq. 2.5 we find

$$\sum_{i=1}^{z} \sum_{j=1}^{z} \pi_i(t) a_{ij} = \sum_{i=1}^{z} \pi_i(t) \sum_{j=1}^{z} a_{ij} = 0 \tag{2.6}$$

Equation 2.6 must hold for all values of the $\pi_i(t)$'s and this, in turn, can be true if and only if Eq. 2.3 is satisfied.

The solution of Eq. 2.2 is given by the relation

$$\underline{\pi}(t) = \underline{\pi}(0) \exp(\underline{A}\, t) \tag{2.7}$$

where $\underline{\pi}(0)$ is the value of the state probability vector at time t = 0.

A discrete-state, discrete-time Markov process is a random process such that:

(a) state transitions occur at discrete times t_n, where $t_n = t_{n-1} + \Delta t(n)$ or, with t(n) = constant, $t_n = t_0 + n\Delta t$; and

(b) the probability that the system will perform a state transition from state i to state j at time t_n depends only on the states i and j of the transition.

It can be shown that the 1 × z state probability vector $\underline{\pi}(n)$ obeys the relation

$$\underline{\pi}(n+1) = \underline{\pi}(n) \cdot \underline{P}(n) \tag{2.8}$$

where the z × z transition probability matrix $\underline{P}(n)$ has as elements the transition probabilities $p_{ij}(n)$, for i,j = 1,2...,z.

A.2.2. State-transition

A discrete-state Markov process is customarily represented by a state-transition diagram such as sketched in Fig. A.2.1. The arrows in the diagram correspond to the possible transitions of the system and are assigned the corresponding transition rates. The diagram in Fig. A.2.1 depicts a system that can transit from state 1 to state 2, with a rate a_{12}, from state 1 to state 3 with a rate a_{13}, and from state 2 to state 1 with a rate a_{21}. Transitions from state 2 to state 3 and from state 3 to states 1 and 2 are not possible. The transition-rate matrix for the process shown in Fig. A.2.1 has the form:

$$\underline{A} = \begin{bmatrix} a_{21} & a_{12} & a_{13} \\ a_{21} & a_{22} & 0 \\ 0 & 0 & a_{33} \end{bmatrix} \tag{2.9}$$

where $a_{11} = -(a_{12}+a_{13})$, $a_{22}=-a_{21}$, $a_{33}=0$.

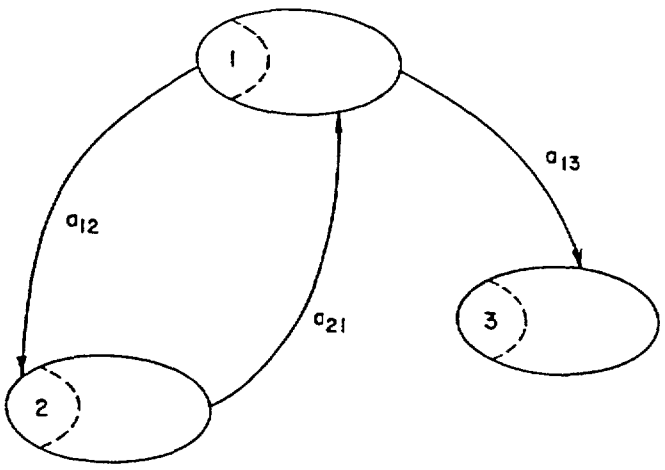


FIG. A.2.1. Example of a state transition diagram.

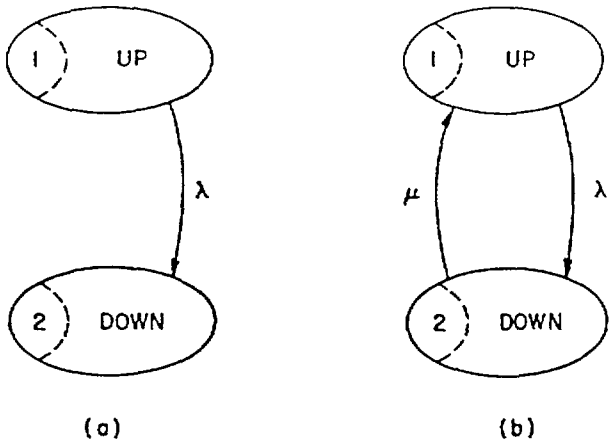


FIG. A. 2.2. State transition diagrams for a two-state system.

A.2.3. One component system

We will consider a system that can be in either of two states: (a) state 1, the system is operating; and (b) state 2, the system has failed.

If the system is non-repairable, a transition from state 2 back to state 1 is not possible. Then the state-transition diagram is as shown in Fig. A.2.2(a). The transition rate a_{12} is the failure rate λ of the system. If the system is repairable, a transition from state 2 back to state 1 is possible. Then the state transition diagram is as shown in Fig. A.2.2(b). The transition rate a_{21} is the repair rate μ of the system.

The transition rate matrix and the state evolution equation for the repairable system are

$$A = \begin{bmatrix} -\lambda & \lambda \\ \mu & -\mu \end{bmatrix} \tag{2.10}$$

and

$$[\dot{\pi}_1(t),\ \dot{\pi}_2(t)] = [\pi_1(t),\ \pi_2(t)] \cdot \begin{bmatrix} -\lambda & \lambda \\ \mu & -\mu \end{bmatrix} \tag{2.11}$$

respectively.

If at time zero the system is in state 1, i.e., $\underline{\pi}(0) = [1,0]$, the solution of Eq. 2.11 is

$$\pi_1(t) = \frac{\mu}{\mu+\lambda} + \frac{\lambda}{\mu+\lambda} \exp[-(\mu + \lambda)t] \tag{2.12a}$$

$$\pi_2(t) = \frac{\lambda}{\mu+\lambda} \{1 - \exp[-(\mu + \lambda)t]\} \tag{2.12b}$$

If the system is non repairable (μ = 0), the solution reduces to

$$\pi_1(t) = \exp(-\lambda t) \tag{2.13a}$$

$$\pi_2(t) = 1 - \exp(-\lambda t) \tag{2.13b}$$

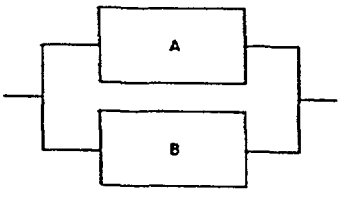
In the repairable case, $\pi_1(t)$ (Eq. 2.12a) gives the probability that the system is operating at time t though it may have failed and been repaired several times in the time interval (0,t). This probability is the point availability, A(t), at time t. The complementary probability $\pi_2(t)$ (Eq. 2.12b) is the point unavailability, U(t), at time t.

In the nonrepairable case, the system can leave state 1 but cannot return to it. Accordingly, the probability $\pi_1(t)$ (Eq. 2.13a) that the system be in state 1 at time t gives the probability that the system be operating continuously from time 0 up to time t. This probability is the reliability, R(t), of the system. The complementary probability $\pi_2(t)$ (Eq. 2.13b) - the probability that the system occupies state 2 at time t - gives the probability that the system has failed between 0 and t. It is the failure probability, F(t), of the system.

A.2.4. Two-component systems

We will consider a system consisting of two components A and B connected in parallel (Fig. A.2.3). Each component has two possible states, an operating state and a failed state.

In general, a system state is defined as a combination of component states. The number of system states is equal to the number of all possible combinations of component states. Hence, for the system in Fig. A.2.3, the number of system states is four.



Component states		
Type	Comp. A	Comp. B
Operating	A	B
Failed	$\bar{A}$	$\bar{B}$

System states	
Number	Component states
1	AB
2	$\bar{A}B$
3	$A\bar{B}$
4	$\bar{A}\bar{B}$

FIG. A.2.3. Two-component system. Component and system states are listed in the tables.

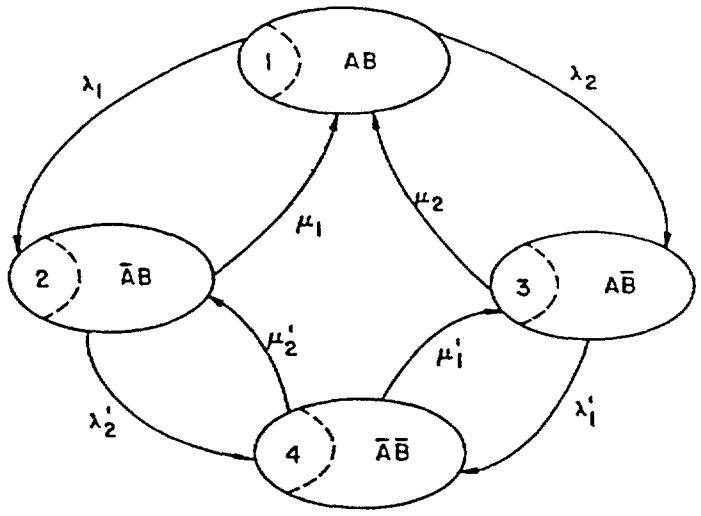


FIG. A.2.4. Transition state diagram for two-component system in Fig. A.2.3.

The state-transition diagram for the system is shown in Fig. A.2.4. A transition from state 1 to state 2 is equivalent to failure of component A, a transition from state 4 back to state 2 is equivalent to repair of component B, etc. Since the components are connected in parallel (Fig. A.2.3), the system is operating if at least one component is operating. Thus, the system is operating if it is in one of the states 1,2, or 3 (Fig. A.2.4), and failed if it is in state 4.

The availability of the system at time t is the probability that the system be operating at time t or that it be in one of the states 1, 2 or 3. Hence, the availability of the system is given by

$$A(t) = \pi_1(t) + \pi_2(t) + \pi_3(t) \tag{2.14}$$

Similarly, the unavailability of the system at time t is the probability that both components have failed, or the probability that the system be in state 4. Hence,

$$U(t) = \pi_4(t) \tag{2.15}$$

In general, if the set Z' of all possible states of a system is partitioned into two subsets X and Y containing all the operating and failed states, respectively, then we have that

$$A(t) = \sum_{i \in X} \pi_i(t) \quad \textit{and} \quad U(t) = \sum_{i \in Y} \pi_i(t) = 1 - A(t) \tag{2.16}$$

The importance of the Markovian model lies in the fact that it allows the transition rates of the system to depend on the initial and final states of the transition. For example, in Fig. A.2.4 a transition from state 1 to state 2 is equivalent to a failure of component A. The same is true for a transition from state 3 to state 4. Yet, the failure rate of component A may depend on whether component B is operating or not.

This possibility is indicated in the state-transition diagram by denoting by λ'_1 and λ_1 the failure rates of component A for the system transitions from state 3 to state 4 and from state 1 to state 2, respectively, and taking $\lambda'_1 \neq \lambda_1$.

Such dependence of the stochastic behavior of the components on the state of the system arises in many practical applications, as illustrated by the following examples.

A.3. STANDBY REDUNDANCY

We will consider again the two-component system of Fig. A.2.3 and assume that one of the components is operating while the other is either on a cold standby mode or on a warm standby mode.

A.3.1. Cold standby redundancy

In cold standby redundancy the non operating component is not subject to any stress and cannot fail.

(a) Markov model

The state transition diagram for this case is as shown in Fig. A.3.1. It is noteworthy that state 3 cannot be reached because component B cannot fail while component A is operating. Here, the important feature is that the failure rate of component B depends on the state of component A. This rate is equal to zero if component A is operating and to λ_2 if component A is failed. Hence, component B cannot be examined independently of component A.

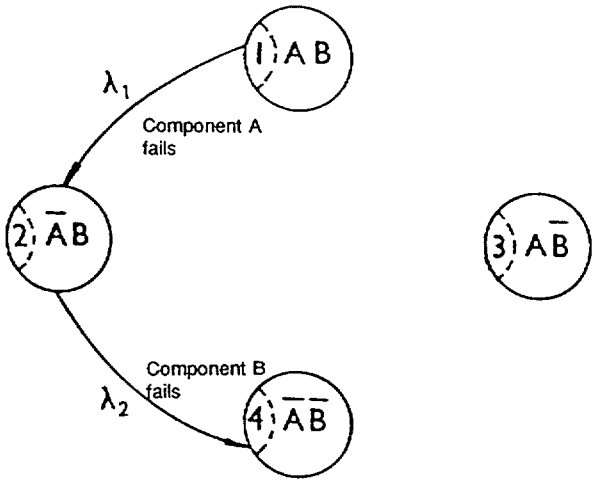


FIG. A.3.1. State-transition diagram for a two-component system with one component in cold standby.

The transition rate matrix for the process is

$$\underline{A} = \begin{bmatrix} -\lambda_1 & \lambda_1 & 0 \\ 0 & -\lambda_2 & \lambda_2 \\ 0 & 0 & 0 \end{bmatrix} \tag{3.1}$$

Using Eq. 3.1 in Eq. 2.2 and solving for the failure probability $\pi_4(t)$ of the system, we find the relation

$$F(t) = \pi_4(t) = 1 - \frac{\lambda_2}{\lambda_2-\lambda_1} exp\ (-\lambda_1 t) + \frac{\lambda_1}{\lambda_2-\lambda_1} exp(-\lambda_2\ t) \tag{3.2}$$

For $\lambda_2 = \lambda_1 = \lambda$, Eq. 3.2 reduces to

$$F(t) = 1 - (1 + \lambda t)\ \exp(-\lambda t) \tag{3.2a}$$

(b) Fault tree model

The fault tree for the system in Fig. A.2.3 is shown in Fig. A.3.2. The top event T (system failure) is given in terms of the basic events as follows

$$T = \overline{A} \cdot \overline{B}$$

Hence, the probability for the top event is

$$Pr(T) = Pr(\overline{A}\ \overline{B}) \tag{3.3}$$

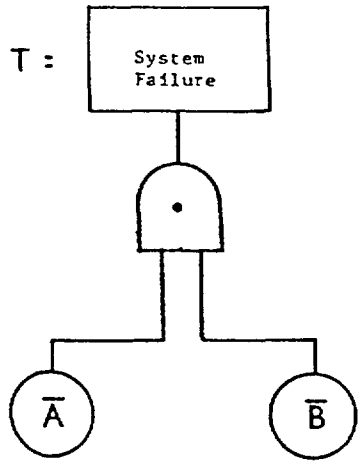


FIG.A.3.2. Fault-tree for system in Fig. A.2.3.

To calculate $Pr(\bar{A}\ \bar{B})$, i.e. the probability that both components are down, taking into consideration the cold standby characteristics of the system, we must solve the Markov model of the preceding subsection. Assuming that the two components are statistically independent, we could calculate erroneous values. Indeed, then we find that

$Pr(\bar{A}) = 1-\exp(-\lambda_1 t)$ = failure probability for component A, (Eq.2.13b),

$Pr(\bar{B}) = 1-\exp(-\lambda_2 t)$ = failure probability for component B, (Eq.2.13b),

and the system failure probability

$$F(t) = Pr(T) = Pr(\bar{A})\ Pr(\bar{B}) = 1-\exp(-\lambda_1 t)-\exp(-\lambda_2 t)+\exp[-(\lambda_1+\lambda_2)t] \tag{3.4}$$

or, if $\lambda_1 = \lambda_2 = \lambda$,

$$F(t) = 1 - 2\exp(-\lambda t) + \exp(-2\lambda t) \tag{3.4a}$$

These results differ from those given by Eqs. 3.2 and 3.2a.

A.3.2. Warm or hot standby redundancy

In warm or hot standby redundancy, the non-operating component can fail even when it is not on line. If the failure rate of a component in a standby mode is different (usually less) than the failure rate of the online mode, the standby is called warm. If the failure rate of a component in a standby mode is equal to that of the online mode, the standby is called hot.

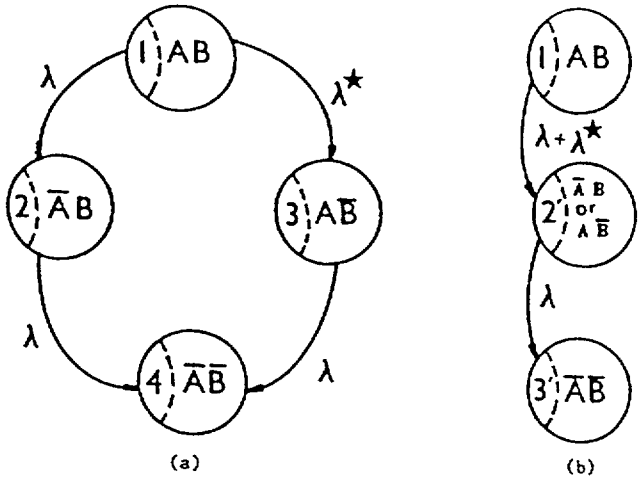


FIG. A.3.3. State-transition diagrams for a two-component system with one component in warm standby.

The state-transition diagram for such standby conditions is shown in Fig. A.3.3(a). If the two components A and B are identical, the state transition diagram in Fig. A.3.3(a) can be reduced to that of Fig. A.3.3(b). In general, the reduction is called merging. It simplifies the numerical difficulties associated with reliability analyses [28].

Solving the state evolution equation corresponding to the state-transition diagram in Fig. A.3.3(b), we find

$$\pi_3(t) = F(t) = 1-(1 + \frac{\lambda}{\lambda^*})\exp(-\lambda t) + \frac{\lambda}{\lambda^*}\exp[-(\lambda+\lambda^*)t] \tag{3.5}$$

Again, this result differs from that given by Eq. 3.4a except when $\lambda = \lambda^*$, namely, when the failure rate of component B does not depend on the state of component A and vice versa.

A.4. COMPONENTS SHARING COMMON LOADS

We will assume that the two components of the system shown in Fig. A.2.3 share a common load so that if one of the two fails the other must operate at 100% of the load. In many applications, the failure rate of each component at partial load differs substantially from that at full load.

Here, the state-transition diagram is as shown in Fig. A.4.1. The failure rate of component A (or B) depends on the state of component B (or A), and therefore, on the state of the system. The process can be merged (Fig. A.4.1b), and the failure probability of the system is given by the relation

$$F(t) = \pi_4(t) = 1 - \frac{2\lambda}{2\lambda-\lambda^*}\exp(-\lambda^* t) + \frac{\lambda^*}{2\lambda-\lambda^*}\exp(-2\lambda t) \tag{4.1}$$

This correct result reduces to that given by Eq. 3.4a only if $\lambda = \lambda^*$.

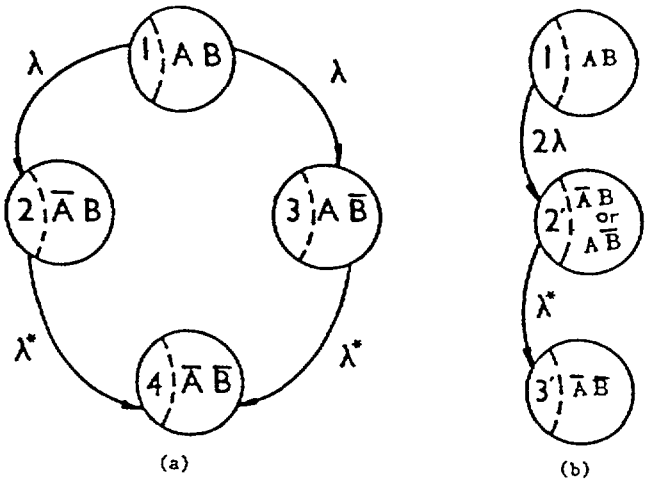


FIG. A.4.1. State transition diagram for a system with two components sharing a common load.

A.5. EXTREME ENVIRONMENT

The failure rates of the components of a system depend on the environment to which they are exposed. For example, the failure rate of a high voltage transmission line depends on whether or not there is a storm.

The arrival of a storm is in itself a random process. Hence, we can distinguish three states of the environment-transmission line system. In state 1 (Fig. A.5.1) there is no storm and the transmission line is up. In state 2, there is a storm and the transmission line is up. In state 3, the transmission line is down. The failure rate of the transmission line when there is no storm is λ_1 (transition rate between states 1 and 3). The failure rate of the transmission line when there is a storm is λ_2 (transition rate between states 2 and 3). The arrival rate for the storm is λ_s (transition rate between states 1 and 2). The failure probability of the transmission line is the probability that the system will be in state 3.

Solving the relevant state evolution equation we find

$$F(t) = \pi_3(t) = 1 - \frac{\lambda_2-\lambda_1}{\lambda_2-\lambda_1+\lambda_s} \exp\left[-(\lambda_1+\lambda_s)t\right] - \frac{\lambda_s}{\lambda_2-\lambda_1+\lambda_s} \exp(-\lambda_2 t) \tag{5.1}$$

If a Markovian model is not used, the failure probability must be approximated by either

$$1-\exp(-\lambda_1 t) = \text{failure probability under normal conditions} \tag{5.2a}$$

or

$$1-\exp(-\lambda_2 t) = \text{failure probability under storm} \tag{5.2b}$$

The probability given by Eq. 5.1 may differ by orders of magnitude from that given by Eq. 5.2.

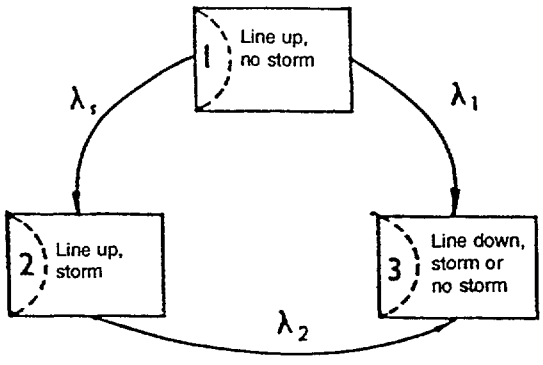


FIG. A.5.1. State-transition diagram for the extreme environment example.

A.6. RELIABILITY OF SYSTEMS WITH REPAIRABLE COMPONENTS

The reliability of a system is by definition the probability that the system will operate continuously from time 0 to time t or the probability that no system failure will be observed during the time interval (0, t). Whenever this quantity is of interest for a system with repairable components a Markovian model is necessary.

As an example, we will consider two repairable components connected in parallel (Fig. A.2.3) under the conditions:

(a) Repair of the components is possible even if the system is not operating. Then, the state transition diagram is as shown in Fig.A.6.1(a). Transitions from state 4 back to states 2 and 3 are possible. The probability that the system will occupy state 4 at time t is the unavailability of the system at time t. It is the probability that the system is unavailable at time t regardless of whether it has failed and been repaired during the time interval (0,t).

(b) Repair of a unit is possible only if the other unit is operating. Then, the state transition diagram is as shown in Fig. A.6.1.(b). Transitions from state 4 back to states 2 and 3 are not possible. If the system enters state 4, it cannot leave again. Here, the probability that the system will occupy state 4 at time t is the probability that the system will fail during the time interval (0,t). It is the failure probability, F(t), the complement of the reliability.

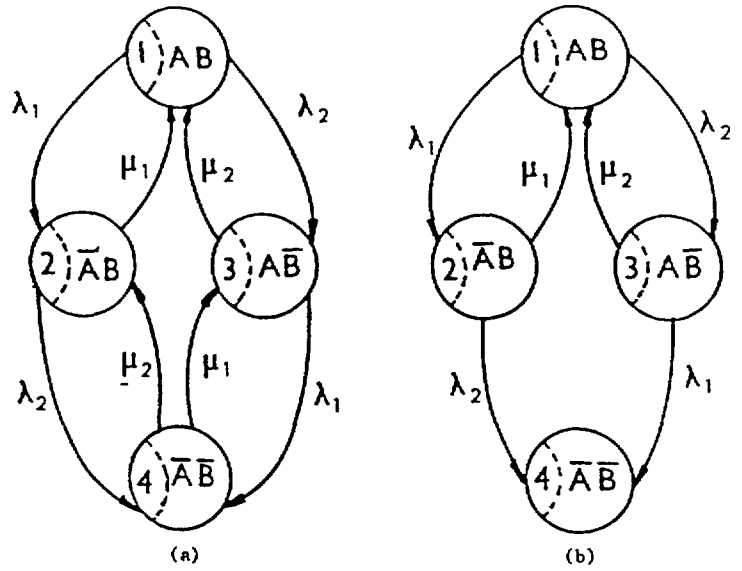


FIG. A.6.1. State transition diagram of two-component system in Fig.A.2.3: (a) when system is down, repair is possible; (b) when system is down, repair is impossible.

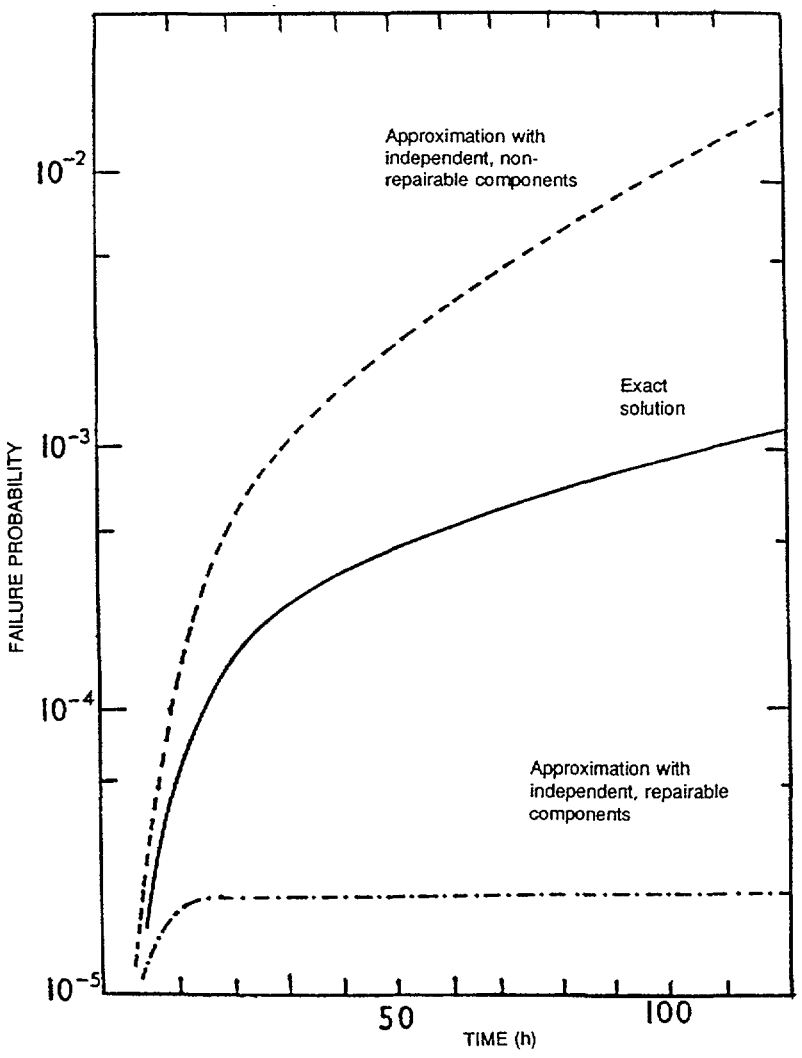


FIG. A.6.2. Failure probability of two-component system with on line repair possible (Fig. A.6.1(b))
$\lambda_1 = \lambda_2 = 10^{-3}\ h^{-1}$ $\mu_1 = \mu_2 = 2\times10^{-1}\ h^{-1}$

If we assume no dependence and use the fault tree model of Fig. A.3.2, we can calculate the unavailability of the system. This is equivalent to considering the system under conditions (a). If, however, we are interested in the failure probability we must consider conditions (b).

This distinction and the need for a Markov model are essential in the analysis of an engineered safety system of a nuclear reactor that starts operating at a certain time during the course of an accident and must continue to operate for a period of T hours. If the system fails before T hours have elapsed, unacceptable damage to the core will result. To calculate the probability of unacceptable damage to the core because of system failure we must consider conditions (b) and the corresponding Markov model. If we assume no dependence, we will miscalculate the probability. Assuming nonrepairable independent components, we will overestimate the value of the failure probability (conservative answer). Assuming repairable independent components, we will underestimate the value of the failure probability (nonconservative answer).

These remarks are illustrated by the numerical results shown in Fig. A.6.2. In particular, if the system must operate for a period of T = 100 hours, the correct probability of unacceptable core damage is equal to 9.4×10^{-4}. A model that assumes independent nonrepairable components yields a failure probability of 9×10^{-3}, an overestimation by a factor of 10. A model that assumes independent repairable components yields a failure probability of 2.5×10^{-5}, an underestimation by a factor of 40.

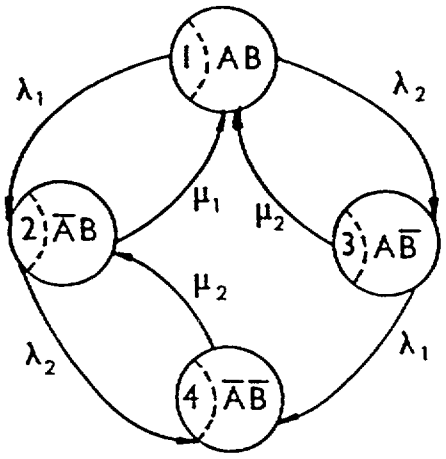


FIG. A.7.1. State transition diagram for a repairable two-component system but one repairman available.

A.7. SYSTEMS WITH SPECIAL REPAIR POLICIES

In many applications, the repair policy of the components of a system depends on the state of the system. Then, a Markov model is necessary for the calculation of the unavailability or the failure probability. Two examples of special repair policies follow.

A.7.1. Limited repair capability

For some systems, the number of components that can be under repair at any instant of time depends on the number of repairmen (or repair crews) that are available. For example, for the two-component system examined in the previous sections, if only one repairman is available then only one component can be repaired at a time and, if we decide that component B will be the first to be repaired, then the state transition diagram will be as shown in Fig. A.7.1. Again, if two repairmen are available, then the state transition diagram will be as shown in Fig. A.6.1a.

Values of unavailability versus time for a specific system are shown in Fig. A.7.2.

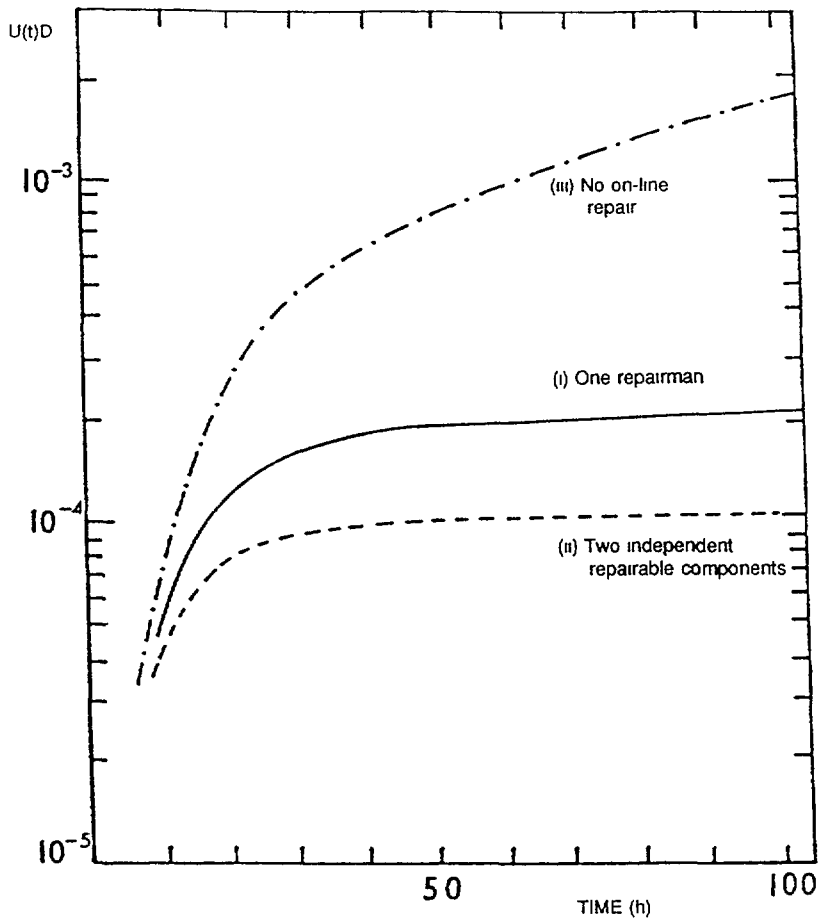


FIG. A.7.2. Unavailability of a two-component system under different repair policies:

(i) one repairman available (Fig. A.7.1), $\lambda_1 = \lambda_2 = 10^3$ h ^{1};

(ii) two repairmen available (Fig. A.6.1a), $\mu_1 = \mu_2 = 10^{-1}$ h^{-1};

(iii) no online repair possible (Fig. A.7.3), $\lambda_1 = \lambda_2 = 10^3$ h $^{-1}$;

$\mu_1 = \mu_2 = 1.5 \times 10^1$ h ^{1}.

A.7.2. Repair all components before resuming operation

In some situations, repair of components is more expedient if the system is not operating. In other situations, because of practical difficulties such as radiation fields or in-vessel components, repair is possible only when the system is not operating. For these situations our two-component example will have the state-transition diagram shown in Fig. A.7.3. In this diagram, we have introduced two new states, state 5 and state 6, in which the components are under repair but the system is not operating.

The unavailability, U(t), of the system is equal to the probability that the system will be in any of the states 4, 5 or 6 and, therefore,

$$U(t) = \pi_4(t) + \pi_5(t) + \pi_6(t) \tag{7.1}$$

Its values versus time for a specific system are shown in Fig. A.7.2.

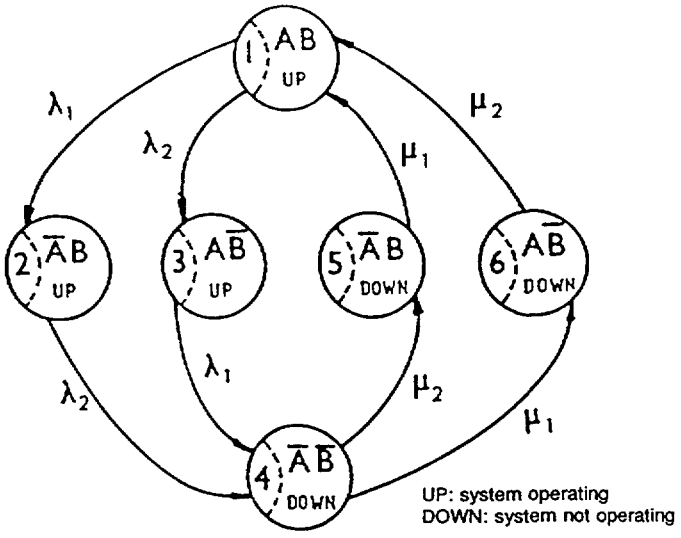


FIG. A.7.3. State transition diagram of a two component system (Fig. A.2.3) when online repair is not possible.

A.8. CHALLENGE-DEPENDENT FAILURE PROBABILITY

Usually a safety system remains in a standby mode until there is a need for it to operate. An undesirable event (an accident) occurs if the system is not available to operate when challenged to do so. Hence, the probability that an accident will occur during a time period T is the probability that a challenge will occur at some instant in the period T and at that instant the system is unavailable.

The correct calculation of the accident probability requires proper handling of the dependence between the frequency of the challenge and the unavailability of the system. If we assume no dependence, then we will grossly overestimate the accident probability. We will confirm this assertion by using a simple numerical example.

A.8.1. Model with no dependence

We will consider a safety system consisting of two components in parallel. We will assume that a challenge (a need for operation) for this system arrives according to a Poisson random process with an arrival rate λ_c.

It can be shown that if the unavailability of the system is independent of the occurrence of challenges, then the accident probability,

F(T), is given by the expression [28]

$$F(T) = 1 - \exp[-\lambda_c T\overline{U}(T)] \tag{8.1}$$

where $\overline{U}(T)$ is the average unavailability of the system during the time period T given by the relation

$$\overline{U}(T) = \frac{1}{T}\int_0^T U(t)dt \tag{8.2}$$

For small values of $\lambda_c T\overline{U}(T)$, Eq. (8.1) can be approximated by the relation

$$F(T) = \lambda_c T\overline{U}(T) \tag{8.3}$$

The state-transition diagram for the two-component system is shown in Fig. A.8.1. We have assumed that the failures are undetectable and, therefore, that the components are unrepairable. The unavailability of the system is the probability that the system will be in state 4. Hence,

$$U(t) = \pi_4(t) = 1\text{-}2\exp(-\lambda t) + \exp(-2\lambda t) \tag{8.4}$$

The same result could have been obtained with other methods such as fault tree, reliability block diagrams or state enumeration.

Using Eq. 8.4 in Eq. 8.2 we find

$$\overline{U}(T) = \frac{1}{T}\int_0^T \pi_4(t)dt = 1 - \frac{2}{\lambda T}[1-\exp(-\lambda T)] + \frac{1}{2\lambda T}[1-\exp(-2\lambda T)] \tag{8.5}$$

Finally, substituting Eq. 8.5 in Eq. 8.1, we find F(T).

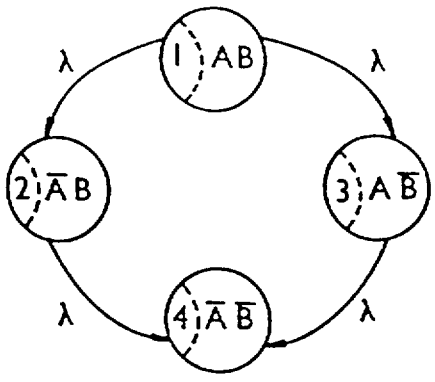


FIG. A.8.1. State transition diagram for a two-component system with no dependence on the challenge rate.

A.8.2. Model with dependence

To account for dependence in the system of Section A.8.1, we must include an additional state - accident state 5 - in the state transition diagram (Fig. A.8.2). A transition to state 5 occurs if the system is unavailable (state 4) and the challenge occurs. The accident probability for a period of time T is the probability that the system will be in state 5 at time t = T.

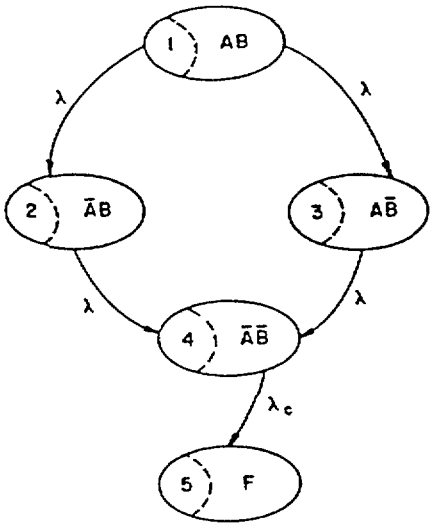


FIG. A.8.2. State transition diagram for a two-component system with dependence on the challenge rate.

Solving the state evolution equation for the process in Fig. A.8.2, we find

$$F(T) = \pi_5(T) = 1 - \frac{2\lambda_c}{\lambda_c-\lambda}\exp(-\lambda T) + \frac{\lambda_c}{\lambda_c-2\lambda}\exp(-2\lambda T) - \frac{2\lambda^2}{(\lambda_c-2\lambda)(\lambda_c-\lambda)}\exp(-\lambda_c T) \qquad (8.6)$$

The values of the accident probability given by Eq. 8.6 are lower than those obtained from Eqs. 8.1 and 8.5. This assertion is verified by the numerical results shown in Fig. A.8.3. In particular, for T = 8500 hours the accident probabilities are 6×10^{-3} and 5.6×10^{-2} for the models with and without dependence, *respectively.*

A.8.3. Model with dependence and renewal effects

Another dependence of the unavailability of the system on the frequency of challenges is due to the renewal effect that successful challenges have on the system. For example, if a challenge occurs when the system is in either state 2 or 3 (Fig. A.8.2) then the failure of the failed component is revealed and can be repaired. Thus, a challenge in either state 2 or state 3 will bring the system back to state 1.

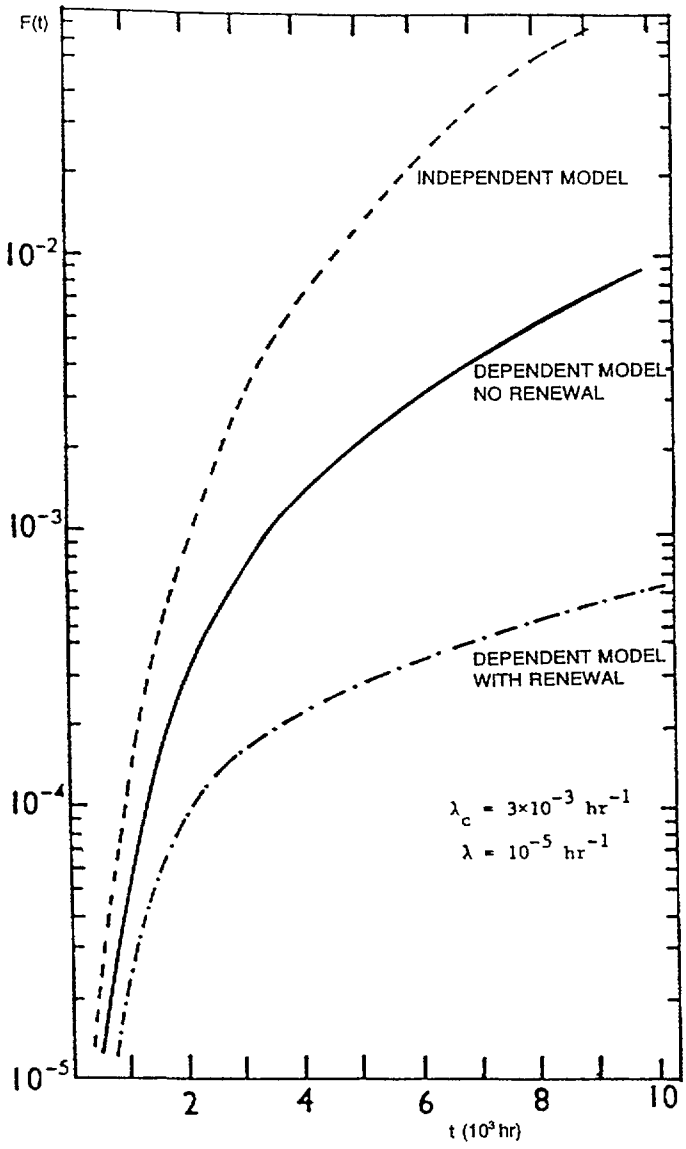


FIG. A.8.3. Failure probability with challenge-dependence.

The corresponding state transition diagram is as shown in Fig. A.8.4. Again the accident probability is the probability of being in state 5 at time t = T. Numerical results for a specific system are shown in Fig. A.8.3. For T = 8500 hours, this model yields an accident probability of 5.2 x 10^{-4}, two orders of magnitude less than the model with no dependence.

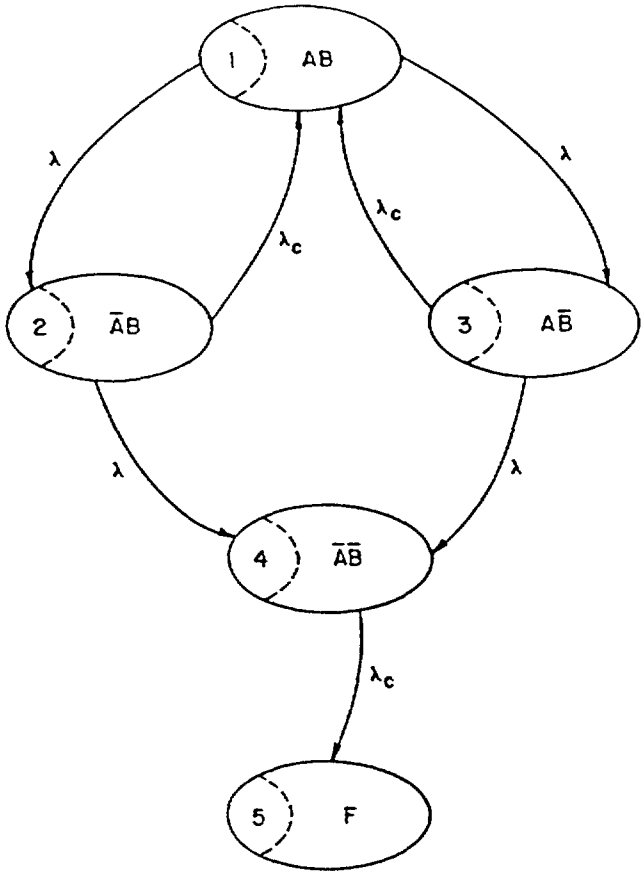


FIG. A.8.4. State transition diagram with dependence on the challenge rate and renewal effect of successful challenges.

A.9. LITERATURE REVIEW

The advantages of using Markov processes in reliability problems have been recognized since the inspection of the reliability discipline. Almost every book published on reliability presents Markov modeling as the most powerful reliability technique because it can incorporate a great variety of system characteristics. Numerical difficulties, however, have limited the use of the technique to relatively small systems consisting of only a few components. A successful effort has been made to apply this powerful technique to large systems, through the use of three techniques: state ordering, state merging and judicious choices of time steps. The three techniques are discussed by Papazoglou and Gyftopoulos in BNL-NUREG-50864 (1978) and in a paper in Nuclear Science and Engineering, Vol. 73, No. 1, Jan. 1980.

What follows is a short list of publications together with a brief comment on each publication.

A.9.1. Books on Markov processes

1. HOWARD R., Dynamic Probabilistic Systems, Vols. I and II, Wiley (1971).

Probably the most complete book on applications of Markov processes in studying dynamic probabilistic systems. Though it includes some examples, this treatise is not specifically oriented toward reliability analysis.

2. KEMENY, J.G., SNELL, J.L., Finite Markov Chains, D. Van Nostrand (1961).

A classic reference for Markovian analysis but not specifically oriented toward reliability analysis.

A.9.2. Books on reliability analysis

3. BARLOW, R.E., PROSHAN, F., Mathematical Theory of Reliability, Wiley (1965).

This book presents the Markov approach in Chapter 5, "Stochastic Models for Complex Systems".

4. BILLINTON, R., RINGLEE, R., WOOD, A., Power System Reliability Calculations, MIT Press (1973).

The authors use exclusively Markov models in calculations of reliability of electric power systems.

5. DHILLON, B.S., and SINGH, C. Engineering Reliability: New Techniques and Applications, Wiley (1981).

In this book, the authors make the following comment on Markovian reliability analysis (Section 3.6.2, p. 37): "The state space approach (Markov processes) is a very general approach and can generally handle more cases than any other method. It can be used when the components are independent as well as for systems involving dependent failure and repair modes. There is no conceptual difficulty in incorporating multi-state components and modeling common cause failures".

They treat common cause failures in terms of Markovian models (Section 4.14), and present applications of Markovian reliability analysis in software reliability, repairable three-state devices, generating capacity reliability (electric power systems), transmission and distribution systems (electric power systems), transit system reliability, and computer system reliability. The book also includes an extensive bibliography.

6. ENDRENYI, J., Reliability Modeling in Electric Power Systems, Wiley (1978).

The author uses almost exclusively the state space approach (Markov models) to analyze many problems of reliability of electric power systems.

7. GNEDENKO, B.V., BELYAYEV, Y. and SOLOVYEV, A., Mathematical Methods of Reliability Theory, Academic Press (1969).

The authors use Markov models to study a variety of problems on standby redundancy with renewal. Combinatorial analysis and the Markov approach are the only reliability techniques discussed.

8. GREEN A.E., BOURNE A.J., "Reliability Technology", Wiley Interscience (1972).

The authors introduce the concept of state-change and use the corresponding Markov processes to derive general reliability and availability expressions (Chapters 10 and 11).

9. HENLEY, E., KUMAMOTO, H., Reliability Engineering and Risk Assessment, Prentice-Hall Inc. (1981).

This book contains one of the most complete lists of reliability techniques. The Markov approach is presented as the only methodology capable of answering reliability questions for systems with dependence (Chapter 8: System quantification for dependent basic events), and for calculating the reliability of systems with repairable components (Chapter 9: System quantification, Reliability).

10. SANDLER, G.H., System Reliability Engineering, Prentice-Hall (1963).

This book is devoted almost exclusively to Markovian reliability models. It is perhaps the most complete reference on Markovian models of small systems.

11. SINGH, C., BILLINTON R., System Reliability Modeling and Evaluation, Hutchinson, London (1977).

This book is exclusively devoted to Markovian reliability models.

12. SHOOMAN, M.D., Probabilistic Reliability: An Engineering Approach, McGraw-Hill (1969).

This book includes many reliability techniques. Markov models are used for the analysis of systems incorporating dependence, repair or standby operation. The author comments: "The Markov model approach is perhaps the best and most straightforward approach to computations in systems with dependence, repair, or standby operation", (Section 5.8.4, p. 243).

A.9.3. Papers and reports

A.9.3.1. Review documents

13. GENERAL ELECTRIC CO., "Reliability manual for LMFBR", Vol. 1, Report SRD-75-064. Prepared by Corporate Research and Development, General Electric Co., for the Fast Breeder Reactor Department, General Electric Co., Sunnyvale, CA (1975).

This manual presents an extended list of reliability analysis techniques pertinent to nuclear reactor systems. Markovian analysis is described as the most suitable technique for reliability analysis of repairable systems (Section 3.5.7, Complex repairable systems, Markov Analysis).

14. RASMUSON, D.M., BURDIC, G.R., WILSON, J., "Common Cause Failure Analysis Techniques: A Review and Comparative Evaluation", EG&G Report TREE-1349, (1979).

This report contains reviews and evaluations of selected common cause failure analysis techniques. Markovian reliability analysis is listed among the available techniques for quantitative evaluation of common cause failures. In evaluating the Markovian technique the authors state (Section 11.6, p. 113): "In terms of the variety of system characteristics which it can calculate, Markov modeling probably represents the most powerful reliability technique. However, due to limitations on the number of states for which calculations are feasible, the technique has been essentially ignored in the nuclear field until recent years.

Two approaches have been used to solve the problem of size limitation: (a) small systems or resolution to subsystem level only; and (b) special calculation and reduction techniques. These approaches have still not resulted in widespread use of Markov modeling in nuclear industry. Perhaps as failure data become more detailed the versatility of Markov modeling in calculating diverse reliability characteristics will be more appreciated".

15. BLIN, A., CARNINO, A., GEORGIN, J.P., "Use of Markov Processes for Reliability Problems", in Synthesis and Analysis Methods for Safety and Reliability Studies edited by Apostolakis et al., Plenum Press (1980).

This paper summarizes French reliability efforts in nuclear systems. The authors state: "It is not possible to use methods such as fault tree analysis, to assess the reliability or the availability of time evolutive systems. Stochastic processes have to be used and among them the Markov processes are the most interesting ones."

A.9.3.2. Applications of Markovian analysis in large nuclear systems

16. PAPAZOGLOU, I.A., GYFTOPOULOS, E.P., "Markovian Reliability Analysis Under Uncertainty with an Application on the Shutdown System of the Clinch River Breeder Reactor". Brookhaven National Laboratory Report, NUREG/CR-0405, (BNL-NUREG-50864) (1978).

The authors develop a methodology for the assessment of the uncertainties about the reliability of nuclear reactor systems described by Markov models and present an assessment of the uncertainties about the probability of loss of coolable core geometry of the CRBR due to shutdown system failures.

The Markov model used in this study includes common cause failures, interdependence between the unavailability of the system and the occurrence of transients, and inspection and maintenance procedures that depend on the state of the system, and the possibility of human errors.

17. WESTINGHOUSE ELECTRIC CORPORATION, "Reliability Assessment of CRBR Reactor Shutdown System", WARD-D-0118, (1975).

18. ILBERG D., "An Analysis of the Reliability of the Shutdown Heat Removal System for the CRBR", UCLA-ENG-7682 (1976).

A Markovian model for the calculation of the reliability of SHRS of the CRBR was used. The Markovian model was chosen because ..." it is convenient for the analysis of time dependent reliability (or availability) of safety systems, when subsystems rather than a large number of components are included. A Markov model treats easily repair rates, failure to start upon demand, changes with time of the system functional configuration, and common mode failure transitions between states of the systems" (Section 4.1, p. 5).

19. BLIN, A., CARNINO, A., BOURSIER, M. GREPPO J.F., "Détermination, par une approche probabiliste, d'une règle d'exploitation des alimentations de 6.6 kV des réacteurs à eau sous pression (tranches de 900 MW(e))", "Reliability of Nuclear Power Plants", Proceedings of a Symposium, Innsbruck, IAEA (1975).

A.9.3.3. General applications of Markovian reliability analysis

20. BUZACOTT, J.A., "Markov Approach to Finding Failure Times of Repairable Systems", IEEE Trans. Reliability, Vol. 19, (1979), p. 128-134.

21. ENDRENYI, J., BILLINTON R., "Reliability Evaluation of Power Transmission Networks: Models and Methods", CIGRE, Paper No. 32-06, (1974).

22. ENDRENYI, J., MAENHAUT, P.C., PAYN, L.E., "Reliability Evaluation of Transmission Systems with Switching after Faults: Approximations and a Computer Program", IEEE Transactions on Power Apparatus and Systems, Vol. 92, pp. 1863-1875, (1973).

23. FLENHIGER, B.J., " A Markovian Model for the Analysis of the Effects of Marginal Testing on System Reliability", An. Math. Stat., Vol. 33, (1962) pp. 754-766.

24. SINGH, C., BILLINTON, R., "Frequency and Duration Concepts in System Reliability Evaluation", IEEE Trans. Reliability, Vol. R-24, (1975), pp. 31-36.

25. SINGH, C., BILLINTON, R., "Reliability Modelling in Systems with Non-Exponential Down Time Distributions", IEEE Transactions on Power Apparatus and Systems, Vol. 92, (1973), pp. 790-800.

26. ZELENTSOV, B.P., "Reliability Analysis of Large Nonrepairable Systems", IEEE Trans. Reliability, Vol. R-19, (1970), pp. 132-136.

A.9.3.4. Simple applications of Markov models in fault trees

Modeling of small portions of a system by a Markov process in relation to a fault tree is presented in the following papers.

27. NEUMAN, C.P., BONHOME, H.M., "Evaluation Maintenance Policies using Markov Chains and Fault Tree Analysis", IEEE Transactions of Reliability, Vol. R-24, (1975).

28. CALDOROLA, L., "Fault Tree Analysis of Multistate Systems with Multistate Components", ANS topical Meeting on Probabilistic Analysis of Nuclear Reactor Safety, Los Angeles, California Paper VIII. 1, (1978). Also appearing in Synthesis and Analysis Methods for Safety and Reliability Studies, edited by Apostolakis et al., Plenum Press (1980).

The following two reports present a fault-tree technique that can incorporate Markovian models for single components.

29. MODARES, M., RASMUSSEN, N., WOLF, L., "Reliability Analysis of Complex Technical Systems using the Fault Tree Modularization Technique", MITNE-228 (1980).

30. KARIMI, R., RASMUSSEN, N., WOLF L., "Qualitative and Quantitative Reliability Analysis of the Safety Systems". MITEL-80-015 (1980).

REFERENCES

[1] WESTINGHOUSE ELECTRIC CORPORATION, Reference Safety Analysis Report, RESAR-3S (1975).

[2] US NUCLEAR REGULATORY COMMISSION, Standard Technical Specifications for Westinghouse Pressurized Water Reactors, NUREG-0452, Revision 3 (1980).

[3] JANSEN, R.L., LIJEWSKI, L.M., MASARIK, R.J., "Evaluation of Surveillance Frequencies and Out of Service Times for the Reactor Protection Instrumentation System", Westinghouse Electric Corporation, WCAP-10271 (1983).

[4] APOSTOLAKIS, G., CHU, T.L., "The Unavailability of Systems Under Periodic Test and Maintenance", Nuclear Technology, 50 (1980).

[5] VESELY, V.E., et al., "FRANTIC II - A Computer Code for Time Dependent Unavailability Analysis", Brookhaven National Laboratory, NUREG/CR-1924 (1981).

[6] ROSS, S.M., Introduction to Probability Models, Academic Press, New York (1973).

[7] HOWARD, R., Dynamic Probabilistic Systems, Volumes I and II, John Wiley and Sons, Inc. New York (1971).

[8] SHOOMAN, M.D., Probabilistic Reliability: An Engineering Approach, McGraw-Hill Book Company, New York (1968).

[9] PAPAZOGLOU, I.A., GYFTOPOULOS, E.P., "Markovian Reliability Analysis Under Uncertainty with an Application on the Shutdown System of the Clinch River Breeder Reactor", Nuclear Science and Engineering, 73, 1 (1980).

[10] PAPAZOGLOU, I.A., GYFTOPOULOS, E.P., "Markov Processes for Reliability Analyses of Large Systems", IEEE Trans, Reliability, R-26, 232 (1977).

[11] PAPAZOGLOU, I.A., "Elements of Markovian Reliability Analysis in Reliability Engineering, edited by A. Amendola and A. Saiz de Bustamante, Kluwer Academic Publishers (1988).

[12] FLEMING, K.N., RAABE, P.H., " A comparison of Three Methods for the Quantitative Analysis of Common Cause Failures", Proceedings of the ANS Topical Meeting on Probabilistic Analysis of Nuclear Reactor Safety, May 1978, Los Angeles, California (1978).

[13] MCCLYMONT, A.S., POEHLMAN, B.W., "ATWS: A Reappraisal Part 3: Frequency of Anticipated Transients", Electric Power Research Institute, EPRI NP-2230 (1982).

[14] KOLB, G.J. et al., "Review and Evaluation of the Indian Point Probabilistic Safety Study", Sandia National Laboratories, NUREG/CR-2934 (1982).

[15] COMMONWEALTH EDISON COMPANY, Zion Probabilistic Safety Study (1981).

[16] IEEE, Guide to the Collection and Presentation of Electrical, Electronic, and Sensing Component Reliability Data for Nuclear Power Generating Station, IEEE Std. 500-1977.

[17] MILLER, C.F., et al., "Data Summaries of Licensee Event Reports of Selected Instrumentation and Control Components at U.S. Commercial Nuclear Power Plants", EGG Idaho, Inc., NUREG/CR-1740 (1981).

[18] POWER AUTHORITY OF THE STATE OF NEW YORK AND CONSOLIDATED EDISON COMPANY OF NEW YORK, INC., Indian Point Probabilistic Safety Study (1982).

[19] PAPAZOGLOU, I.A., et al., "Bayesian Analysis Under Population Variability with an Application to the Frequency of Loss of Offsite Power and Anticipated Transients in Nuclear Power Plants", Brookhaven National Laboratory, BNL-NUREG-31794, Informal Report (1983)

[20] PAPAZOGLOU, I.A., CHO, N., "Review and Assessment of Evaluation of Surveillance Frequencies and Out of Service Times for the Reactor Protection Instrumentation System", Brookhaven National Laboratory, BNL-NUREG-51780 (1984).

[21] SWAIN, A.D., GUTTMAN, H.E., "Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications", NUREG/CR-1278, Draft Report (1982).

[22] KAPLAN, S. et al., "Methodology for Probabilistic Risk Assessment of Nuclear Power Plants", Pickard, Lowe and Garrick, Inc., PLG-0209 (1981).

[23] US NUCLEAR REGULATORY COMMISSION, Reactor Safety Study: An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants, NUREG-75/014 (WASH-1400) (1975).

[24] APOSTOLAKIS, G., KAPLAN, S., "Pitfalls in Risk Calculations", Reliability Engineering, 2, 135 (1981).

[25] PAPAZOGLOU, I.A., "STAGEN-MARELA: A Computer Code for Markovian Reliability Analysis", BNL Letter Report to NRC (1985).

[26] BIZZAK et.al., "Risk-Based Evaluation of Technical Specification Problems at the La Salle County Nuclear Station". EPRI NP-5238 (1987).

[27] WAGNER, D.P., et al., "Risk Based Evaluation of Technical Specifications" (Interim Report). EPRI NP-4317, Battelle Colombus Division (1985).

[28] PAPAZOGLOU, I.A., GYFTOPOULOS, E.P., "Markovian Reliability Analysis Under Uncertainty with an Application on the Shutdown System of the Clinch River Breeder Reactor". Brookhaven National Laboratory Report, NUREG/CR-0405, (BNL-NUREG-50864) (1978).

LIST OF ABBREVIATIONS

ABT	Allowable Bypass Time
AOT	Allowable Out-of-Service Time or Allowable Outage Time
ATWS	Anticipated Transient Without Scram
FSAR	Final Safety Analysis Report
PCD	Probability of Core Damage per year of reactor operation
PSA	Probabilistic Safety Assessment
PWR	Pressurized Water Reactor
RPIS	Reactor Protection Instrumentation System
RPS	Reactor Protection System
SF	Surveillance Frequency
STI	Surveillance Test Interval
TS	Technical Specification
USNRC	United States Nuclear Regulatory Commission
UV	Under Voltage
WOG	Westinghouse Owner's Group

CONTRIBUTORS TO DRAFTING AND REVIEW

I. A. Papazoglou
Institute of Nuclear Technology - Radiation Protection
N.C.S.R. "Demokritos"
15310, Aghia Paraskevi
Athens - Greece

Oversight Committee for the Development of a Series of PSA Case Studies

J. Caisely
Nuclear Energy Agency
of the OECD
Paris - France

A. Carnino[1]
Electricité de France
32, rue de Monceau
75384 Paris CEDEX 08 - France

J. Gaertner
Electric Power Research Institute
Palo Alto
California 94303 - USA

S. Hall
Safety & Reliability Directorate
UKAEA
Culcheth, Warrington WA3 4NE - United Kingdom

P. Kafka
Gesellschaft für Reaktorsicherheit (GRS) mbH
Forschungsgelände
8046 Garching - Germany

J. Villadoniga
Consejo de Seguridad Nuclear
S/Sor Angela de la Cruz 3
28020 Madrid - Spain

IAEA

M. Cullingford[2]	Scientific Secretary Division of Nuclear Safety
L. Lederman	Division of Nuclear Safety
S.M. Shah	Division of Nuclear Safety

[1] Now at IAEA, Division of Nuclear Safety.

[2] Now at USNRC, Office of Nuclear Reactor Regulation.