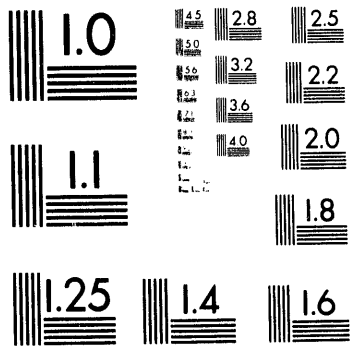

1.0
1.1
1.25
1.4
1.6
1.8
2.0
2.2
2.5
2.8
3.2
3.6
4.0
4.5
5.0
5.6

1 of 2

NUREG/CR-5995
BNL-NUREG-52364
RG, RX

Technical Specification Action Statements Requiring Shutdown

A Risk Perspective with Application to the RHR/SSW Systems of a BWR

Manuscript Completed: October 1993
Date Published: November 1993

Prepared by
T. Mankamo, Avaplan Oy
I. S. Kim, P. K. Samanta, Brookhaven National Laboratory

Avaplan Oy
Kuunsade 2 DE
SF-02210 Espoo
Finland

Under Contract to:
Brookhaven National Laboratory
Upton, NY 11973

Prepared for
Division of Systems Research
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001
NRC FIN L2289

DISTRIBUTION OF THIS DOCUMENT IS UNLIMITED

ABSTRACT

When safety systems fail during power operation, the limiting conditions for operation (LCOs) and associated action statements of technical specifications typically require that the plant be shut down within the limits of allowed outage time (AOT). However, when a system needed to remove decay heat, such as the residual heat removal (RHR) system, is inoperable or degraded, shutting down the plant may not necessarily be preferable, from a risk perspective, to continuing power operation over a usual repair time, giving priority to the repairs.

The risk impact of the basic operational alternatives, i.e., continued operation or shutdown, was evaluated for failures in the RHR and standby service water (SSW) systems of a boiling-water reactor (BWR) nuclear power plant. A complete or partial failure of the SSW system fails or degrades not only the RHR system but other front-line safety systems supported by the SSW system.

This report presents: (a) the methodology to evaluate the risk impact of LCOs and associated AOT; (b) the results of risk evaluation from its application to the RHR and SSW systems of a BWR; (c) the findings from the risk-sensitivity analyses to identify alternative operational policies; and (d) the major insights and recommendations to improve the technical specifications action statements.

CONTENTS

CONTENTS (Cont'd)

FIGURES

FIGURES (Cont'd)

TABLES

EXECUTIVE SUMMARY

Limiting conditions for operation (LCOs) of Technical Specification (TS) define the allowed outage time (AOT) to complete repair of failed component(s), and the associated action requirements to be taken if the repair cannot be completed within the defined AOT. Typically, the action required is plant shutdown. However, when failures are detected in those standby systems needed for plant shutdown, such requirements may be undesirable from a risk point of view. This report presents a methodology to evaluate the risk impact of TS requirements for such situations. Plant-specific evaluations focussed on the residual heat removal (RHR) and standby service water (SSW) systems of a boiling water reactor (BWR). Based on this evaluation, specific recommendations to define risk-effective TS requirements are presented for these systems for the plant studied.†

The TS improvements studied here are expected to serve the general objectives of risk control during plant operation in the following ways:

1) identify risky situations for operation quickly,

2) alert plant personnel to situations where safer alternatives are not available, requiring quick diagnosis and resolution of the problem, and

3) avoid TS requirements that may increase risk, as opposed to providing safer action requirements.

The risk-based methodology is presented to analyze two major decision paths: (1) continued operation in such failures, and (2) plant shutdown to complete repairs in the cold shutdown state. In addition to evaluating these decision paths, specific sensitivity evaluations are presented to seek operational policy alternatives or additional guidelines within each of the decision choices, so that the risk impact is controlled, as far as possible, whenever the LCOs for failures in such systems are entered.

I. SUMMARY OF FINDINGS FROM RISK EVALUATIONS

To analyze the risk impact of TS action requirements, we compared the risks associated with continuing power operation and with shutting down the plant for single and multiple failures in the RHR and SSW systems of a BWR. These findings are based on a single plant, a General Electric BWR/6 plant that has a 2-train RHR and a 3-train SSW system. (Although there is a third train in the RHR system, it cannot be used to remove decay heat but is dedicated to the low pressure coolant injection mode).

Single Train Failure in the RHR and SSW Systems

- Single RHR train failure results in a small increase in the operational risk (i.e., the core-damage frequency). The core-damage probability (CDP) from shutdown in such a situation is slightly larger than the CDP for continued operation over the mean repair time, which is also small.

---

†This report describes a research method and presents an example analysis using the Grand Gulf Nuclear Power Station. The results of this analysis do not reflect any position or policy of the US Nuclear Regulatory Commission on technical specifications; rather, they include recommendations that would need to be considered in light of the existing legal and regulatory requirements for technical specifications.

- Single SSW train failure results in about a 7-fold increase in the core-damage frequency (CDF) level for continued operation. The plant shutdown incurs a smaller probability of core damage than continued operation if the repair takes longer than about 3 days.

Multiple Train Failures in the RHR and SSW Systems

- Failure of two RHR trains also results in relatively small increase in the level of CDF, if full-power operation is continued. In this situation, the CDP due to plant shutdown is larger than that of continued operation over the mean repair time by about a factor of 7, but the expected core damage probability in either case is relatively small, i.e., less than 1×10^{-7}.

- Failure of two SSW trains results in approximately a factor of 160 increase in the CDF, if power operation is continued. When shutting down the plant the CDP is approximately 1×10^{-6} over the mean repair time, by about a factor of 2 larger than that for continued operation. Thus, the current TS requirement of immediate shutdown in this situation appears to be a candidate for reconsideration.

- Failure of three SSW subsystems results in a large increase in the CDF during operation (by almost 4 orders of magnitude over the baseline risk). The risk associated with plant shutdown also is large, approximately a factor of 3 larger than that of continued operation over the mean repair time. Both options have significant effects on risk. TS action statements in this case also are a candidate for reconsideration.

II. ANALYSES OF OPERATIONAL POLICY ALTERNATIVES

- When failures are detected in the RHR or SSW systems, the most risk-effective measure is to quickly repair at least one train of the system. This implies that a reasonable AOT may be given for multiple failures in the RHR/SSW systems.

- For longer repair times, the condition of redundant train(s) should be determined, preferably by diagnostic measures, especially if an actual demand test is expected to adversely affect any degraded component. This measure is intended to detect the presence of any common cause failure, or assure availability of an alternate success path.

- Shutdown may be the risk-effective alternative, if the repair time is assessed to take long. However, attempting to repair the failed component, and then proceeding to shutdown because the repair cannot be completed within the AOT should be avoided because it will incur risk both from continued operation and from transition to shutdown. The decision to shutdown, if considered evident, should be made as soon as possible.

- When going to shutdown, the intent should be to quickly reach the cold shutdown state, where alternate capability for removing decay heat is available. To minimize the risk, the availability of power conversion system should be maintained, and alternate capability for decay heat removal should be assured during transition from full power to cold shutdown state.

- If the need for shutdown is evident and the decision to shut down is made, it should be achieved as quickly as possible without incurring undue transient risk. In these special cases, the time required to reach cold shutdown may be reduced from the current maximum of 36 hours to approximately 12 hours.

III. GENERAL OBSERVATIONS FOR IMPROVING THE LCO REQUIREMENTS

- The standby safety systems needed for safe shutdown, such as the RHR and SSW systems, require different considerations from other systems in evaluating potential improvements in their LCO requirements (including AOTs and action statements). As opposed to other safety systems that are not required for shutdown, failures in these systems can result in a large shutdown risk which may be higher than the risk of continued operation. The TS action statements need to reconcile this risk implication.

- Not surprisingly, the risks for multiple failures are significant. For the systems needed for shutdown, the risks for both alternatives (i.e., continued operation and shutdown) can be significant. However, there is no clear requirement in TS to identify the multiple failures. Even with the TS surveillance requirements, it is quite conceivable that such multiple failures may remain undetected when the risk impacts are large.

- Caution is needed in devising TS action requirements for failures in the systems needed for shutdown. Numeric comparison of the risk of alternative courses of action should not be the only consideration in defining the action statements. Such approach would result in longer AOTs for multiple failures, thus possibly providing incentives to declare multiple failures when repairs for a single failure cannot be completed within the prescribed AOT.

IV. IMPLICATIONS FOR TECHNICAL SPECIFICATION

From our work, we can suggest several improvements to the TS requirements for the systems studied. Our idea has been to use the insights gained to suggest modifications, rather than directly attempting to use the quantitative data. Accordingly, the timing of the actions suggested is based on qualitative considerations, where insights from quantitative risk analyses are important inputs. The suggested modifications will provide guidance for improving TS requirements, but additional plant-specific evaluations may be required to develop individual strategies to effectively control risk during failure of the systems needed for shutdown.

Specific TS improvements suggested for consideration for RHR/SSW systems are as follows:

a) Provide a 3-day AOT for double failures in the RHR system, as opposed to the current requirement of 8 hours.

b) For single failures in the SSW system, the AOT should remain 3 days, but operability of redundant trains should be tested before the end of the first day, if repair has not been completed.

c) For double/triple failures in the SSW system:

- provide a 2 day AOT, if by the end of the first day it is judged that repair of one of the trains can be completed by the end of the second day.

  require that shutdown be initiated immediately, if by the end of the first day it is judged that repair of one of the trains will not be completed by the end of the second day.

d) The time allowed to reach cold shutdown, for these special cases (double/triple failures of the SSW systems), should be reduced to a total of 12 hours (6 hours to reach hot shutdown, and another 6 hours to reach cold shutdown) from a current maximum of 36 hours (12 hours to reach hot shutdown, and another 24 hours to reach cold shutdown).

Our results are based on a plant-specific application carried out for the RHR and SSW systems of a BWR. However, similar situations may exist for other systems; namely, emergency power (EP) system in a BWR, and auxiliary feedwater (AFW), service water (SW), component cooling water (CCW), RHR, and EP systems in a PWR.

ACKNOWLEDGMENTS

The authors would like to thank Carl Johnson, Jr., Technical Monitor of the project and Millard Wohl of USNRC for their many insightful comments and suggestions in carrying out this research. We also thank the technical staff at Grand Gulf Nuclear Station for their willingness to support and help in obtaining very important plant-specific information. Specifically, we thank Kenneth Hughey and Emmett Roan of Entergy Operations, Inc. in this effort. The report benefitted from many discussions with all of the above individuals.

We appreciate the valuable comments from Gerald Andre, Westinghouse Electric Corp., Andy Dykes, PLG, Inc., William Vesely, SAIC, and Mikko Kosonen, TVO of Finland. We also acknowledge our colleague Jeanne Penoyar for her help in a number of computations, and J. Higgins, R. Hall, and L. Chu for their review of the report.

Finally, we thank Donna Storan for her excellent help in typing many versions of the report and preparing this manuscript.

1. INTRODUCTION

When safety systems fail during power operation, the action statements of technical specifications typically require that the plant transfer to a safer operational mode, e.g., cold shutdown, within the limits of allowed outage time (AOT). However, if the plant personnel can repair the equipment and restore its operability within the allowed outage time, then they may continue power operation. If they cannot, they must shut down the plant to comply with the action statements.

The action statements associated with the limiting conditions for operation (LCOs) of technical specifications are mostly based on engineering judgments. In general, the more serious the failure, and correspondingly, the higher the relative increase of the risk level, (e.g., multiple failures in important safety systems), the shorter is the allowed outage time. For particularly serious failures, the action statements require immediate plant shutdown.

However, in the special case where a system needed for safe shutdown is inoperable or degraded, shutting down the plant may not necessarily be preferable, from a risk perspective, to continuing power operation over a usual repair time. This concern arises because the plant may have a degraded capability to remove decay heat during shutdown. Besides the non-negligible risk of being in a shutdown state, an additional risk may be associated with changing the plant's state.

1.1 Objectives

The objectives of this study are to develop methods to evaluate the risk impact of technical specification action statements that require shutdown, to explore alternative approaches to the action statements, and to provide a technical basis for improvements. This report summarizes the results of the following tasks performed to meet those objectives:

(1) Define the methodology to evaluate the risk impact of action statements requiring shutdown, explicitly considering the shutdown risk.

(2) Apply the methodology to the residual heat removal (RHR) and standby service water (SSW) systems of a boiling water reactor (BWR) nuclear power plant.

(3) Evolve practical guidelines to improve the action statements for the RHR/SSW systems.

1.2 Approach

This study builds on work performed in Finland to resolve the AOT issue, i.e., the problem with those action statements requiring shutdown when the plant has insufficient capability to remove decay heat. This Finnish approach, called the risk-comparison approach,[1-3] is based on comparing the impacts on risk associated with basic operational alternatives in such a failure, i.e., continued operation and plant shutdown.

We applied this approach to RHR and SSW systems of a BWR, because the RHR system is the major means of removing decay heat from the primary system, and the SSW system subsequently removes heat from the RHR system. The reference plant selected was the Grand Gulf Nuclear Power Station in Port Gibson, Mississippi. This plant, which began commercial operation in July 1985, has a General Electric BWR/6 reactor with a Mark III containment.

1.3 Organization of the Report

Chapter 2 presents the basic concepts of the methodology to evaluate action statements requiring shutdown. Chapter 3 describes the RHR and SSW systems of the Grand Gulf plant, and the present action requirements for these systems, focusing on the AOTs.

Chapter 4 describes our approach to sequence modeling and risk quantification, including shutdown transient diagrams (STDs) and extended event sequence diagrams (EESDs) that we used to better model the shutdown cooling missions which challenge the systems needed for plant shutdown. The risks for the basic operational alternatives are compared in Chapter 5 with the assumptions for the LCO shutdown risk evaluations.

Chapter 6 discusses the sensitivity analyses to evaluate alternative operational procedures and presents insights for action requirements in the failure situations studied. Chapter 7 gives our recommendations on approaches to improving the action requirements, specifically for RHR/SSW systems of the Grand Gulf plant. The summary and conclusions of the study are given in Chapter 8, along with suggestions for future research.

This report has seven appendices. Appendix A lists the acronyms and initialisms used in this report. Appendix B describes the various operational modes of the RHR system in more detail, along with a brief description of the alternate decay heat removal system (ADHRS). Appendix C describes the LCOs and associated action statements defined in the current technical specifications of Grand Gulf for the RHR system and the ADHRS.

Appendix D describes the preparation of STDs for Grand Gulf, and derivation of associated data. The preparation of EESDs is discussed in Appendix E, focusing on the plant responses to the RHR challenge events. Appendix F outlines the heatup scenarios, i.e., the classification of the plant responses used to consider recovery from Near Mission Failure (NMF) states. A NMF state means a state where a critical safety function is lost and an undesirable consequence will occur if no recovery is made. Appendix G gives an example quantification of risk for selected sequences.

2. METHODOLOGY TO EVALUATE ACTION STATEMENTS REQUIRING SHUTDOWN

This chapter presents the basic concepts of the methodology we used to evaluate the LCOs and associated action statements requiring shutdown. Specifically, we describe: (1) the basic operational alternatives, i.e., continued operation or plant shutdown, available in failure or degradation of systems needed for a safe shutdown; (2) our approach to modeling and quantifying accident sequences in such LCO situations to assess the associated risk impacts; (3) the basic notion of comparing the LCO operating and shutdown risks to evaluate a prescribed AOT or to determine risk-effective action statements; and (4) other considerations needed in defining action requirements.

2.1 Basic Operational Alternatives: Shut Down the Plant or Continue Power Operation?

When a normally operating system, such as the reactor coolant system, malfunctions out of the tolerance limit, the plant may be shut down to go to a safer operational mode, e.g., hot shutdown or cold shutdown, which poses much less risk than staying at power. However, when a standby safety system needed to remove decay heat, such as the RHR system, is inoperable, we are faced with a decision: should we shut down the plant, or continue power operation with the RHR system out of service? Shutting down the plant may not necessarily be preferable, from a risk point of view, to continuing power operation over a usual repair time, and giving the repair priority.

Figure 2.1 shows the basic operational alternatives (i.e., continued operation or shutdown) for the example of all RHR trains being detected failed. Before the detection of failures in the RHR system, the plant was in baseline operation; namely, there were no known failures in the plant systems.

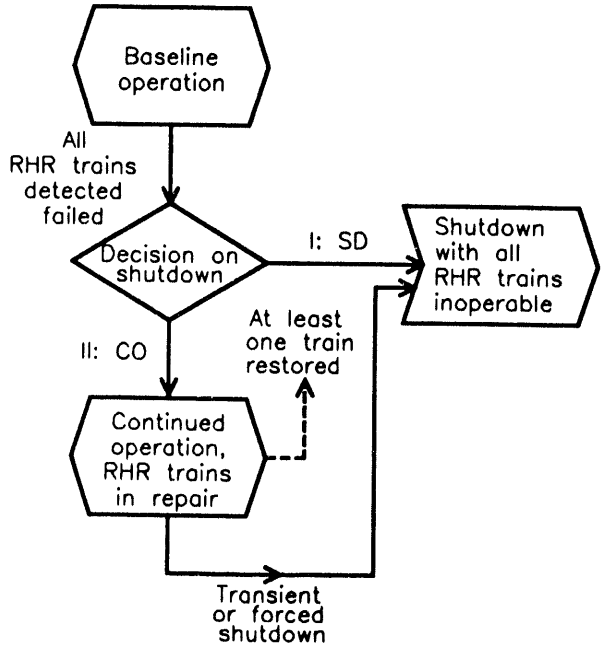


Figure 2.1. Basic operational alternatives in the case of all RHR trains being detected failed: shutdown (SD) and continued operation (CO)

If the shutdown alternative is taken, the plant will be vulnerable to transients that may occur during the transition to shutdown state, because of insufficient capability of removing decay heat. However, if the continued-operation alternative is taken, the plant may not have to be shut down, although there is a possibility of a transient occurring during the repair time and forcing a shutdown with all the RHR trains inoperable. In general, the likelihood of a transient occurring during a mean repair time is typically less than 1%.

2.2 Assessment of the LCO Operating and Shutdown Risks

For a risk-based evaluation of the basic operational alternatives in failure or degradation of systems needed for shutdown, we first should assess the risks associated with the alternatives. The risk associated with continuing power operation with the equipment inoperable will be called "LCO operating risk." This risk is incurred by the initiating events that may occur while the plant remains at power. The risk associated with shutting down the plant with the equipment inoperable will be called "LCO shutdown risk." This risk is incurred by the initiators occurring while the plant is being brought to shutdown or while in the shutdown mode.

Only the LCO operating risk was explicitly considered in a previous study to evaluate plant-specific AOTs,[4] and in the feasibility studies for a configuration control system[5,6] which can generate an AOT for a given configuration in real or semi-real time. Consideration of only the LCO operating risk will be adequate when the LCO shutdown risk is judged to be relatively small. However, recent studies of probabilistic safety analysis (PSA) on the low-power and shutdown stages of plant operation[7-12] suggest that the risk of shutdown is not insignificant when compared to the risk of full-power operation. For example, the PSA of potential safety problems during shutdown conditions at the Zion nuclear power plant concludes that the annual risk of core damage from events initiating during shutdown is less, only by a factor of 5 to 20, than the risk of core damage from transients initiated at power.[12] Furthermore, the LCO shutdown risk also includes the risk associated with the changes in state during power reduction and the evolution of shutdown. Thus, for failures of standby safety systems required for shutdown, the LCO shutdown risk can be significant, and should be evaluated to determine action requirements in such conditions.

This section describes the basic concepts of the approach to modeling and quantifying accident sequences for failures in safety systems. This approach, which was originally developed in Finland while re-evaluating AOTs for the RHR system of the Teollisuuden Voima Oy (TVO) nuclear plant, allows assessing both the LCO operating and shutdown risks.[1]

Sequence Modeling

The risk-comparison approach to analyzing operational alternatives[1-3] models accident sequences using extended event sequence diagrams (EESDs) with embedded state submodels. The development of EESDs as a new sequence-modeling tool evolved from the recognition of the need for realistic, time-dependent risk quantification encountered in modeling shutdown-related transients, and for the consideration of operational alternatives in failure situations of standby safety systems.

The EESD model is an extended variant of event sequence diagrams (ESDs). These diagrams have matured from safe shutdown logic diagrams (SSLDs), and subsequently, from sequence of events diagrams (SEDs) both of which were used to define the systems responding to accomplish safety functions and their order of actuation following an initiating event.[13] ESDs are sometimes used in PSAs as part of the event sequence analysis to identify complex relationships between initiating events and

detailed system responses. Recently, another variant of ESDs, called functional event sequences diagrams (FESDs),[14] was used as an aid in identifying recovery options and priorities, as well as the potential for failure to achieve recovery.

An EESD is composed of several symbols shown in Figure 2.2. The central feature of this variant of ESD is the inclusion of a process state block to describe temporary or stable system/plant states; the original ESD contained only an activation event block. The rectangular block is reserved for activation events, whose failure exit is quantified by a conditional probability. The state block is used for intermediate or stable states, whose failure exits are quantified by conditional transition rates. The time lag between "enter" and "exit" events of a state block may be substantial, whereas, in an activation block, this time difference is negligible.

To enhance the process or operational analogy, the EESD is arranged such that: (1) success flows from left to right; (2) failure flows from top to bottom towards undesired conditions; and (3) recovery from failures rises up back to safer conditions. This layout provides a well-structured "map" of the success and failure paths.

The merits of EESDs in modeling dynamic sequences are summarized below, especially as compared to the conventional event tree-fault tree technique:

(1) The EESD is comparable to the event tree, but allows more descriptive sequence modeling, including intermediate plant states, and also backward looping.

(2) In the event tree/fault tree approach, recovery is typically accounted for in cutsets, from which the analyst must infer the chronological sequences and situational contexts. The EESD facilitates incorporation of recovery options (from operators' actions or equipment restoration) within the model e.g., by establishing the context for operators' actions.

(3) The EESD improves the documentation of assumptions and other relevant items in the model itself, because of its sequence-by-sequence representation. Also, it is easier for the staff to review the plant's response to a given initiating event on a sequence-by-sequence basis; the expert opinion and input from their review can be incorporated in the model.

(4) The process-oriented approach of the EESD, with embedded state submodels, allows the incorporation of realistic phase durations, e.g., stochastic repair time distribution of failed components or suppression pool heatup time providing time margin for restoration of near mission failure states.

However, using EESDs to model sequences may overwhelm the user, because of 1) the explicit representation of many success/failure paths, and 2) the elaborate consideration of all potential recovery options and their incorporation in the models. Hence, the resolution of analysis should be limited to an appropriate level, such as a system or subsystem.

Sequence Quantification

We will describe here the formulation of the fundamental equations to quantify the event sequences from EESDs. Chapter 4 has more accounts of the principal features of this risk quantification approach.

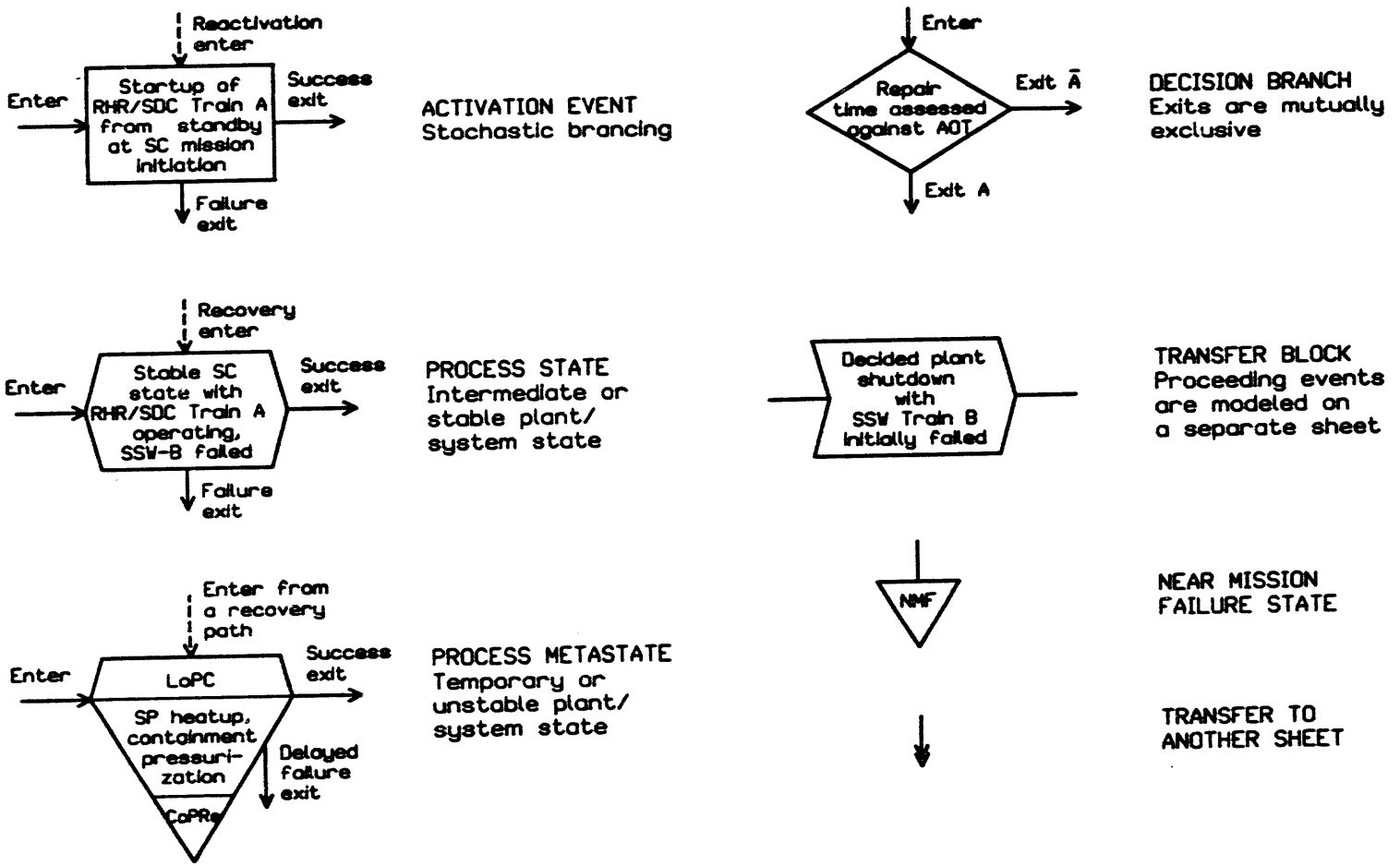


Figure 2.2. Basic symbols of extended event sequence diagram (EESD)

Let

$pmp(i)$ = total mission failure probability for a given initiating event, i, of shutdown cooling (ISC)

= P {mission failure | initiating event i}

The frequency of the undesirable end state, i.e., core damage, for the continued-operation alternative can then be obtained by:

$$f_{CO} = \sum_i f_{ISC/CO}(i) * pmp(i)$$

where the summation is over all the initiating events of shutdown cooling and,

f_{CO} = core-damage frequency for the continued-operation alternative

$f_{ISC/CO}(i)$ = frequency of an initiating event, i, of shutdown cooling

Then, we can estimate the expected core-damage probability for the continued-operation alternative, R_{CO}:

$$R_{CO} = f_{CO} * a_{mean}$$

where a_{mean} denotes the mean repair time that can be estimated from the distribution of repair time for the initially failed equipment. We will call R_{CO} expected risk per failure situation for CO alternative.

Similarly, we can obtain the expected probability of core damage for the shutdown alternative, R_{SD}:

$$R_{SD} = \sum_i P_{ISC|SD}(i) * pmp(i)$$

where the summation is, again, over all initiating events and

$P_{ISC|SD}(i)$ = probability that an initiating event, i, will occur during the mission phase for the SD alternative

We will call R_{SD} expected risk per failure situation for SD alternative.

The total mission failure probability for an initiating event, i, requiring shutdown cooling can be assessed using the following expression:

$$pmp(i) = pch(i) + \int_{a=o}^{\infty} da * fsc(i,a) * prs(a)$$

where,

$pch(i)$ = probability of mission failure at the start of shutdown cooling

$fsc(i,a)$ = frequency of mission failure during the shutdown cooling period at time a

prs(a) = probability of non-recovery from the initial repair state up to time a

In the expressions above, the total mission failure probability for a given initiating event of shutdown cooling, i.e., pmp(i), as well as the risk variables, f_{CO}, R_{CO}, and R_{SD}, are all conditional on a given initial failure situation, which is the main subject in the AOT evaluations. However, the given failure situation is not explicitly indicated in the expressions for simplicity. Appendix G presents example risk quantifications using these equations.

2.3 Comparison of LCO Operating and Shutdown Risks

Given a failure in safety systems, we can assess the LCO operating and shutdown risks, following the method discussed in the previous section. These results then can be used to evaluate a prescribed AOT or to determine risk-effective LCO action statements.

Figure 2.3 shows a conceptual plot of instantaneous risk frequency for the failure of a safety system which is needed for a safe shutdown. At time A when the failure is detected, there are two basic operational alternatives, i.e., continued operation and plant shutdown. The solid line represents the risk profile for the continued-operation alternative, while the dotted line is the profile for the shutdown alternative.

Figure 2.3 shows that, upon detection of the failure at time A, the LCO operating risk increases above the baseline risk level. This is due to the increased unavailability of the initially affected (i.e., failed or degraded) system during potential occurrences of accident scenarios which require the system to be operational to prevent core damage. Traditionally, the action statements of technical specifications were based on a subjective consideration of only the LCO operating risk levels, as we discussed in the previous section.

The peak in the LCO shutdown risk shown in Figure 2.3 results from the system's unavailability during the potential occurrences of accident scenarios which are initiated by events occurring while the plant is being brought to shutdown. Specifically, the risk peak in the initial stage of shutdown arises from: 1) the unreliability of the systems which are needed during the change in plant state or which must be started up, and 2) the vulnerability of the plant to transients caused by the changes in state. After entering a stable shutdown state, the risk level usually decreases with time because of the diminishing decay heat, meaning lower capacity requirements on safety systems and longer time available for recovery if a critical safety function is lost during shutdown-cooling mission. Obtaining a lower risk level in stable shutdown mode, as compared to the continued-operation alternative, is the principal motivation of going to shutdown.

At time B, when the component is repaired and returned to service, both operating and shutdown risks decrease. The operating risk decreases to the baseline risk level, i.e., the level before the failure detection, whereas the shutdown risk decreases below the baseline risk level for the power operational mode, because of the much lower rate of heat production in the reactor during shutdown, compared to power operation. Another small peak in the shutdown risk at time C arises from the unavailabilities of systems that are needed when the plant is restarted up, and the plant's vulnerability to transients that may be caused by the change in the operational mode.

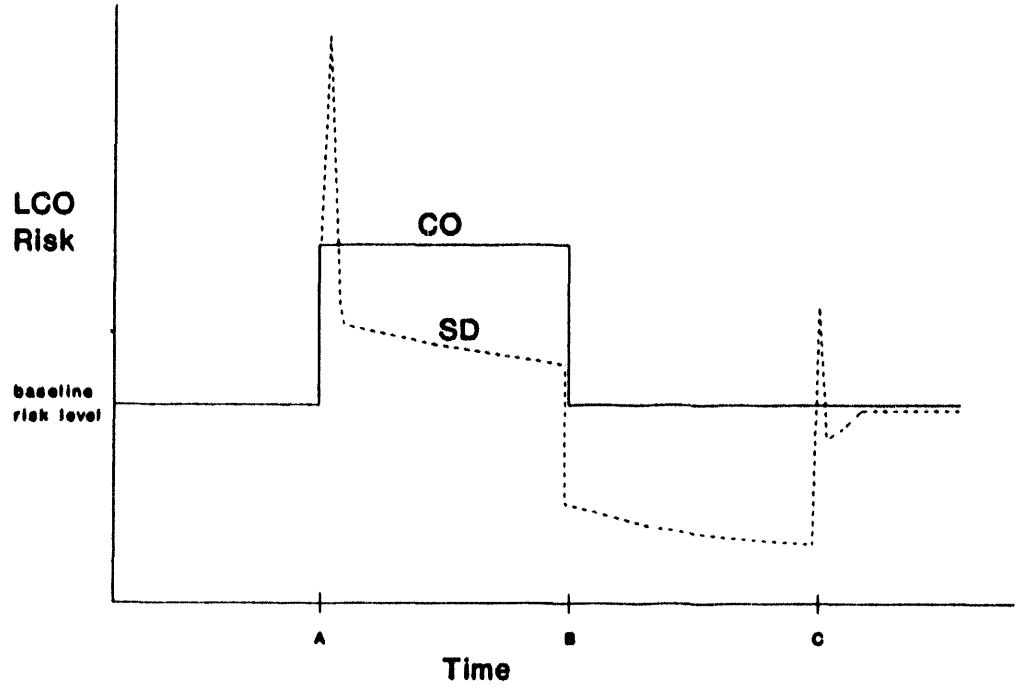


Figure 2.3. Profiles of instantaneous risks for basic operational alternatives with the assumption of non-delayed shutdown following the detection of failure (The solid line is for continued operation; A = failure detection, and B = completion of equipment repair. The dotted line is for shutdown; A = failure detection and immediate shutdown, B = completion of equipment repair, and C = re-startup of the plant.)

The period, which is directly relevant to the evaluation of action requirements or AOTs, is from time A to time B, i.e., the predicted or actual component repair time. We can assess the cumulative AOT operating and shutdown risks by integrating the instantaneous risks over this period. If the cumulative operating risk is smaller than the cumulative shutdown risk, then the alternative of continued operation is preferable, from a risk point of view, to the shutdown alternative, and vice versa.

Figure 2.4 shows a plot of the cumulative LCO operating and shutdown risks versus repair time, beginning from time A, i.e., the time when the failure is detected. This figure is based on the information in Figure 2.3. The cumulative operating risk is smaller than the cumulative shutdown risk, until time X, when the two curves intersect. Therefore, from the viewpoint of quantitative risk, we conclude that it is more beneficial to continue power operation than to shut down the plant if the operability of the initially affected system can be restored before time X. Where the repair takes longer than the period of A to X, it is advisable to shutdown the plant. However, we also should take into account other considerations, such as uncertainties in the risk evaluations, the timing of shutdown, and the testing of redundant trains. These considerations will be discussed later in the report.

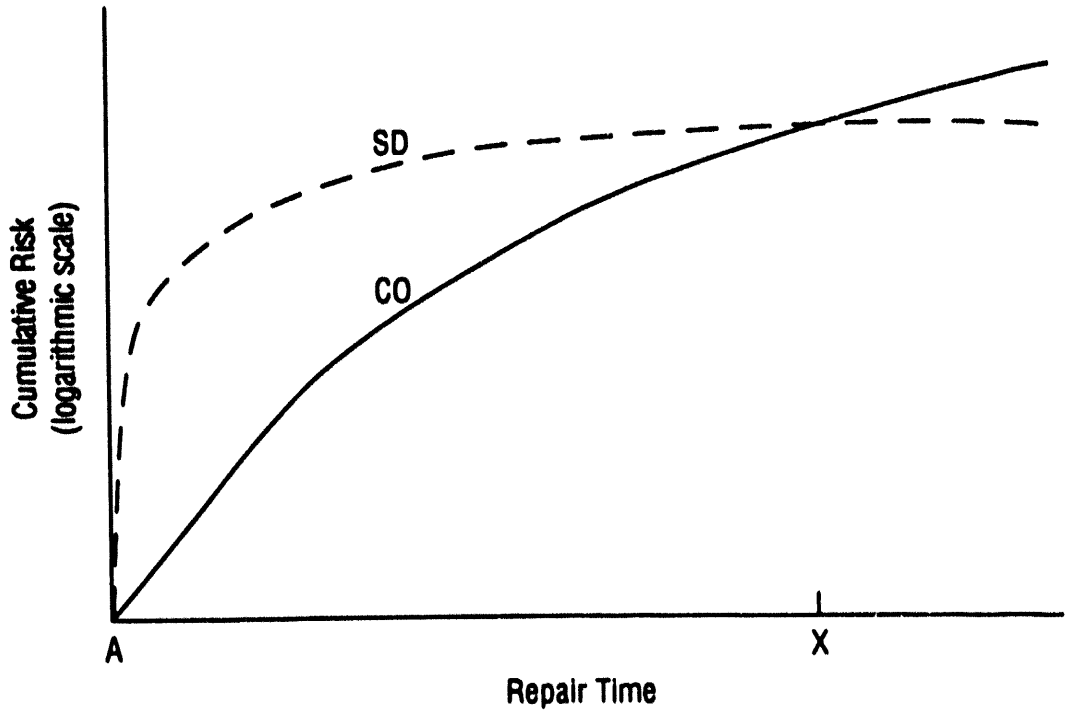


Figure 2.4. Cumulative risk over predicted repair time for the basic operational alternatives. (The solid line is for the continued-operation alternative, and the dotted line for the shutdown alternative).

2.4 Other Considerations in Defining Action Requirements

The example risk profiles discussed in the previous section are based on several assumptions. An important assumption was that, in the case of shutdown alternative, the plant is shut down directly after the failure detection. However, some AOT may be given, in general, so that the plant personnel can evaluate the repair measures needed, to try to restore the operability of the failed equipment at least for the shorter repairs without shutting down the plant.

Suppose that 3 days of AOT is given for a failure situation in the technical specificaitons and the plant personnel cannot repair the component within the AOT. As a result, they may shut down the plant three days after the failure detection. In this case, the failure will incur LCO operating risk during the period between the failure detection and the time when the shutdown is initiated, and also LCO shutdown risk. As compared to the plant shutdown just after the failure detection, this case will incur larger risk by the risk accumulated before the plant is actually shut down. Hence, the timing of shutdown should be considered in determining risk-effective action requirements that will minimize the total risk impact associated with a given failure situation.

Another assumption made in the previous section was that the failed component is repaired at the same time regardless of whether the continued operation alternative is taken or the shutdown alternative is taken. In a real situation where the shutdown should be taken, attention may have to be

paid to shutdown operations, delaying the repair of the failed component until a certain plant state, e.g., cold shutdown, is reached. In this case, the predicted repair time will be longer for the shutdown alternative than for the continued operation alternative.

Furthermore, we oftentimes do not know exactly how long the repair of certain failures will take. The distribution of repair time should be taken into account in assessing the cumulative risk associated with the failures. In addition to the timing of shutdown and the repair time, there are also other considerations that should be taken into account in determining risk-effective action requirements, e.g., whether the status of redundant train(s) should be checked or not, and whether the plant should go to hot shutdown or cold shutdown as the optimum target state of plant shutdown. All these will be considered later in the report.

3. PILOT APPLICATION TO THE RHR/SSW SYSTEMS AND PRESENT ACTION REQUIREMENTS

In this pilot study, the Grand Gulf Nuclear Power Station was chosen as the reference plant. This section briefly describes the residual heat removal (RHR) and standby service water (SSW) systems of the plant, along with the present action requirements defined for these systems in the plant's technical specifications.

3.1 Description of the Grand Gulf RHR and SSW Systems

The Grand Gulf plant is a General Electric BWR/6 unit of 1250 MWe capacity housed in a Mark III containment. This plant was chosen as a reference plant mainly because of the availability of PSAs, i.e., low-power and shutdown PSA as well as full-power PSA. Although our methodology can be performed without such PSAs, the sequence modeling and quantification for AOT risk evaluations were greatly facilitated by the analyses of the PSA studies to estimate the average plant risks. The PSA for full-power operation[15] was performed as a part of the NUREG-1150 study, and the PSA for low-power and shutdown[7,8] is underway at Sandia National Laboratories.

Figure 3.1 shows the flow paths of major safety systems of the Grand Gulf plant, including the coolant-injection flow paths of the coolant supply systems, and the paths for decay-heat removal of the RHR and SSW systems. The coolant injection systems are grouped into the high pressure mode (HPM) and low pressure mode (LPM). One important characteristic of the Grand Gulf plant design and operation is the redundancy and diversity of coolant supply systems, as shown in the figure; e.g., the firewater system can be used for coolant makeup and the condensate system as an LPM system.

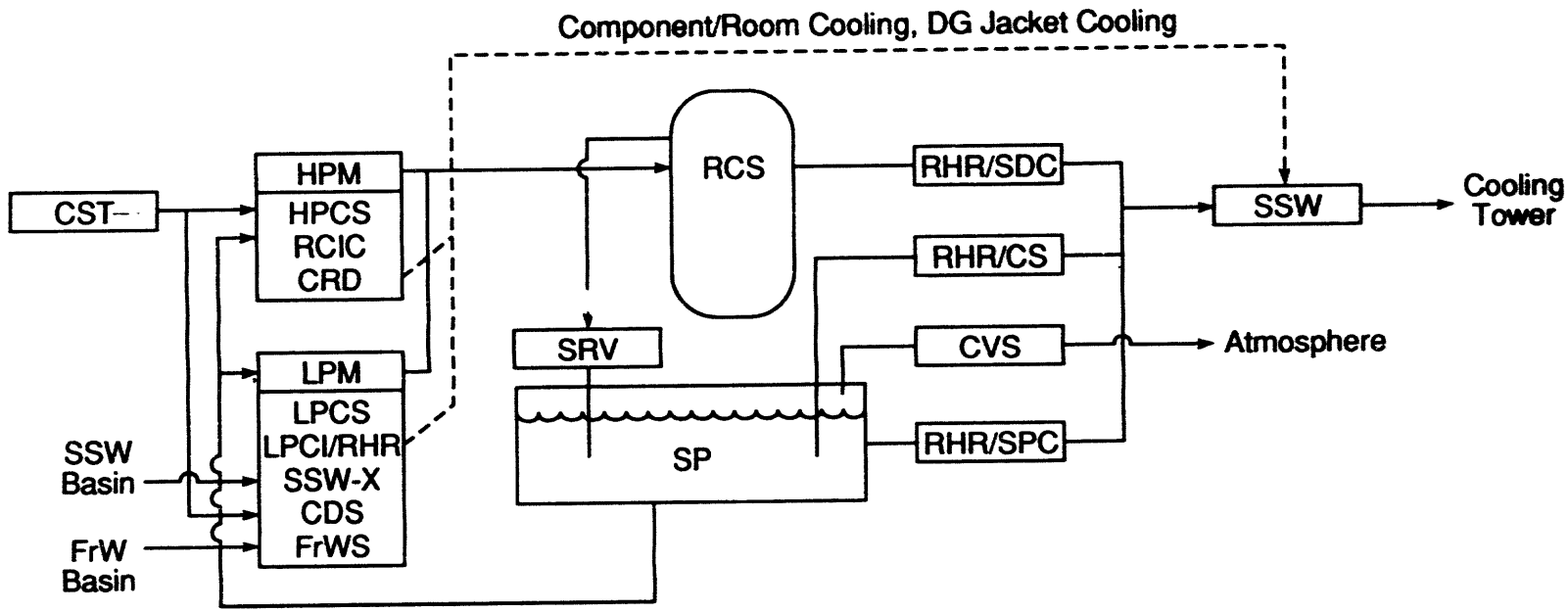
Description of the RHR System

The residual heat removal (RHR) system consists of three subsystems, A, B, and C. Subsystems A and B each has a motor-driven pump, motor-operated valves, and heat exchangers, whereas subsystem C has only a motor-driven pump and motor-operated valves, i.e., no heat exchangers. (See Figure B.1 of Appendix B for a schematic of the RHR system.)

The RHR system can be operated in several modes: shutdown cooling (SDC), suppression pool cooling (SPC), containment spray (CS), and low pressure coolant injection (LPCI). Figure 3.1 shows simplified flow paths for these modes.

Only subsystems A and B can be used for ordinary RHR modes, i.e., SDC, SPC, and CS modes, because they require the operation of heat exchangers to remove heat. The SDC mode removes heat from the reactor, the SPC mode from the suppression pool, and the CS mode from the containment. The third subsystem without heat exchangers, i.e., subsystem C, is dedicated only to the LPCI mode.

During normal power operation, all the subsystems of the RHR system are placed in the LPCI mode to cope with a loss of coolant accident (LOCA). The SDC mode can be used to remove decay heat from the reactor during shutdown evolution (primarily cold shutdown) following a controlled shutdown or a transient initiator. The reactor pressure should be less than 135 psig for the operation of the SDC mode. The SPC mode is activated by the operator, according to the plant operating procedure, whenever the suppression pool reaches 95°F. This mode is used in the case of loss of power conversion system to remove heat which is released from the reactor coolant system to the suppression pool. The CS mode is initiated by a high containment pressure (if containment pressure is +9 psig and



Acronyms:

CDS	Condensate System
CRD	Control Rod Drive System
CST	Condensate Storage Tank
CVS	Containment Venting System
DG	Diesel Generator
FrW	Firewater
FrWS	Firewater System
HPCS	High Pressure Core Spray System
HPM	High Pressure Mode
LPCI/RHR	Low Pressure Coolant Injection Mode of the RHR System
LPCS	Low Pressure Core Spray System
LPM	Low Pressure Mode
RCIC	Reactor Core Isolation Cooling System
RCS	Reactor Coolant System
RHR	Residual Heat Removal System
RHR/CS	Containment Spray Mode of the RHR System
RHR/SDC	Shutdown Cooling Mode of the RHR System
RHR/SPC	Suppression Pool Cooling Mode of the RHR System
SP	Suppression Pool
SRV	Safety Relief Valves
SSW	Standby Service Water System
SSW-X	Standby Service Water Cross-Tie System

Figure 3.1. Simplified schematic of safety-system flow paths at Grand Gulf

drywell pressure is +2 psig). Actuation of the CS mode closes the LPCI injection valves on subsystems A and B, and opens the CS spray valves on subsystems A and B. However, subsystem C will stay in the LPCI mode, since this subsystem is dedicated only to coolant injection.

Appendix B describes the various modes of the RHR system in more detail, with the alternate decay heat removal system (ADHRS) that can be used to remove decay heat during cold shutdown and refueling, i.e., when the reactor's temperature is less than 200°F.

Description of the SSW System

The SSW system removes heat from plant equipment that require cooling water for a safe reactor shutdown. As such, the SSW system removes heat from the RHR heat exchangers to the ultimate heat sink, i.e., the SSW cooling tower basins, when the RHR system is used in a SDC, SPC, or CS mode. The simplified flow paths are shown in Figure 3.1.

The SSW system consists of three subsystems, A, B, and C. Each subsystem has a motor-driven pump, motor-operated valves, and heat exchangers. SSW pump A of subsystem A and SSW pump B of subsystem B each has a 12,000 gpm capacity. SSW pump C of subsystem C, which is dedicated to the high pressure core spray (HPCS) system, has a 1300 gpm capacity.

The specific SSW cooling loads are:

1) SSW subsystem A: RHR A heat-exchanger coolers, RHR A room/pump coolers, room cooler for the low-pressure core-spray (LPCS) system, room cooler for the reactor-core-isolation cooling (RCIC) system, and diesel generator (DG) A jacket cooler

2) SSW subsystem B: RHR B heat-exchanger coolers, RHR B room/pump coolers, RHR C room/pump coolers, and DG B jacket cooler

3) SSW subsystem C: HPCS room cooler and DG C jacket cooler

Hence, a failure or degradation in the SSW system will affect the operability of other systems which are supported by the SSW system. For example, the failure of SSW subsystem A also will fail RHR subsystem A and DG subsystem A along with front-line systems, LPCS and RCIC.

3.2 Present Action Requirements for the RHR and SSW Systems

Technical specifications define LCOs (including action statements and AOTs) for various plant operational modes, i.e., power operation, startup, hot shutdown, and cold shutdown. We are primarily concerned with LCOs for the power operation mode, because these LCOs contain the action statements requiring shutdown from power operation.

This section summarizes the action requirements for the RHR and SSW systems defined in the Grand Gulf technical specifications[16] as applicable to the power operation mode. Appendix C gives a more detailed description of LCOs for the RHR system, including those for other plant operational modes, and also a description of LCOs relevant to the alternate decay heat removal system (ADHRS).

Action Requirements for the RHR System

Table 3.1 summarizes the action requirements for the RHR system which are applicable to the power operation mode; no action requirement for the RHR/SDC mode is specified in the technical specifications, and therefore, this system is not included in the table. The reason for this lack of requirement for the power operation state is that this system is used to remove decay heat from the reactor only when its pressure remains low, i.e., less than 135 psig.

In a single failure of the LPCI system, i.e, where one of the LPCI subsystems is down, its operability should be restored within 7 days, or the plant should be in, at least, hot shutdown within the next 12 hours and in cold shutdown within the following 24 hours. For double-failures, 3 days of AOT is given. However, in a triple failure, the plant should comply with LCO Specification 3.0.3 which states:

> When an LCO is not met, except as provided in the associated action requirements, within one hour action shall be initiated to place the unit in an operational condition in which the Specification does not apply by placing it, as applicable, in: (1) at least startup within the next 6 hours; (2) at least hot shutdown within the following 6 hours; and (3) at least cold shutdown within the subsequent 24 hours.

Table 3.1. Action Requirements for the RHR System Applicable to the Power Operation Mode

RHR Operational Mode	Inoperable Subsystems	AOT	LCO Specification
LPCI	A, B, or C	7 days	3.5.1
LPCI	A&B, A&C, or B&C*	3 days	3.5.1
LPCI	A,B, and C*	0 hours	3.0.3
SPC	A or B	3 days	3.6.3.3
SPC	A and B**	8 hours	3.6.3.3
CS	A or B	3 days	3.6.3.2
CS	A and B**	8 hours	3.6.3.2

*Whenever two or more RHR subsystems are inoperable, if cold shutdown cannot be attained as required by this action, maintain reactor coolant temperature as low as practical by using alternate methods of heat removal.

**Whenever both RHR subsystems are inoperable, if cold shutdown cannot be attained as required by this action, maintain reactor coolant temperature as low as practical by alternate methods of heat removal.

For the SPC mode, 3 days are given for the single failure situation, i.e., where either of the two subsystems is inoperable, and 8 hours are given in double failures, i.e., where both subsystems are down. For the CS mode, the action requirements are the same as for the SPC mode.

Action Requirements for the SSW System

The SSW system consists of three subsystems (A, B, and C), as previously described. Among these, subsystem C is different in that its capacity is much lower than that of the other two subsystems and dedicated only to the HPCS system.

Table 3.2 summarizes the action requirements for the SSW system which are applicable to the power operation mode. For the SSW subsystems A and B, LCO Specification 3.7.1.1 defines 3 days of AOT for a single failure (i.e., where either SSW subsystem A or B is inoperable). For a double failure, i.e., where both SSW subsystems A and B are down, the specification requires "immediate" plant shutdown; the plant should be in, at least, hot shutdown within the next 12 hours and in cold shutdown within the following 24 hours.

Table 3.2. Action Requirements for the SSW System Applicable to the Power Operational Mode

Inoperable SSW Subsystems	AOT	LCO Specification
A or B	3 days	3.7.1.1
C	3 days	3.7.1.2 (3.5.1 and 3.8.1.1)
A and C	3 days	3.7.1.1 and 3.7.1.2
B and C	3 days	3.7.1.1 and 3.7.1.2
A and B*	0 hours	3.7.1.1
A, B, and C*	0 hours	3.7.1.1 and 3.7.1.2

*Whenever both SSW subsystems (A and B) are inoperable, if cold shutdown cannot be attained as required by this action, reactor coolant temperature should be kept as low as practical by using alternate methods of heat removal methods.

The action statement for the HPCS-dedicated SSW system, i.e., the SSW subsystem C, is contained in Specification 3.7.1.2. When the SSW subsystem C is inoperable, this specification requires that the HPCS system be declared inoperable and the action required by Specification 3.5.1 be taken, and that the associated diesel be declared inoperable and the action required by Specification 3.8.1.1 be taken. Specification 3.5.1 for emergency core cooling water (ECCS) systems gives 14 days of AOT when the HPCS system is inoperable. Specification 3.8.1.1 for AC power sources gives 3 days of AOT when the DG subsystem C is inoperable. Therefore, the plant's technical specifications gives 3 days of AOT when the SSW subsystem C is inoperable.

For double failures of the SSW system, different AOTs are given in the technical specifications, depending on which subsystems are inoperable. When SSW trains A and C, or B and C are down, the plant may continue power operation with the equipment inoperable up to 3 days. With SSW subsystems A and B inoperable (Specification 3.7.1.1), and with all SSW trains down (triple failures) the plant should be in, at least, hot shutdown within the next 12 hours and in cold shutdown within the following 24 hours.

4. MODELING OF SHUTDOWN COOLING MISSIONS

This chapter summarizes the event-sequence models developed to analyze shutdown cooling missions for various operational options challenging decay heat removal capabilities of the plant. The focus will be on conveying the conceptual aspects of our risk-modeling approach, pinpointing the differences with conventional approaches, such as the fault tree-event tree of a typical PSA. The methodological details and representative models are described in Appendices D, E, and F.

4.1 General Summary of Modeling Approach

The key target in the risk-comparison approach is to consistently evaluate the credit from the diminishing decay heat production when going to plant shutdown, because this is the principal motivation for an LCO shutdown. Besides, the likelihood of accident initiators and system configurations do vary in different shutdown states. These features have necessitated the development of a method for time-dependent analysis of accident sequences, which is based on the concepts of state-transition model and phased mission analysis.

The major steps of the risk-comparison approach are structured in Figure 4.1, showing also the main relationships between the analysis tasks. More details of the methodology are presented in references 1 and 2.

4.1.1 Phased Mission Approach

The LCO shutdown includes shutdown cooling (SC) phase, during which the power conversion system is idle and the normal SC system, i.e., RHR/SDC, is used for decay heat removal. If RHR/SSW trains are initially degraded, the plant is vulnerable with respect to entering SC phase and during the SC mission.

In the shutdown alternative, the SC mission will be intentionally undertaken for the time of repair, in the nominal LCO shutdown scheme with cold shutdown as target state. In the continued operation alternative, the SC mission may be forced by a transient initiator occurring, or also because of some special shutdown need arising, during the repair time in the power operation state. Thus, the consideration of the SC mission, as well as the evaluation of the credit from the diminishing decay heat production while in zero power state, applies to both operational alternatives in a specific way.

4.1.2 Time-Dependent Analysis

The diminishing decay heat production during shutdown states implies that, in a critical failure situation, called Near Mission Failure (NMF) state, the time margin available for recovery actions increases as the function of time elapsed following the entry into the zero power state. The time margin can be considered for different types of heatup situations such as: (1) heatup of suppression pool, when the normal RHR function is lost, (2) decrease in water level in the reactor vessel, when the coolant supply function is lost, and (3) heatup of a component, when the component or room cooling is lost. These different situations are categorized into several heatup scenarios, and then, the accident sequences are associated with the relevant heatup scenarios for quantification of the sequences.

There are also other time-dependencies explicitly taken into account in the risk-comparison approach; e.g., the influence of the passed tests of standby components, or the state of initially operating components, which may significantly contribute to the risk comparison of operational alternatives.

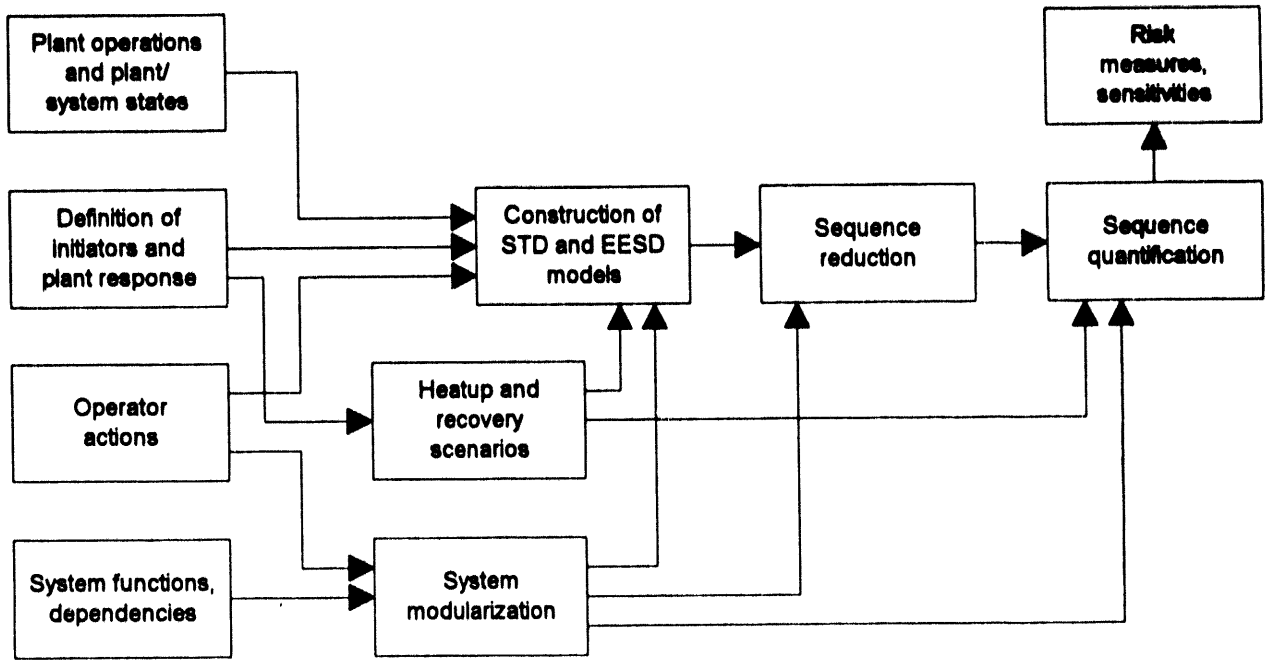


Figure 4.1 Major steps of phased mission analysis in the risk-comparison approach

4.1.3 Modeling of Event Sequences

The most essential methodological development is concerned with the use of extended event sequence diagram (EESD) for the description of event sequences, as a replacement for the traditional event tree-fault tree approach. EESD incorporates intermediate and stable process states as embedded. This enhances modeling of system state and time-dependent event scenarios, and allows description of the recovery paths in parallel to success and failure paths, within the same model frame. Despite the essential differences, there are still much similarity with the standard PSA modeling, and existing event tree-fault tree models are of great help in the construction of EESDs.

Quantification of event sequences, reduced from the EESD model, has a connection with the underlying SC mission. Both transition probabilities and rates are calculated in the form of (1) failure probability at the beginning of the SC phase, including failures of standby systems to start, and (2) failure rate during the SC mission, including failures of operating systems to run. These two type of variables are then combined, when deriving integrated and expected risk variables over the SC mission.

4.1.4 Data needs

Input data needed for sequence quantification in the risk-comparison approach is, to a large extent, similar to those required in a standard level-1 PSA. Additional, special data are needed for the likelihood of disturbance transients during a controlled shutdown, and for the repair and recovery time

distributions. Also specific physical data are needed to derive available time margins for the heatup/recovery scenarios (Appendix F).

4.2 Shutdown Transient Diagram

Shutdown transient diagrams (STDs) are used at the highest level of the modeling hierarchy to describe:

- Initiating events for power operation state, i.e., for the alternative of continued operation over repair time
- Disturbance transients during a controlled shutdown (the decided shutdown, i.e., DecSD, branch in Figure 4.2), corresponding either with a forced, controlled shutdown in the continued operation alternative, or with the decided SD alternative in an LCO situation

In the continued operation alternative, the initiating events for full power operation state are called initiating transient events (ITRs). If an ITR occurs during full-power operation, the plant will then be shut down, entering shutdown cooling (SC) mission phase with the failed equipment unavailable. This SC mission phase is of particular importance in this study, because the plant will become vulnerable during this phase as a result of the insufficient decay heat removal capabilities. In the LCO shutdown alternative, the plant will go to shutdown even if no ITR occurs. However, a transient may occur during power reduction and reactor cooldown stages. The STDs for both alternatives, i.e., continued operation and controlled LCO shutdown, are drawn until the initiating events of shutdown cooling (ISC) are encountered.

Figures 4.2 and 4.3 show STDs for full-power operation state and controlled LCO shutdown, respectively. The STD for full-power state (Figure 4.2) also contains an exit branch, DecSD, for completeness and consistency with the LCO shutdown model (Figure 4.3). Appendix D describes screening of initiating events, modeling details, and derivation of transition frequencies and probabilities between events or states.

AOT considerations are aimed at comparing relative risks associated with a failure, i.e., the risk of continued operation over repair time versus the risk associated with transition to plant shutdown. Therefore, different types of simplifications in modeling initiators, often stronger than in probabilistic safety analyses (PSAs), are acceptable.

In general, the initiating events of the PSA for Grand Gulf (GG/PSA) are retained, but in a failure situation of RHR systems, the relative importance of initiating events may substantially differ from those in the PSA which estimates the contributions to average risk. In particular, those initiating events, where the RHR function is an essential part of the plant's response, increase in importance.

For instance, the initiating events, which are Common Cause Initiators (CCIs) of RHR function, i.e. which directly challenge the function of, and render part of, the RHR systems unavailable, may increase drastically in relative importance, if it is assumed that some part of the RHR systems is known to be initially failed. Examples of these CCIs are the loss of offsite power (LOSP), the loss of power conversion system (PCS), and the loss of instrument air system (IAS) which causes unavailability of the PCS. These initiators are well-handled in the GG/PSA, thereby, enhancing the modeling work in this study.

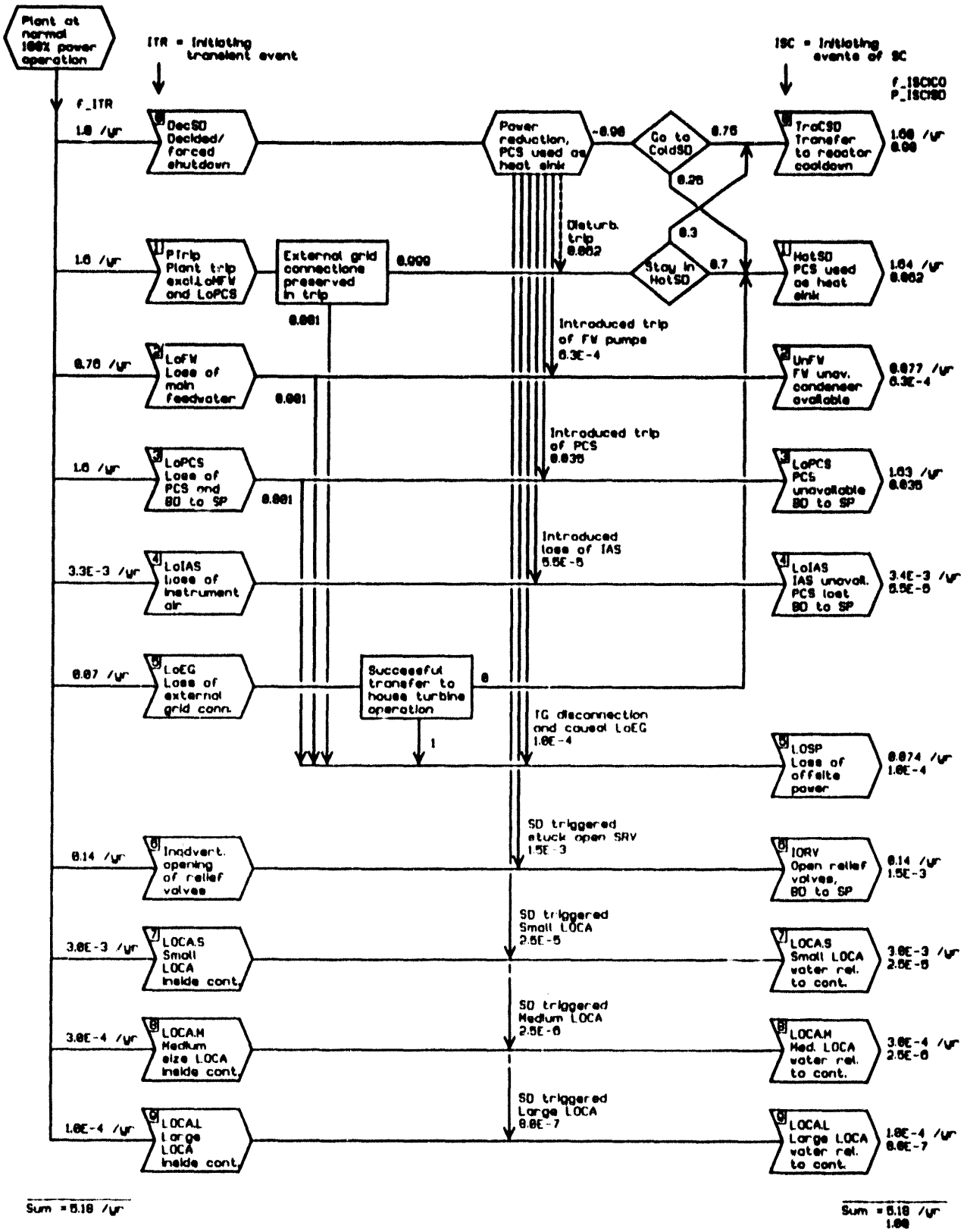


Figure 4.2 Shutdown transient diagram for full power operation state

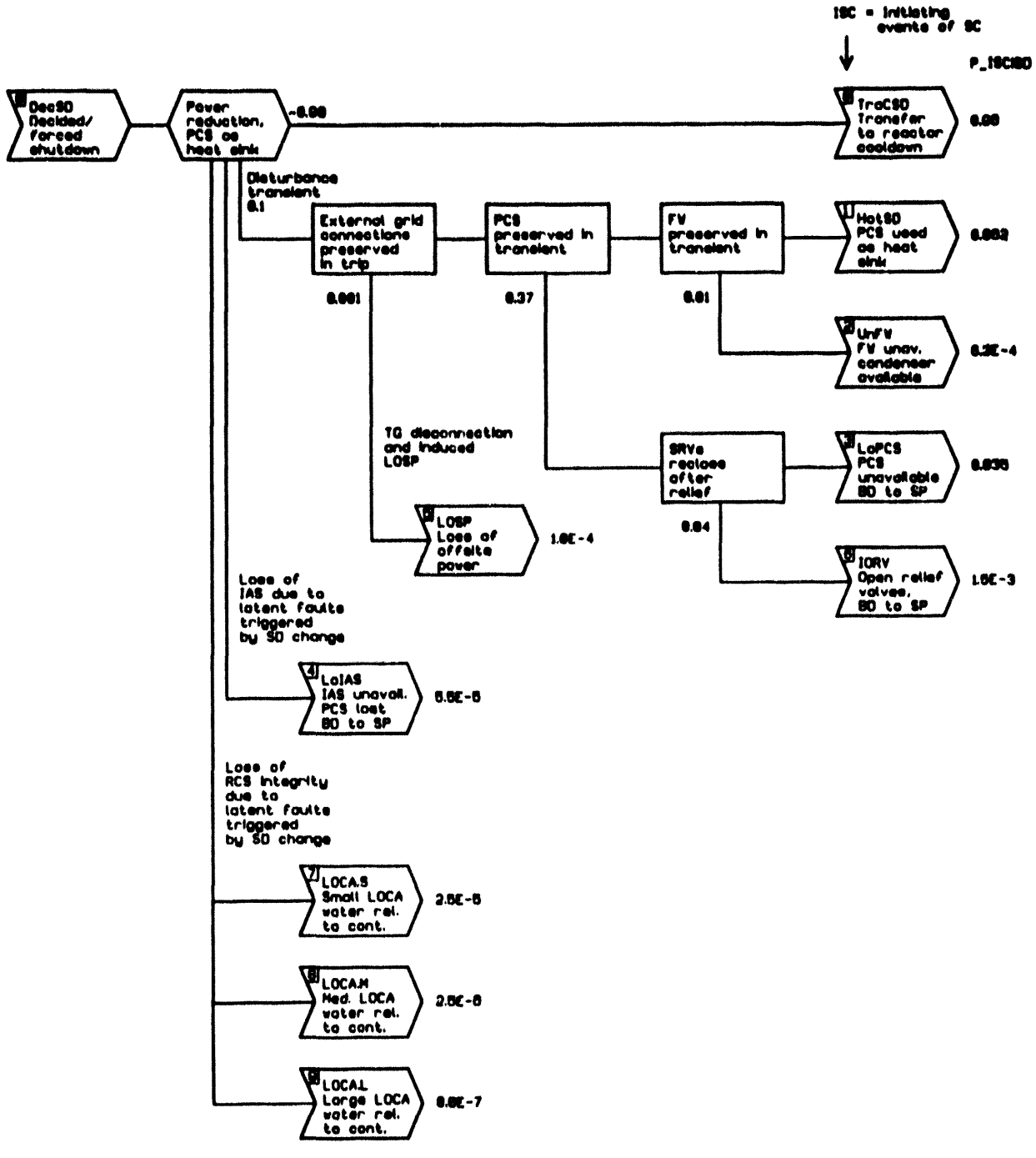


Figure 4.3 Shutdown transient diagram for controlled LCO shutdown

4.3 Shutdown Cooling Phases

Table 4.1 defines plant operational states (POSs) in terms of pressure and temperature of the reactor coolant system (RCS), following the scheme developed in the low-power and shutdown PSA study for Grand Gulf.[7] In a controlled SD, such as in an LCO situation with RHR or SSW trains failed, we assumed as a nominal case that the plant will go down to POS 5, i.e., the cold shutdown state. After the repair is finished in POS 5, the plant will be started up to re-enter the full-power operational state.

However, depending on the specific failure situations of the RHR or SSW systems (e.g., both trains of RHR/SDC may be inoperable), the repair may be made while the plant is in other POSs, e.g., POS 2. More details of the optimum target states for repair are discussed in Section 6.4 along with the sensitivity analysis of corresponding risks.

PSA studies typically has focused only on evaluating the risk while the plant is in POS 0, i.e., the plant state of larger than 15% power. However, an extension to these studies is being made to consider other POSs; namely, the refueling states (i.e., POSs 6 and 7) as well as POSs 1 through 5.[7-10]

Figure 4.4 shows the behavior of the RCS process variables during a controlled SD, as required by an LCO. In the non-delayed SD scheme where the plant is shut down directly after the failure detection without any delay, then the power reduction is assumed to be performed in two phases, to 60% and 0% in 0.5 and 2.5 hours, respectively. The time lag in the first stage of hot shutdown, i.e., POS 2, is assumed to be negligible, i.e., the reactor cooldown is assumed to be started without delay after reaching zero power. A constant cooldown rate of 80°F/hour is assumed, so that the cooldown down to 135 psig takes about 4 hours. Thus, the minimum time for power reduction and cooldown to change over to the SDC mode of the RHR system (RHR/SDC) is about 7 hours.

This analysis assumes that if there is at least one RHR/SDC train intact, the plant operation proceeds according to this minimum delay scheme. If both RHR/SDC trains are inoperable, we assumed that the operators stay in hot shutdown (HotSD), using the PCS as a heat sink during repairs of the initial failures of RHR or SSW trains. The sensitivity analysis discussed in Chapter 6 will show the effect of transferring to cold shutdown (ColdSD) to use the ADHRS or RWCU system.

4.4 Reactor Coolant Supply Paths

For the RHR system to transfer heat from the reactor core to the ultimate heat sink (a cooling tower at the GG plant), maintaining the reactor coolant inventory is essential. In fact, the risk related to the failure situations of RHR or SSW trains, at least at the GG plant, is dominantly concerned with the loss of core cooling caused by the failure of the coolant supply and unsuccessful recovery during the boil-off time of the reactor water down to a critical height (assumed as the top of the reactor core).

It is convenient to group the coolant supply function into the high pressure mode (HPM) and low pressure mode (LPM) (Figure 3.1), because the pressure condition of the RCS affects the operability and success criteria of injection systems, and the operational preference and operability of RHR paths. For example, the preferred SD cooling path, RHR/SDC-SSW, can be used only in LPM (below 135 psig). However, as the reactor coolant is recirculated through the RHR heat exchangers, no bulk coolant supply is needed, assuming that the RCS boundary is intact.

Table 4.1. Changes in Plant Operational States (POSs) during a Controlled Shutdown to Repair RHR/SSW Train Failures in the Cold Shutdown State

Plant State	Description	Power	Pressure; Temperature	Remarks on Systems and Plant Configurations
POS 0	First stage of power reduction; full power	100% - ~15%	1000 psig; 550°F	Normal plant operating configuration.
POS 1	Second stage of power reduction; low power	~15% - 0%	950 psig; 540°F	Turbine bypass valves (TBVs) open below 20% power at 950 psig setpoint. Manually trip turbine for shutdown, with TBVs open.
POS 2	First stage of hot shutdown (reactor cooldown)	Decay Heat (~60 MW_{th})	950 - 500 psig	Take TBVs in manual to continue cooldown. Control reactor level with feedwater pumps.
POS 3	Second stage of hot shutdown (reactor cooldown)	Decay Heat (~40 MW_{th})	500 - 100 psig	Place RHR in SDC at ~135 psig with TBVs still open. Control reactor level with condensate and booster pumps below ~500 psig.
POS 4	Third stage of hot shutdown (reactor cooldown)	Decay Heat (~35 MW_{th})	100 - 0 psig	Shut TBVs at ~100 psig; RHR on SDC.
POS 5	Cold shutdown	Decay Heat (below ~30 MW_{th})	0 psig; below 200°F	Cooldown to ~120 to 130°F if desired and maintain with RHR on SDC.

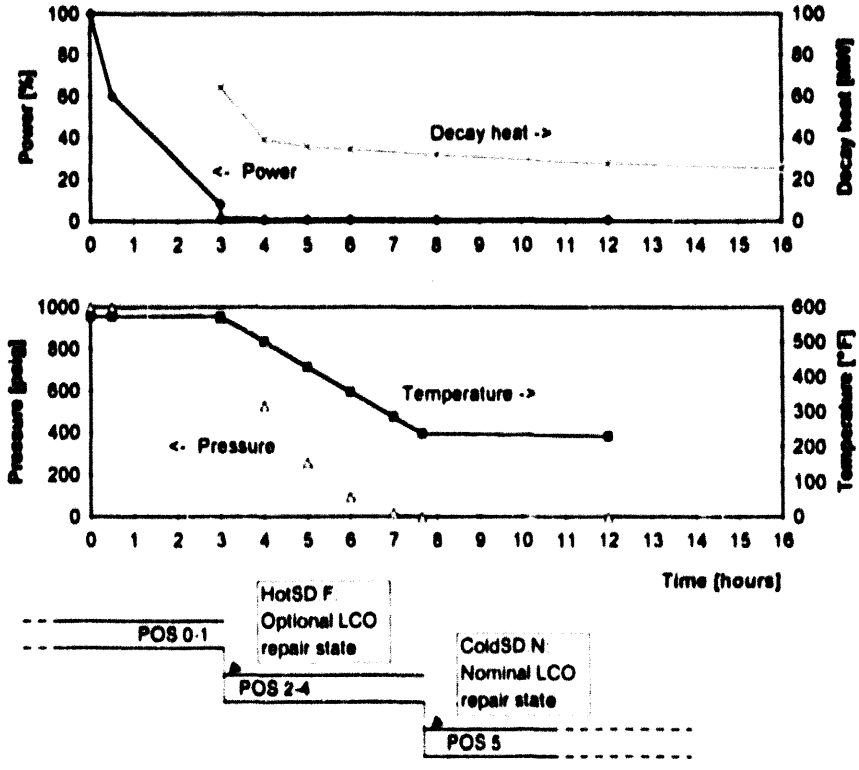


Figure 4.4 Profiles of the plant power and the RCS temperature and pressure during a controlled shutdown

4.5 RHR Paths

The primary paths for decay-heat removal (Figure 3.1) are RHR/SDC-SSW and RHR/SPC-SSW; the ultimate heat sink at Grand Gulf is the cooling tower, as mentioned earlier. Of special importance is the fact that SSW trains also serve component/room cooling for most injection systems as well as diesel-generator (DG) jacket cooling. These other SSW functions are found to be critical, because the failure in the SSW system will also fail the front-line systems and the DG needing cooling water from the system. Therefore, the SSW system becomes more important than the actual RHR system. This is in a good agreement with the results of the AOT study for the RHR system of the TVO plant. At the TVO plant, the shutdown service-water system and the shutdown secondary-cooling system (which circulates seawater to the heat exchangers of the shutdown service water system and cools DGs) together correspond with the SSW system at Grand Gulf. The containment vessel spray and pool cooling system of the TVO plant corresponds to the RHR system of Grand Gulf (with its different operation modes), and also was found in the TVO/RHR study to be of lesser importance.

Another principal reason for the lower importance of the RHR/SDC and RHR/SPC is that containment venting can be used as a redundant, last resort (this will be called the containment pressure relief state, i.e., CoPRe). The reactor core can be saved in this state, assuming that there is adequate reactor coolant supply to replace the boil-off, and that the steam relief function is operating.

4.6 Modeling of Event Sequences

The phased missions and event sequences of plant response to RHR challenges are modeled using extended event sequence diagrams (EESDs), following the modeling approach described in reference 9. Figure 4.5 shows a portion of the simplified EESD developed for phased missions following a loss of offsite power (LOSP) as an initiating event of shutdown cooling. In this EESD, it is assumed that safety relief valves successfully open and reclose to relieve the pressure surge caused by the reactor scram due to the LOSP transient.

Appendix E describes general principles of EESD modeling and presents the EESDs for LOSP developed in this study. It should be emphasized that initiating events of shutdown cooling, such as LOSP and LoIAS, are considered as basic events throughout the plant shutdown states, representing the fact that those initiators may occur any time during the shutdown states.

EESD models would become overly extensive if drawn down to the fine level of system detail. Hence, it is desirable to use functional entities such as the HPM coolant supply, ADS, and RHR/SDC. The ESD models primarily describe operational states, dependencies, and preferences. The connection with plant hardware is established through Boolean expressions, which describe how the functional entities are realized by system modules. Actually, inverted logic is used, i.e., loss of function is presented as logical combinations of the module failures, which is equivalent to a fault tree presentation. Effectively, this means that event sequences are first identified using functional entities, and then developed into hardware details using system module failures and other basic failure events.

4.7 Modularization Approach to System Modeling

Components are grouped into functional blocks called modules that are basic entities in the reduced block diagrams, used for system modeling. A typical module is an RHR pump train, including the pump, associated isolation valves, and the minimum-flow recirculation line. Another important module is the SSW pump train, defined to include the so-called common elements of the SSW redundancy.

This type of compressed modeling is not a substitute for the detailed modeling of fault trees, but it is convenient for describing and quantifying event sequences with explicit consideration of time-dependencies. The simplifications introduced in the module reduction were checked against fault-tree models by comparing the minimal cut sets for systems up to an acceptable truncation threshold.

The functional block diagrams correspond to the Boolean expressions for the system functions, which link hardware structures with function-level EESD models discussed earlier. The block diagrams also incorporate the hard-wired functional dependencies such as power supply, room and component cooling, and instrument air supply. The minimal cut sets (MCSs) were reduced by retaining only the dominant contributors for the operational alternatives, and some additional failure combinations to reasonably cover each initiating event.

4.8 Modeling of Power Supply and Support Systems

AC power supply to the safety system trains is described through modularization, up to the level of DG aggregates, startup batteries, and DG jacket cooling. DC power supply was not explicitly modelled because the GG/PSA showed its relatively small contribution.

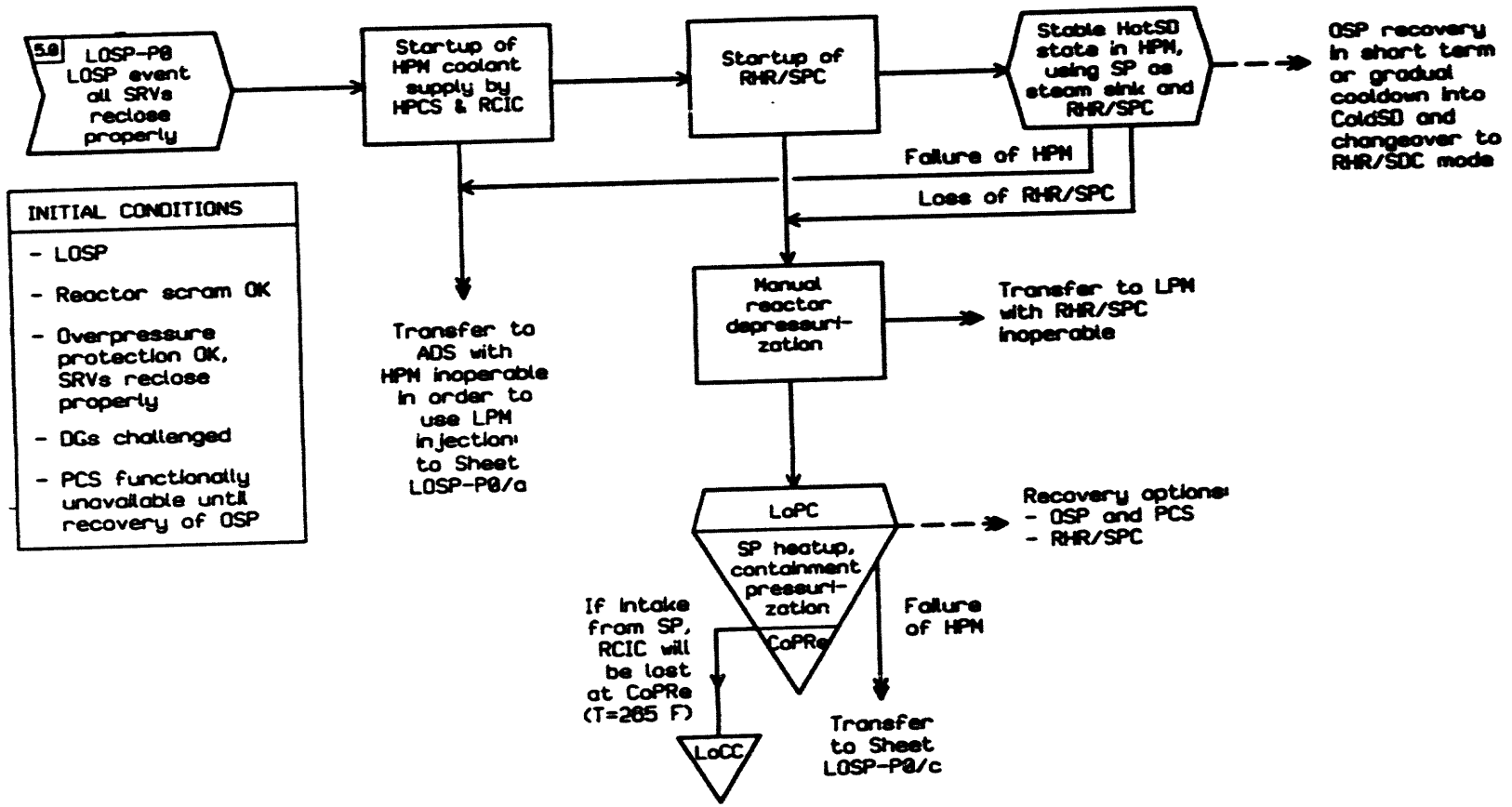


Figure 4.5 Example EESD for the partial, simplified presentation of the LOSP scenario

All essential support systems were included in the reduced modularization and also those containment systems which have a direct relationship to the coolant supply or RHR function. Other aspects of containment functions are not covered, in accordance with the limitation of level-1 PSA.

4.9 Operator Interactions

To some extent, operator interactions are covered implicitly within system modules, e.g., errors of omission for starting up or realigning standby systems. Realignment of system will be necessary particularly for the RHR system because of its diverse operating modes. For instance, in cases where the RHR system was in the SDC mode and the need arises to cool down the suppression pool, the operator must align the pump suction valves from the reactor recirculation line to the suppression pool and realign the SPC and SDC injection valves for the SPC success. Another example can be found in the CS mode: (a) for those sequences where RHR train B is in SDC prior to using CS, the operator must realign the RHR pump B suction valves from the reactor recirculation line to the suppression pool for CS B to be successful, and (b) for those sequences where ADHRS is/was in operation before using CS, the operator must realign the RHR pump B suction valves to the SP for CS success.

However, these types of system realignment errors and valve restoration errors are not unique for shutdown operations (although they may more likely occur during shutdown). Even in the continued-operation alternative, such realignment of the RHR system, e.g., from the SDC to the SPC mode, may be needed if the suppression pool gets too hot during a forced shutdown. Hence, detailed modeling of these operator errors may not be necessary, especially where only the relative risks, e.g., between continued operation and shutdown alternatives, are of interest as in this study.

If operators make errors in realigning systems or restoring valve positions, these errors sometimes may result in flow diversion, causing losses of coolant inventory, losses of decay heat removal, or losses of service water. In the full-power PSAs, this type of flow diversion through valving errors is typically assumed to be negligible compared to other system failures. In the on-going low-power and shutdown PSAs,[7-10] these events are quite extensively modeled in terms of initiating events and subsequent plant responses during shutdown states. The flow diversion through valving errors has not been explicitly considered in this study, but may be potentially important in comparing risks for the AOT evaluation. In the comparison of risks for the continued-operation and shutdown alternatives discussed later in the report, a more explicit consideration of this issue will result in an increase in the shutdown risk as compared to the continued-operation risk to some extent; as such, it was taken into account in our considerations for risk-based improvement of the action requirements.

4.10 Recovery Paths and Heatup Time Scenarios

Near Mission Failure (NMF) is defined as a state where a critical safety function is lost and an undesired consequence state will be entered without recovery measures. The following NMF states are defined:

(1) LoCC (loss of core cooling) where the reactor coolant supply is lost.

(2) LoRHR (loss of RHR function) where the heat transport from the reactor core to an ultimate heat sink, such as seawater or the atmosphere, is inoperable.

(3) LoSPC (loss of suppression pool cooling), a subset of LoRHR, which has a central role because the pool water is an important delay buffer.

These states are listed in the order of descending importance. In some event sequences they may be causally related. When an overlap of the NMF states occurs, the analysis focuses on the more important state.

When the plant enters an NMF state, there is a time margin until an undesired end event occurs, e.g., core damage from the loss of core cooling. This time margin available for recovery will be called "heatup time," which is determined by delaying buffers such as the following (relevant for a BWR plant):

- heatup of the suppression pool in the case of LoRHR, but with the feedwater and steam-relief functions retained
- decrease in the water level of the reactor in the case of LoCC
- depletion in the DC supply from station batteries for vital instrumentation in the case of station blackout

The relative importance of these delaying buffers depends on the specific event sequence.

Figure 4.6 shows an example of heatup scenarios to estimate the time margin until the suppression pool reaches its threshold temperature, i.e., 255 °F where the limit of primary containment pressure is reached. The scenario IH0 is concerned with LoSPC at zero time point, i.e., at the beginning of SC mission. It means regulated steam relief to SP, and is relevant for the transients with loss of PCS and with RHR/SPC initially inoperable. The time margin before crossing the threshold for containment pressure relief (~ 255 °F) is 9.2 hours. The scenario IH1 is concerned with loss for PCS transients and with one RHR/SPC train initially operating. When staying in this state, SP temperature increases to about 160 °F, and then decreases as the heat transfer capacity of the operating RHR/SPC train exceeds the decay heat power. The scenario IH1:16 shows the temperature increase in the case that the operating RHR/SPC train fails to run 16 hours during the IH1 scenario. The CoPRe threshold will be crossed inthe following 10.8 hours, if no recovery is made.

The selection of heatup scenarios and the derivation of recovery time margins at discrete time points are presented in more detail in Appendix F.

4.11 Quantification of Event Sequences

The central feature of the approach used to quantify event sequences is that the quantification is based on transition rates (expressed as probabilities per unit of time). This feature is connected to the use of EESDs for event sequence modeling, which incorporates plant states. A benefit of this approach is that various time-dependent aspects can be consistently handled, such as functional or operational dependencies on the actual state of the plant and previous scenarios of events. This approach contrasts with the conventional event tree-fault tree approach, which averages time-dependencies at the basic event level, and uses the average basic-event probabilities in quantifying sequences.

The quantification of EESDs, as implemented in the TeReLCO computer program,[3] produces risk frequency (or rate) in the first stage as a function of time over the plant response mission, given a specific initiating event. From these risk frequencies, we can derive various predicted or expected risk entities.

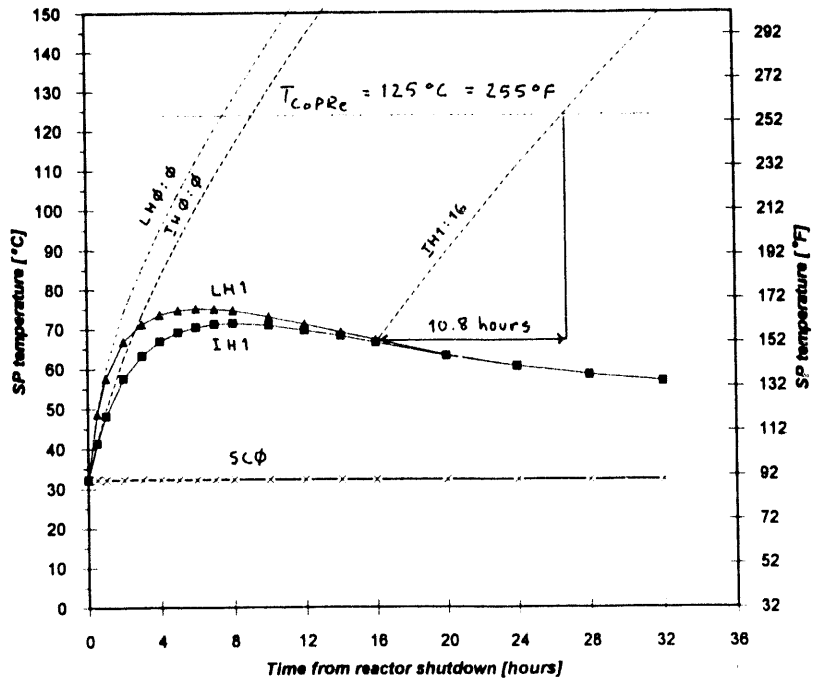


Figure 4.6 Temperature profiles of the suppression pool for various operational and steam-blowdown situations

This approach to quantifying event sequences allows the use of time-dependent component unavailability models; however, this aspect is usually of minor significance. Hence, constant unavailability was used for the standby components and systems. If, for example, a more detailed consideration of test arrangements is needed for certain components, the time-dependent unavailability model may be selectively implemented for those.

In addition to transition rates, another notable feature of our approach is the incorporation of repair or recovery time distributions for component failure events and other corresponding basic events. In this pilot phase, generic distributions were used with insights from the AOT study for the RHR system of the TVO plant.

The refinement of the data base was minimal. To quantify the event sequences, we adopted most of the data from the GG/PSA; consequently, the quantification results are mainly based on generic data, as in the PSA. However, for the predominantly important initiator of loss of offsite power (LOSP) which contributes 97% of the core damage frequency during power operation,[15] we used data from recent operating experiences (Appendix D). Also, for the loss of instrument air system (IAS) initiator, we refined its frequency by including common-cause failures (CCFs), not considered in the GG/PSA.

The CCF model was partly refined, but in most regards, it is compatible with the handling of CCFs in the GG/PSA. The model neglects time-dependence, as for the unavailabilities of standby components and systems. If fine details of test arrangements are required, we may include time-dependence in modeling CCFs of redundant trains.

In AOT evaluations, modeling and quantification of recovery from NMF states is crucial for a consistent comparisons of risk primarily because the time margin for recovery significantly increases, especially during the late stage of repair, when the alternative of plant shutdown is taken. This increasing time margin resulting from the diminishing level of decay heat demonstrates the actual benefit of shutting down the plant in failures of RHR or SSW systems. In this study, the simplified heatup-scenario approach was implemented, as discussed in the previous section; heatup time margins were calculated by a reduced model for decay-heat transfer (Appendix F).

4.12 Modeling Assumptions

The description of the methods in the preceding sections included presentation of the principal assumptions also. To summarize, the most essential bounding feature is equivalent to the limitation of the level-1 PSA only for, so called, internal initiators. This may produce some bias to SD/CO risk comparison, because the external initiators, especially fire and flood, may contribute more to the plant risk in the power operation state than in LCO shutdown states, and because accidents starting from the full power conditions may impose a greater challenge on containment functions.

On the other hand, the potential initiators specific to the LCO shutdown states are not considered in detail. The candidates include flow diversion errors, which may be specially relevant in an LCO shutdown with RHR function affected, because off-normal flow alignments will then be made. The results from the recent PSA extensions for refueling outage indicate that this kind of special initiators may be significant contributors. Their identification would require a careful qualitative analysis of the shutdown operations, which was outside the scope of this study.

The shutdown operations are not considered in detail either with regard to improvised recovery possibilities. Depending on the situation, there may be additional recovery chances, for example, by using feed and bleed cooling of suppression pool, or intermittent use of diversified equipment to avoid pump heatup when component cooling is lost. However, these are expected not to influence strongly the relative results.

The data used in this study are of generic type, and the inherent uncertainties are similar to PSA studies. The influences of data are mostly not strong on the relative results. The important exception is concerned with the conditional frequency of LOSP and loss of IAS in different shutdown states. The data for them are mainly based on the estimates obtained for refueling period in the recent PSA extension. The frequency of LOSP and loss of IAS, as well as some other transient initiators, may however be higher during the non-stationary LCO shutdown stages, which would increase the relative risk of SD alternative.

The nominal calculations, the results of which are presented in Chapter 5, are based on specific assumptions about the non-delayed timing of the LCO shutdown, and cold shutdown as the target state. Alternative timing and target states are considered with a high priority among the sensitivity issues, and will be discussed in Chapter 6.

5. RISK COMPARISON OF THE BASIC OPERATIONAL ALTERNATIVES

This chapter discusses the results of main quantification for the risk comparison of basic operational alternatives, i.e., continued operation (CO) and shutdown (SD), in the failure situations of the RHR or SSW trains. This quantification was performed by using nominal assumptions concerning timing, procedure, and target state of the LCO shutdown. Section 5.1 discusses the assumptions. Sections 5.2 and 5.3 present the results of risk analysis for failure situations in the SSW and RHR systems, respectively. Alternative LCO shutdown schemes and their influences on the risk comparison will be discussed in Chapter 6.

5.1 Assumptions in the Nominal LCO Shutdown Scheme

The nominal calculations for SD/CO risk comparison were done by assuming that specific RHR or SSW trains are detected failed, and that the other redundant trains are tested operable and returned into standby.

It is a different case if the remaining trains have not been tested, because their status is uncertain. In this case, a possible existence of common cause failure (CCF) is crucial, and determines the likelihood of the actual failure multiplicity present. The influence of performing the additional test of the remaining trains will be discussed in Chapter 6.

The motivation of doing the first stage calculations, assuming that the other redundant trains are tested operable and returned into standby, is the fact that from these basic results one can easily superpose the various risk variables for other cases, where the status of the redundant trains is not freshly known.

The following assumptions, concerning the timing and target state of the LCO shutdown, were used for the risk analysis of basic operational alternatives in the failure situations of RHR or SSW trains:

1) In the SD alternative, the controlled shutdown is assumed to be undertaken directly after the fault detection. The aim is to obtain in principle a risk estimate for this alternative.

2) The repair of the detected fault or multiple faults will independently progress during the shutdown operations. Effectively, this corresponds to the assumption that the same repair-time distributions can be used regardless of which plant operational state the repair is made in.

3) The target state of the LCO shutdown is assumed to correspond with the first end of the cold shutdown state (POS 5), where the reactor is nonpressurized below 200°F. The optional use of the alternate decay heat removal system (ADHRS) is not credited. This means that in the case of RHR/SSW trains A and B being inoperable, the use of PCS is assumed to be extended to the cold shutdown state for decay heat removal. The unreliability of PCS hardware is neglected to effectively compensate for the non-crediting of the optional use of the ADHRS. The use of PCS in this mode of operation may, however, be unstable. The modeling details need to be refined to more consistently handle success and failure paths in this case.

The influences of different shutdown schemes will be considered in Chapter 6, after first discussing the main quantification results based on the above assumptions in the following sections.

5.2 Results for Failure Situations in the SSW System

Figures 5.1 and 5.2 show how the instantaneous and cumulative risks change for the continued operation (CO) and shutdown (SD) alternatives in various failure situations of the SSW system, i.e., single, double, and triple failures.

(1) Single-Failure Situation

Where one SSW train (e.g., train B) is detected failed during power operation, the instantaneous risk frequency increases by a factor of about 7 over the baseline risk level (see risk-increase factor for 1*SSW situation in Table 5.1). If the CO alternative is taken, the risk will remain at this level until the operability of the failed train is restored. If the SD alternative is taken (directly after detecting the failure), then the plant will be temporarily placed at a higher risk than the operating risk during the initial transition period of power reduction and state changes. However, after this peak, the LCO shutdown risk slowly declines, resulting in a smaller and smaller risk impact to the plant compared to the operating risk level. The profiles of cumulative risk indicate that the LCO operating risk is smaller than the LCO shutdown risk until the repair time of 3 days (Figure 5.2).

(2) Double-Failure Situation

When two SSW trains (e.g., trains A and B) are detected failed, the risk profiles for both CO and SD alternatives are similar to those in a single failure, except that the risk levels are much higher (by a factor of 160 over the baseline). Figure 5.2 shows that the cumulative risks for CO and SD alternatives over predicted repair time again intersect at about 3 days.

(3) Triple-Failure Situation

Where all the SSW trains (i.e., trains A, B, and C) are detected failed, the instantaneous risk dramatically increases by a factor of about 3600 over the baseline. If the SD alternative is taken, there will be a temporary risk peak during the initial transition of power reduction and state changes, resulting in a higher risk than the LCO operating risk. However, in contrast to single and double failures, for several days after the shutdown there is a higher risk level than for the CO alternative. The intersection of the cumulative risks over predicted repair time occurs about 14 days after shutdown (Table 5.1).

Over all failure multiplicities of the SSW trains, the risk of continued power operation is dominated by loss of offsite power (LOSP) sequences, as well as for the baseline plant state. Accident sequences due to loss of power conversion system (LoPCS), loss of instrument air system (LoIAS), and intermediate LOCA (LOCAM) together contribute less than 10 percent of the core-damage frequency.

The risk of decided shutdown also is dominated by LOSP sequences, but not so strongly as for continued operation, because LoPCS and LoIAS become substantial contributors when the plant goes to shutdown. The peak in shutdown risk in the single and double failures is mainly due to LOSP and LoPCS transients occurring during the power reduction and reactor cooldown stages. In triple failures, LoIAS transients become a substantial contributor (in relation to the loss of component cooling due to all SSW trains being inoperable).

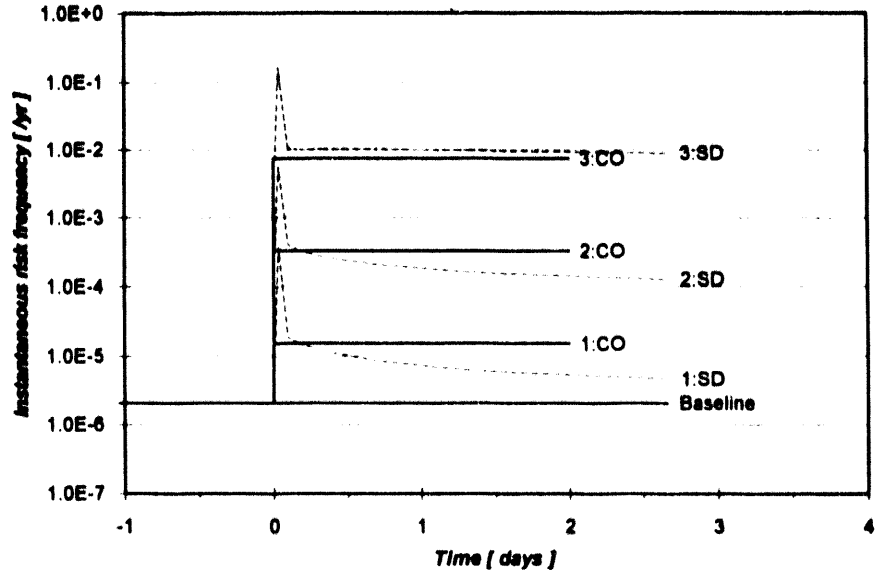


Figure 5.1. Instantaneous risk frequency for the continued operation (CO) and shutdown (SD) alternatives in failure situations of the SSW system (For example, 2:CO denotes the CO alternative for the situation where two SSW trains are inoperable.)

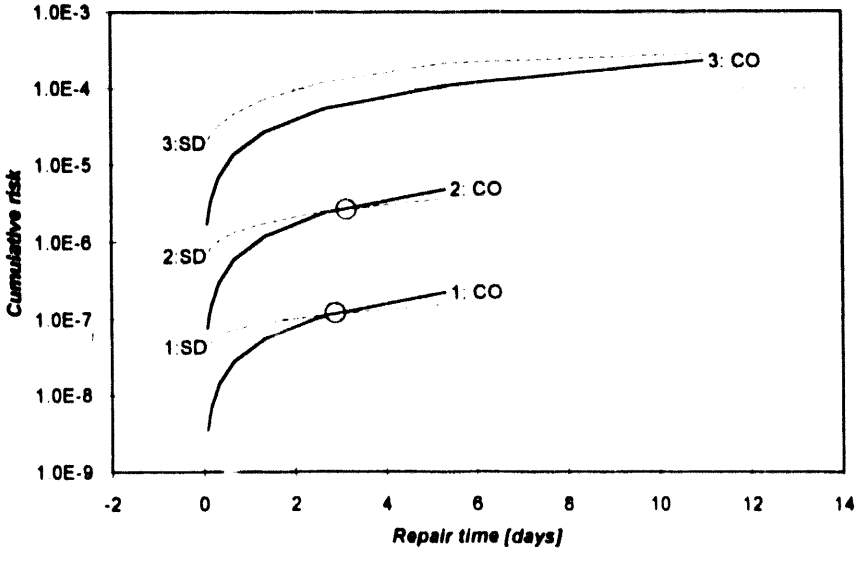


Figure 5.2. Cumulative risk over predicted repair time in failure situations of the SSW system (For example, 2:CO denotes the CO alternative for the situation where two SSW trains are inoperable.)

Table 5.1. Summary of Quantification Results for Failure Situations in RHR and SSW Systems

LCO state	Risk frequency in power operation state [/yr]	Risk increase factor	Crossing point of the SD/CO alternatives [days]	Risk per failure situation			Exp. number of failure situations [/yr]	Relative add. to average CDF	
				Continued operation CO	Controlled shutdown SD	Risk ratio SD/CO		Continued operation CO	Controlled shutdown SD
Baseline	2.1E-6								
1*SSW Train B	1.5E-5	7.4	~3	2.3E-8	5.7E-8	2.5	0.51	0.56%	1.40%
2*SSW Trains AB	3.3E-4	160	~3	4.5E-7	9.6E-7	2.1	0.0074	0.16%	0.35%
3*SSW Trains ABC	7.4E-3	3600	~14	1.1E-5	3.3E-5	3.0	0.0020	1.03%	3.08%
1*RHP Train B	2.2E-6	1.1	~2	2.7E-9	5.3E-9	1.9	0.16	2.2E-4	4.2E-4
2*RHP Trains AB	3.6E-6	1.7	~6	6.1E-9	4.2E-8	6.8	0.002	7.3E-6	5.0E-5
							Sum addition	1.77%	4.88%

Figure 5.1 shows a unique pattern in the SD risk profile for triple failures, as compared to those for single and double failures. When all SSW trains are inoperable, the plant becomes vulnerable especially to the LOSP and LoIAS initiators in shutdown states as well as power operation state, because of the resulting loss of PCS and lack of major means to remove decay heat. In addition, these initiators have a higher frequency in shutdown states than in power operation state. As a consequence, the risk frequency remains high in the cold shutdown state, and the cumulative-risk curves cross only at a long predicted repair time, i.e., 14 days (Table 5.1).

Table 5.1 presents the results of our risk quantification for the pump train failure situations in the RHR and SSW systems, including: the risk frequency in power operation state, the risk increase factor for CO alternative, the crossing point of the cumulative risks for SD/CO alternatives over predicted repair time, the expected risk per failure situation for SD/CO alternatives with the ratio between the two risks, the expected number of failure situations per year, and relative addition to the average core-damage frequency. In particular, the important information on the SD/CO ratio of the expected risk per failure situation indicates that SD alternative is unfavorable in all three failure situations of the SSW system, although not very strongly, in light of the underlying uncertainties in risk evaluations.

5.3 Results for Failure Situations in the RHR System

Figures 5.3 and 5.4 show the instantaneous and cumulative LCO risks for failure situations in the RHR pump trains A and B, i.e., single and double failures. Each situation is discussed below.

(1) Single Failures

Failure of a single RHR train (e.g., train B) causes a minimal increase over the baseline in the instantaneous LCO operating risk (Table 5.1). However, when the plant is shut down, the instantaneous risk peaks sharply and then decreases rapidly below the level of the CO alternative. The cumulative operating and shutdown risks cross at about 2 days, as shown in Table 5.1 and in Figure 5.4.

(2) Double Failures

When both RHR pump trains, i.e., trains A and B, are down, all the operational modes of the RHR system but the LPCI train C will be unavailable. Consequently, the plant becomes vulnerable to LoPCS sequences including the failures of the HPCS and ADS, because the RCIC system is the only means to supply coolant to the reactor. In this event, the containment will pressurize because of the inoperability of the SPC and CS modes of the RHR system, and the RCIC system will be lost at containment venting, if recoveries are not successful up to that point. These sequences contribute to both the operating and shutdown risks. Table 5.1 shows that this situation of double failures also incurs a relatively minimal increase in LCO operating risk over the baseline; however, the risk ratio for SD/CO alternatives is quite high (6.8), meaning that the SD alternative is more risky than the CO alternative. Figure 5.3 shows that the risk frequency for the SD alternative peaks sharply and then decreases markedly, because the effectiveness of the suppression pool as a heat buffer increases with the diminishing level of decay heat. The cumulative operating and shutdown risks intersect at approximately 6 days of repair time.

(3) Triple Failures

Triple RHR-train failures have not been evaluated because Train C is dedicated for LPCI, and its failure is not directly concerned with the AOT issue for the RHR system. On the other hand, the

LPM coolant supply paths are not modelled in sufficient detail to infer the influence of the failure of LPCI train C, although this modeling could be done in the continuation with a few additions.

According to the relative addition to average core-damage frequency in Table 5.1, the triple failure situation in the SSW system is expected to contribute the most to the average CDF among the various failure situations in RHR/SSW systems. The reason for this largest contribution of triple SSW-train failures to the average plant risk is that this failure situation has very high risk impact, although it will occur relatively infrequently. The sum addition in the table indicates that, comparing CO and SD alternatives in failure situations of RHR/SSW systems, the SD alternative will contribute more than double than the CO alternative to the average plant risk.

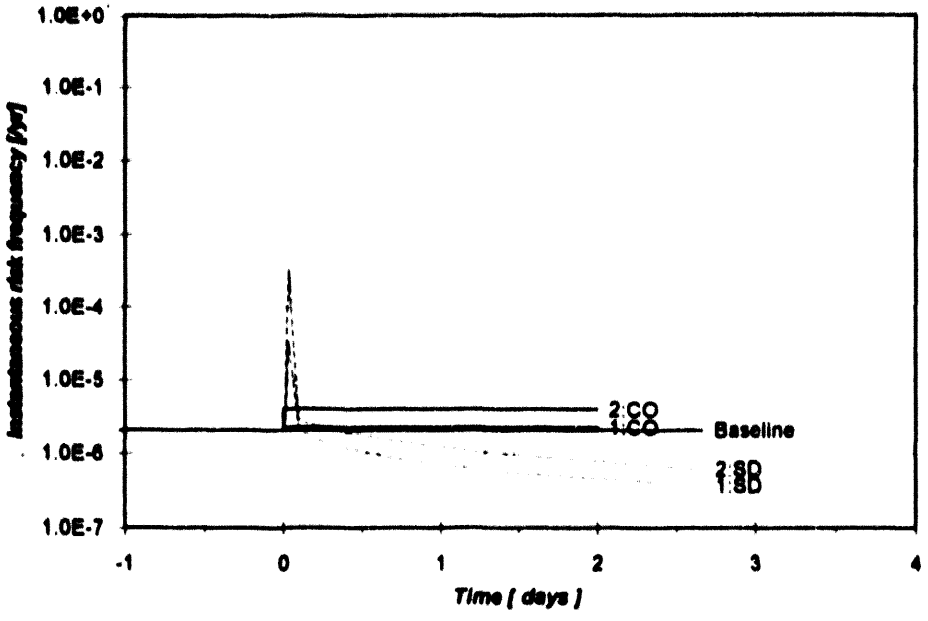


Figure 5.3. Instantaneous risk frequency for the continued operation (CO) and shutdown (SD) alternatives in failure situations of the RHR system (For example, 2:CO denotes the CO alternative for the situation where two RHR trains are inoperable.)

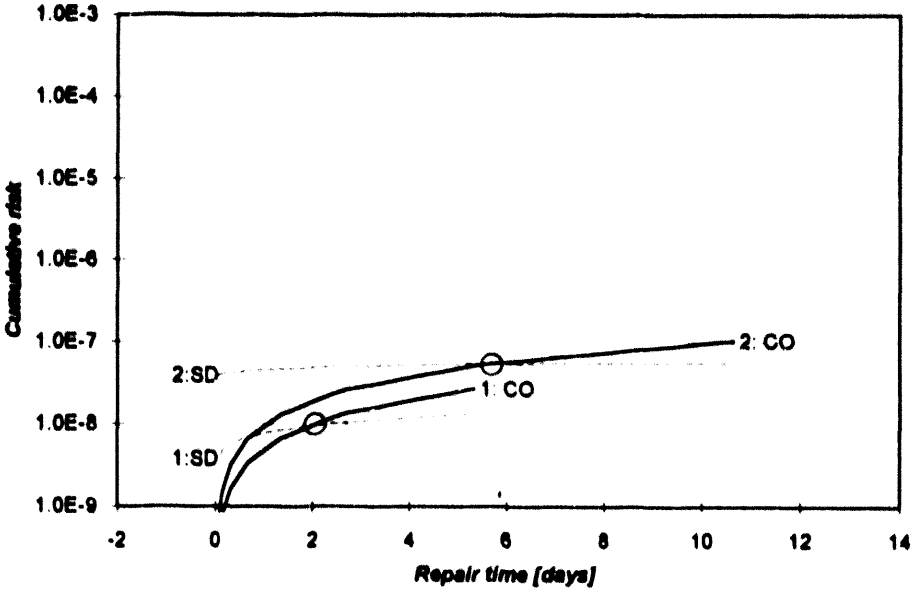


Figure 5.4. Cumulative risk over predicted repair time in failure situations of the RHR system (For example, 2:CO denotes the CO alternative for the situation where two RHR trains are inoperable.)

6. SENSITIVITY ANALYSES TO IDENTIFY OPERATIONAL POLICY ALTERNATIVES

In this chapter we discuss the decision alternatives studied in RHR/SSW system LCO conditions. As stated earlier, we studied the major decision paths between the alternatives: (a) continued operation at power with priority on the repair, and (b) shutting down the plant in order to complete the repairs in a stable shutdown state. Risk analyses show that there is generally no clear advantage of one alternative over the other. Therefore, our objective is to seek other alternatives or additional guidelines within each of the decision choices so that the risk impact is controlled, as far as possible, whenever these LCO conditions are entered.

We discuss the sensitivity evaluations performed in defining the TS action statements for failure situations in RHR and SSW system for a BWR plant. Here, we analyze operational policy issues which will provide specific guidance in the action statements to control plant risk. We also address assumptions in the methodology and the variations in data to assure that the action requirements chosen are robust to such uncertainties. Based on these evaluations, we provide insights on the applicability of the results obtained from analyses of one nuclear power plant.

6.1 Identification of Operational Policy Alternatives

The major decision in an LCO condition is the choice between continued operations and transition to shutdown mode. For LCO conditions in systems that are required during the shutdown, the action statements may require more detailed guidelines (instead of requiring shutdown in case an AOT is exceeded) to assure better control of risk. The operational policy alternatives available can be stated as the following questions:

a) Should additional testing or inspection of redundant RHR/SSW trains be performed to identify multiple failures immediately or to identify an available success path so that a sufficient AOT can be provided to complete repair without incurring undue risk due to continued operation?

b) Is it important from risk considerations to assure availability of other systems and components through testing or inspection to minimize the risk of a RHR/SSW LCO condition?

c) Should an early portion of the AOT be used to decide between shutdown and continued operation to control the total risk?

d) When a decision to transfer to the shutdown mode has been made, should operations proceed quickly to an operational state where alternate decay-heat-removal systems (ADHRS) can be used, or should operations stay in hot SD condition to complete the repair?

e) When a decision to transfer to shutdown mode has been made, should plant personnel postpone any repairs until a stable shutdown state is achieved?

Answering these questions will give clearer guidelines for action statements and so improve the risk-effectiveness of the TS requirements. Our methodology allows evaluation of these policy alternatives. Sensitivity evaluations performed to address these questions, are discussed below.

6.2 Specific Sensitivity Evaluations to Address Operational Policy Alternatives

Table 6.1 presents the sensitivity analyses needed to identify the operational policy issues, the risk implication of the issues, and the TS implication if such guidelines are provided.

Requirement for Testing Other Components

The requirement for testing other components given an LCO condition will either help identify the failure of additional components, or assure alternate success paths. In case of a single failure, it will assure whether redundant trains are capable of performing the function desired. Early identification of multiple failures will clearly result in actions taken where the total risk from the situation will be minimized, while successful test(s) can define longer AOTs to allow completion of repairs. The objective of this sensitivity evaluation will be to identify any specific test arrangements that have significant risk benefits, and to study AOTs that can be prescribed when these additional testings are made. Specific test requirements and the associated AOTs are analyzed to obtain risk implication in a LCO condition.

Timing of Shutdown for LCO Repairs

When a decision is made to transfer to a shutdown mode, operators can satisfy the TS requirement by staying in the hot SD mode and attempting to complete the repair in order to come back to power as quickly as possible. However, such a decision may be unwise compared to both the alternatives studied previously if the risk in the hot SD mode is higher. Particularly for multiple failures in RHR/SSW systems, it may be wise to directly move the plant to a state where the capability for alternate decay-heat removal can be used (POS 5, as defined in the shutdown PRA). In this sensitivity evaluation, these alternatives are quantified to determine if there is a clear advantage. If risk during hot SD condition is higher, then there is an advantage of minimizing the operation time in that state.

Postponing LCO Repairs when Controlled SD is Initiated

Currently, Technical Specifications allow repair of the failed components to continue while controlled SD is initiated. This is preferred by plant personnel to minimize the financial loss associated with a shutdown. Since RHR/SSW failures have significant risk implications, it may be inappropriate to allow repair which may divert attention from or may even delay, a shutdown. If shutdown is desired because repairs cannot be completed quickly, then focussing the operators' attention to achieving the shutdown, and removing any uncertainty about the decision may be desirable. In this sensitivity evaluation, these alternatives are studied, incorporating qualitative considerations and presenting a decision between the choices.

Splitting of AOTs in Two Phases

To control the total risk associated with the LCO conditions discussed here, it may be prudent to make an early decision between continued operation and transition to a shutdown mode. The transition to a shutdown mode may require postponing repairs and quickly proceeding to a state where alternate capability for decay heat removal is available. Under the current requirement, the entire AOT period can be used before proceeding to a shutdown mode, and thereby, incurring significant risk both from continued operation and from transition to shutdown. In this policy alternative, a portion of the AOT is used to assess the situation and the ability of the plant personnel to repair the failed components. Then, a decision is made either to continue operation with repairs being made and additional precautions taken, or to proceed to a safe shutdown state. The objective of this sensitivity evaluation will be to assess

the risk advantage of this alternative. Also, an appropriate way of splitting the AOT will be studied. Clear guidance to decide between the alternatives may also need to be provided. For multiple failures, providing AOTs with a defined early time for such choice may be the most beneficial.

Table 6.1. Sensitivity Analyses Issues for Identification of Operational Alternatives

Operational Policy Issues	Risk Implications	Tech Spec (TS) Implications
1. Requirements for testing redundant trains and other risk-significant components to assure availability of a success path.	Will result in either early detection of multiple failures, i.e., high level of risk to the plant, or will identify a lower level of risk (assuring a success path) during the AOT which will give sufficient time for repair.	TS can require specific testing requirements before repairs are started. The intent of the testing is to avoid the shutdown alternative which has significant risk implications and take appropriate operation paths depending on the test outcome.
2. Timing of LCO shutdown for LCO repairs: deciding between (a) staying longer in hot SD vs. (b) quickly proceeding to POS 5 for repairs.	Decision alternative of quickly proceeding to POS 5, where alternate decay heat removal capability is available, can result in lower risk implication for the shutdown alternative.	TS can provide specific guidance about the timing of SD for LCO repairs.
3. Splitting of AOT in two phases: within the first phase, decisions are to be made to complete the repair within the AOT or to shutdown.	An early decision to proceed to shutdown where eventually shutdown will be required will lower the overall risk when alternate success paths cannot be assured.	Implementation guideline of AOTs for these systems will require SD decision within the first phase of the AOT to be defined.
4. Time to reach cold shutdown from full power state.	Longer time in hot SD or to reach cold SD may imply increased risk.	TS time limits for reaching hot SD (12 hrs.) and achieving cold SD (24 hrs.) can be reduced for these LCOs.

6.3 Operational Policy Alternative: Testing of Redundant Train Following Detection of a Failure

Currently, TSs do not specifically require testing of redundant RHR/SSW trains when failure in one of the trains is detected. In this chapter we analyze the benefits and associated issues related to additional testing of redundant trains to address the need of such tests in situations where a clear advantage exists.

The benefits desired from additional tests are: a) to identify the failure of redundant trains, primarily due to existence of a common cause failure, where the risk implication is higher, and b) to assure availability of an alternate success path. Early identification of multiple failures will clearly result in actions taken where the total risk from the situation will be minimized, and at the same time, successful outcome of the test(s) can define longer AOTs to allow completion of repairs.

Additional testing, in these situations, is associated with a number of potential adverse effects. These effects can not always be addressed in quantitative manner, but, should be considered in defining the requirement. Briefly, they include: a) the likelihood of failure due to the additional test; i.e., if the demand (or time-independent) part of the component unavailability is substantial in comparison to the standby failure (or time-dependent) part of the component unavailability, then the advantage of the testing may be small, and it is likely that the redundant equipment may suffer a failure due to the test; b) delay in repair of the failed component resulting in increased cumulative risk; the test may divert attention away from the orderly repair of the first failure, which, as will be shown later, is the most important need in such situations; and c) failure to properly restore the component after the test which can negate the benefit that is desired from testing in the first place.

The analysis of additional test requirements includes addressing the risk advantages of the priority and timing of the tests with respect to repair of the initial detected failure and the operational decisions depending on the test results. The questions to be addressed in defining the test need can be summarized as follows:

a) Should other trains be tested promptly after detection of the first failure, before diagnosis of the repair time needed for the failed equipment?

b) Should the test be performed following initial diagnosis of the detected failure, i.e., only if similar failure (or common cause failure) is suspected?

c) Should test be performed, prior to initiating an LCO shutdown when repair could not be completed within the AOT?

d) If the test is successful, should the train be kept in operation to reduce the risk of shutdown, which may be needed?

The questions are interrelated and are addressed below, where alternative scenarios or strategies are defined and their risk impacts are assessed.

Risk Impact of Alternative Strategies for Test Requirements

To analyze the additional test related issues raised above, the following alternative strategies were defined for evaluation and risk-based comparison:

1. *Base Strategy:* No additional test following detection of failure, i.e., prior schedule of test is followed.

2. *Unconditional Additional Test:* Test following detection of a failure.

3. *Alternate Strategy 1:* Test only if similar failure (i.e., common cause failure) is suspected.

4. *Alternate Strategy 2:* Test the remaining trains following repair of the first detected failure. For multiple redundancies, one redundant equipment will be tested at a time and repaired.

Results of Sensitivity Analyses: Additional Test of a Redundant Train Following Detection of a Failure

The additional test scenario is analyzed for failures in the SSW system. The SSW trains are assumed to be tested using a staggered testing strategy, i.e., each test of a train is separated from a test of another train by the same time interval. Figure 6.1 presents the effects of additional test using failure of SSW train B as an example. The figure shows the CDF level during power operation for various failure combinations of SSW trains: a) 1:CO represents the CDF level when SSW train B is failed, and trains A and C are successfully tested, but in standby, b) 1:CO/No Add Test represents the CDF level when SSW train B is failed, but no additional tests are performed of trains A and C, c) 2:CO represents the CDF level for failure of 2 of the 3 SSW trains, and the third train is successfully tested, and d) 3:CO represents the CDF level for failure of all three SSW trains. The figure shows that the risk impact when no additional tests are performed given SSW train B failure is about an order of magnitude higher compared to the risk impact when the remaining SSW trains A and C are successfully tested. This difference is expected to be observed 90.3% of the cases. The likelihood of observing one or two failures are respectively 7.9% and 1.8% and are presented in the figure. These likelihoods are determined primarily by the random failure data and the common cause failure probabilities for the SSW trains. It may be noted that the risk level corresponding to Train B failure without additional test is essentially the superposition of the other conditions resulting from test outcomes weighted by the respective likelihood of each occurring.

A comparison of the risk of continued operation and shutdown, when no additional tests are performed, is presented in Figure 6.2. As shown, for both single and double failures, when no additional tests are performed, the risk of shutdown is higher than the risk of continued operation. When additional tests are performed (Figures 5.1 and 5.2), the risk levels are significantly lower for single and double failures. For triple failures, the question of additional test does not arise, and so the results remain unchanged.

Priority to Repair the Detected Failure

One option is to repair the failure detected, as a first priority, before any tests are performed (Alternate Strategy 2). The reason is to focus attention on assuring a known failure is repaired as quickly as possible.

Figure 6.3 shows the risk effect of repairing the initially failed train. As a comparison, the risk level of various failure situations in the SSW systems, when additional tests are performed, and the risk associated with the shutdown alternative are presented. For the shutdown alternative (1:SD/No Add Test), no additional tests are assumed prior to a controlled shutdown. As shown, there is a significant decrease in the risk level due to repair of initially failed train. The reason of this reduction is the low unavailability of the train, following repair, and a small common cause failure probability of this train and the remaining trains. In the shutdown alternative, if repair is assumed during the cold shutdown state, the risk level will be lower than that shown in the figure, but the integrated risk over the time period will still be larger compared to repair being completed in the power operation state.

In this figure, the repair time is assumed to be 12 hours, which is the mean repair time assumed in the plant PSA. If repair can be performed quickly, then staying in full power state is the effective, and

a less complicated strategy to reduce the risk from such a situation. However, if the repair time is long, then this advantage is lost.

Influence of Keeping Successfully Tested Train in Operation

One strategy may be to keep the successfully tested train in operation for the duration of repair in the full power operation state or when the plant is being moved from power operation to shutdown state. This option will be attractive if the contribution of failure in the "run" mode is significantly lower compared to that in the "standby" mode. The risk levels calculated for each of the failure situations in the SSW system are presented in Figure 6.4. Figure 6.4 presents a comparison of CDF and cumulative CDP as a function of repair time for single and double failures in the SSW systems when remaining trains are either in standby or kept operating following a successful test. In the figure, the cases labeled 'SB' means that remaining trains are in standby following a successful test and 'OO' means that remaining trains are operating following a successful test. The top figure shows comparison of the continued operation and shutdown alternatives for single and double failures in SSW system; in all cases the CDF level when the remaining trains are kept operating is slightly lower. The bottom curve, where the core damage probability impact over the repair time is presented, shows similar results, i.e., the effect of keeping the successfully tested trains in operation is comparable or marginally better.

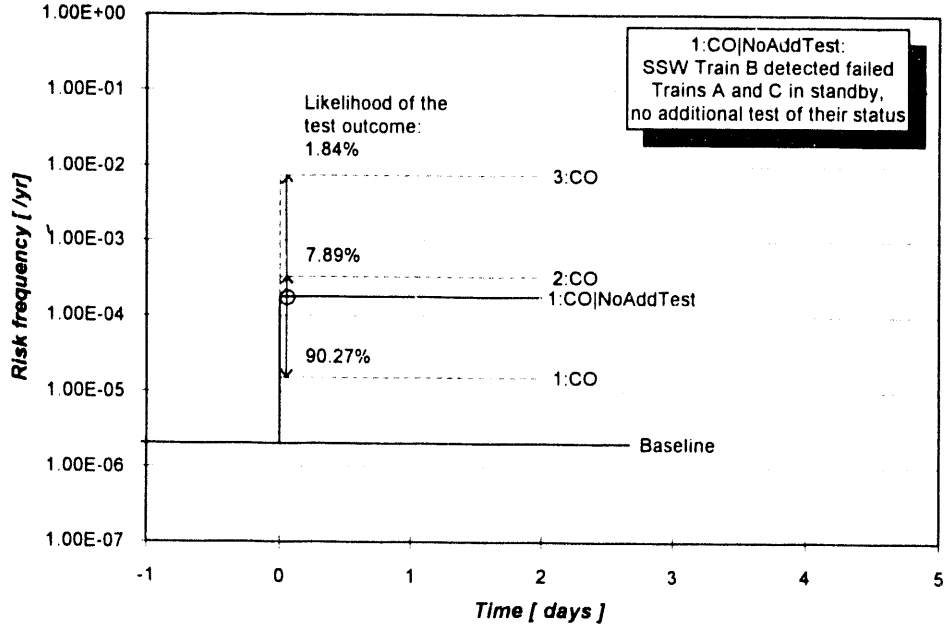
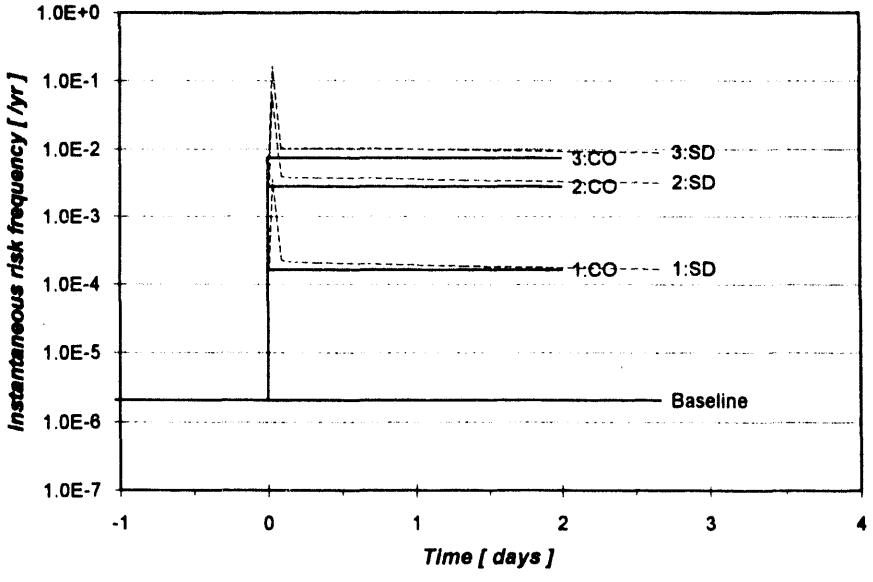


Figure 6.1. CDF level for SSW Train B failure and the effects of additional tests and test results



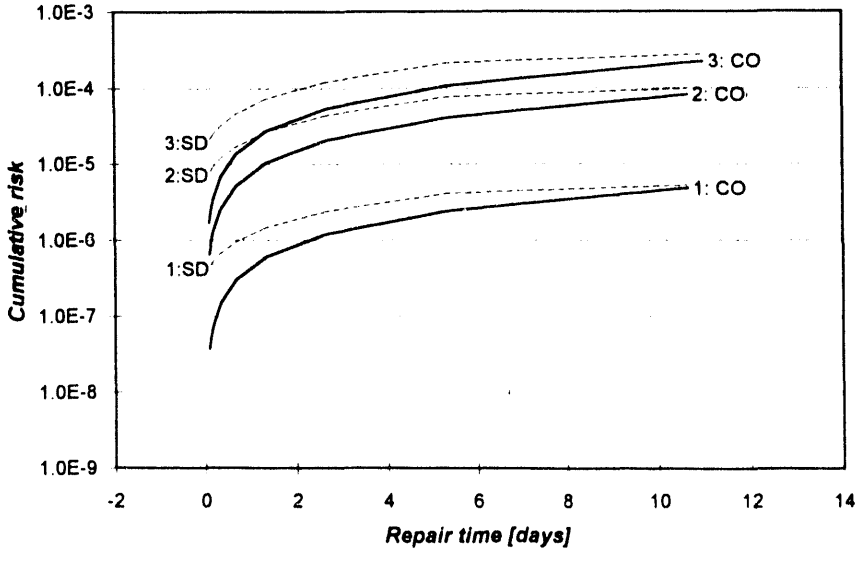


Figure 6.2. CDF and cumulative CDP as a function of repair time in SSW pump train failure situations: the status of remaining trains is not know (no additional test)

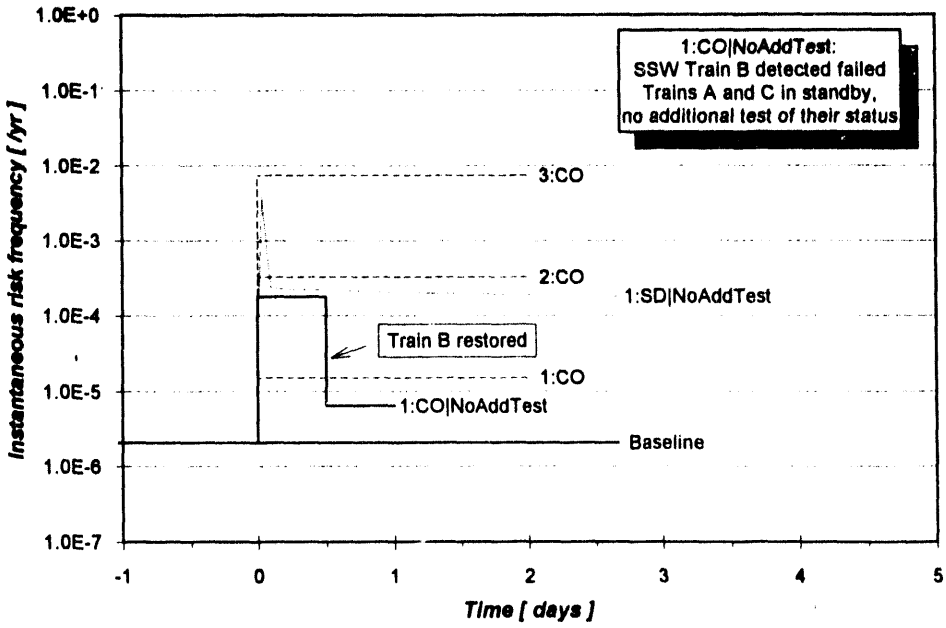


Figure 6.3. Decrease in CDF when repair of SSW Train B is completed first. Decided shutdown alternative without recovery is represented by 1:SD/No add Test

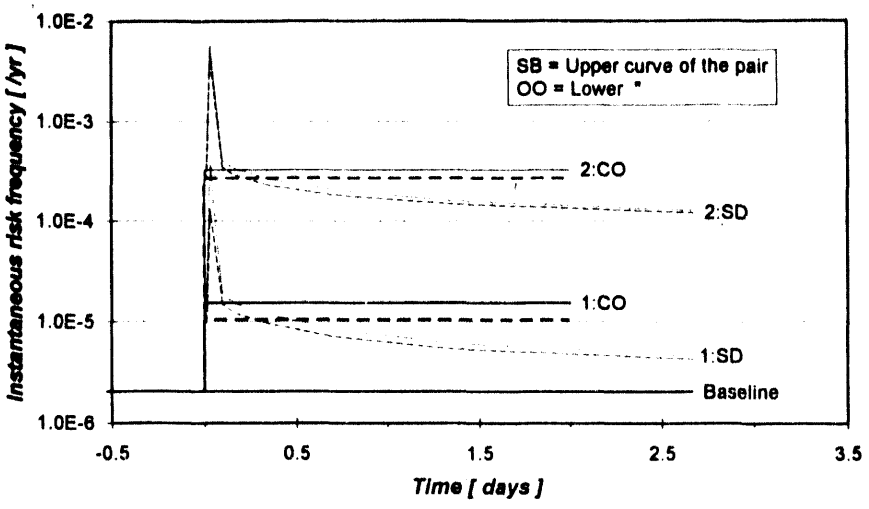
6.4 Analyses of Alternate Plant Shutdown Schemes in Critical Failures

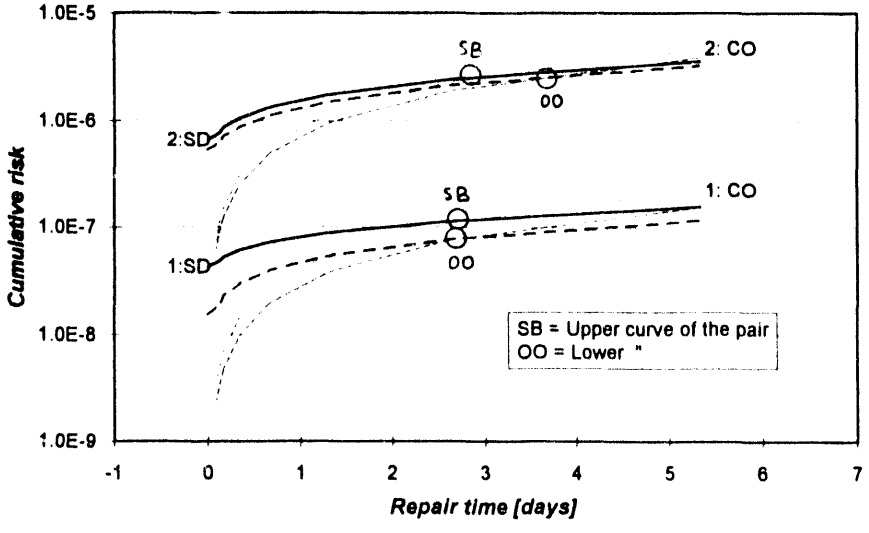
In this chapter, we analyze the details of the plant shutdown scheme to be followed, if shutdown is decided or required because AOT is exceeded. Since the risk of shutting down in these failure situations is significant, the objective here is to identify specific procedural steps that may be followed to minimize the risk in these situations. Our focus, as discussed, is on two aspects:

a) What is the preferred target state (hot shutdown vs. cold shutdown with ADHRS available) in these failure situations?

b) What is the effect of delay in initiating a controlled shutdown?

Sensitivity analyses performed to answer these issues are presented below along with the insights for recommending action requirements for failure situations in the RHR/SSW systems.





SSW Train B failure case

Expected risk	Remaining RHR/SSW trains	
	In standby	Operating
R_CO	2.28E-08	1.57E-08
R_SD	5.67E-08	2.67E-08
SD/CO	2.49	1.70

SSW Trains A&B failure case

Remaining RHR/SSW trains	
In standby	Operating
4.48E-07	3.69E-07
9.63E-07	7.97E-07
2.15	2.16

Figure 6.4. Comparison of CDF and cumulative CDP over predicted repair time in SSW pump train failure situations: RHR/SSW trains are either restored to standby or kept running after successful tests

6.4.1 Comparison of Risk Impacts of Staying in Hot Shutdown Versus Proceeding to Cold Shutdown with ADHRS Available

The action statements in the LCOs typically require that the plant be brought to the cold shutdown within a defined time period if the repair is not completed within the AOT. The same requirements apply for RHR/SSW systems. In case of failures in RHR/SSW systems, since the risk of transferring to a cold shutdown state is large, it is important to evaluate the relative advantage/disadvantage of repairing the failed equipment in these states. Table 6.2 presents the definition of different shutdown states being considered and a summary of benefits/disadvantages for each of the states. The definitions of the shutdown states in terms of the plant variables (power, pressure, temperature, decay heat, etc.) and in relation to the POS definitions are presented previously. For this analysis, the shutdown states being considered are:

Hot SD. F: Hot Shutdown, Full Pressure State (POS 2)
Cold SD. N: Cold Shutdown, RHR/SDC is nominally used (POS 5)
Cold SD. A: Cold Shutdown, ADHRS aligned for RHR (POS 5)

Hot SD. F Alternative

In this alternative, the controlled LCO shutdown is targeted to stay in POS 2 with

- zero reactor power (only decay heat),
- full reactor pressure and temperature (950 psig and 540°F),
- turbine condenser used as a decay heat sink, TBVs are in manual control and MF pumps are aligned for low rate coolant makeup,

i.e., no reactor cooldown is undertaken. In this condition, the reactor is at zero power with diminishing decay heat production, which increases time margin for a recovery in any later critical failure combination occurring while in the hot shutdown state.

The advantages of this alternative, in comparison with the nominal LCO shutdown to a cold shutdown state (Cold SD. N) are the following:

a) Disturbance transients related to reactor cooldown are avoided (especially loss of PCS, LOCAs induced by reactor cooldown)

b) Standby RHR systems need not be challenged. This is particularly relevant, if the normal RHR path is inoperable, and alignment to the use of ADHRS or some improvised RHR path would be needed when entering the cold shutdown state.

On the other hand, the main disadvantage of this alternative is that there is an increased likelihood of full pressure initiating events such as LoPCS, IORV and full pressure LOCAs during this period (which are effectively excluded in Cold SD state). An extended time in Hot SD.F may impose operational problems such as in preserving condenser vacuum, regulating small feedwater flow and controlling radiolysis gas in the RCS.

Table 6.2. Definition of Shutdown (SD) Target States

SD Target State	Definition	Benefits	Disadvantages
Hot SD. F	Hot shutdown, full pressure state (POS 2)	PCS used as heat sink, standby RHR systems not directly needed	Increased likelihood of full pressure initiating events (loss of PCS, IORV and LOCAs) as well as high frequency of LOSP and loss of IAS
Cold SD. N	Cold shutdown state, RHR/SDC is nominally used (POS 5)	Preferable stable state, when 1 SSW train available	RHR/SDC function disabled if RHR/SSW trains A and B failed
Cold SD. A	Cold shutdown state, ADHRS aligned for RHR (POS 5)	More stable than prolonged use of PCS (if RHR/SDC is inoperable)	No clear procedure exists for use of ADHRS in this way

Cold SD. A Alternative

In this alternative, pressure reduction and reactor cooldown take place without any unnecessary delay in order to quickly enter the operational range of ADHRS, or other alternate flow alignment options within RHR, ADHRS and RWCU flow paths. The principal benefit is that the full pressure state initiating events are excluded (compared to Hot SD. F alternative above). The disadvantages include the following:

a) Transient risk of the reactor cooldown phase is incurred,

b) The use of PCS may be very unstable or excluded in the nonpressurized state,

c) Risk of flow alignment errors exists,

d) Special leak initiators or (such as loss of reactor coolant inventory to suppression pool or to fuel pool) are possible when aligning ADHRS.

Results of Sensitivity Analyses

Quantitative evaluation of the alternative shutdown states was performed for the double failure situation in the SSW system. Both the instantaneous core damage frequency and the cumulative core damage contribution are studied and presented in Figure 6.5.

As shown, staying in Hot SD. F is least desirable, and moving quickly to POS 5 in order to be able to use ADHRS (Cold SD. A) is the most preferable option. About 80% of the risk related to the plant state change is due to the power reduction from full power to Hot SD. F. The CDF in Hot SD. F is about a factor of 2 higher when compared to the cold shutdown state, Cold SD. N. This is because of higher frequency of critical, high pressure initiating events, e.g., LOSP and loss of IAS.

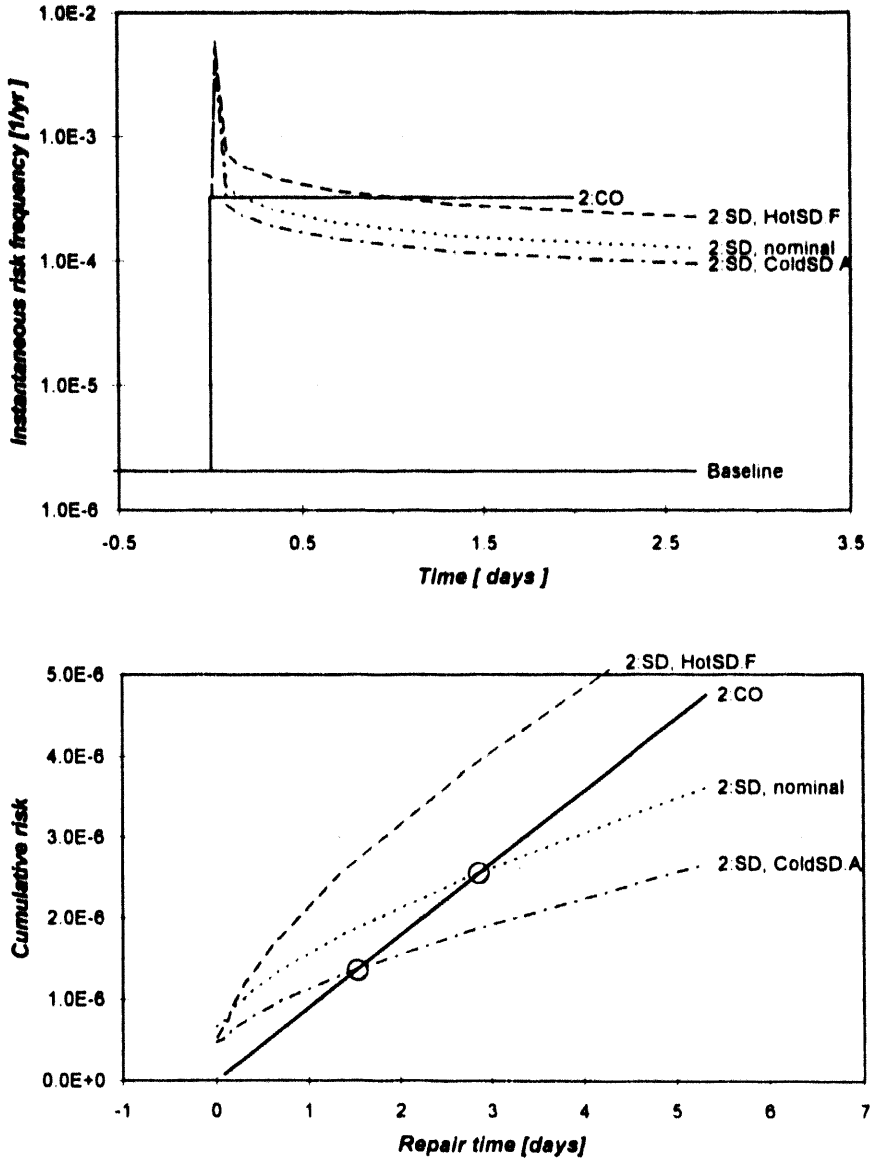


Figure 6.5. Comparative analysis of staying in HotSD. F for repairs of alternatively going to POS 5 in order to use ADHRS (ColdSD.A): double failures in SSW system

Going quickly to POS 5 such that ADHRS can be used, results in reduction of the accumulated risk over the period. Thus, when the use of ADHRS is possible, the shutdown alternative may become preferable. This is particularly so, when otherwise, e.g., in triple failure situations, the risk of shutdown is comparable to the continued operation alternative.

6.4.2 Effect of Delay in Shutdown in Failure Situations

In practice, when the need of an LCO shutdown is identified, some time should be allowed for orderly shutdown preparations. This is usually taken into account in the action statements, which may require, for example, reaching hot shutdown conditions within the next 12 hours and cold shutdown conditions within the following 24 hours. The time required for

- controlled power reduction is about 3 hours (from full power state to hot shutdown conditions)
- reactor cooldown phase is about 3-4 hours (from hot shutdown with full pressure conditions to cold shutdown)

Consequently, the needed time from the identification of the LCO shutdown to the start of power reduction may be about 6-7 hours.

The time allowed in TS action statements (as stated, a maximum of 36 hours) to reach cold shutdown is typically the same for all LCO conditions. The intent in allowing this duration is to assure an orderly shutdown, but, in the failure situations we are discussing, it may be desirable to reduce the incurred risk by reducing the allowed times, as a special case. This will also assure special attention to shutdown, when decided in such situations, as may be desirable. In this chapter, we analyze the effect of delay in initiating a shutdown to justify reduction in the allotted time to achieve a shutdown.

Risk Effect of Delay in Initiating a Shutdown

Delaying initiation of shutdown, in case of failures in RHR/SSW systems, means that during the time lag risk will accumulate in the full power state at the increased risk level resulting from the failure condition. Essentially, this risk will add to the risk of shutdown to determine the total risk in these situations.

The influence of delaying shutdown up to the allowed maximum (to be in hot shutdown within the next 12 hours and cold shutdown within the following 24 hours) is analyzed for double failure situations in SSW system and presented in Figure 6.6. The cumulative risk when the allowed maximum delay time is used is equivalent to the cumulative risk of about 3 days in the full power state. The combined effect of repair time delay and the delay in initiating a shutdown adds to the total risk in such a situation, and to the disadvantage of shutdown alternative. This result shows the need for reducing the allowed time for achieving a shutdown for these special cases. But, at the same time, the time allowed should be sufficient to allow an orderly, planned SD and hence not incur additional risk during the SD.

6.5 Insights on Operational Procedures and Action Requirements

The insights obtained on operational procedures and action requirements based on sensitivity analyses can be summarized as presented below. These insights are particularly applicable to RHR/SSW

systems in the Grand Gulf nuclear power stations, and are also considered generally applicable to all BWRs of similar design, i.e., BWR/6.

- The risk of the available alternatives when failures are detected in RHR/SSW systems is significant, and operational procedures can be defined to minimize the overall risk implication for these situations. LCO requirements within the TS can be redefined to assure that risk-effective actions are taken.

- In these failure situations the most risk effective measure is to restore the initially detected failed component. Thus, first priority will be to quickly repair the initially failed train or at least one train of the system, when multiple trains are detected failed. This implies that reasonable, but relatively short AOT should be defined for double or triple failures in RHR/SSW systems. As noted elsewhere, care should be taken that the defined AOTs when increased number of failures are observed are not larger than AOTs for a lesser number of failures.

- When longer repair time is needed, then other measures are necessary before repair is performed. Shutdown may be desirable rather than repair at power, considering the overall risk. Thus, it is important to determine if repair can be performed quickly, or if longer repair time may be required. To consider such an operational procedure, the AOT may be split into two phases, where the first phase of approximately 24 hours is used to assess the repair time needed, i.e., diagnosis of the problem and to complete short repair. The use of the second phase depends on other measures discussed below.

- For longer repair times, the condition of redundant train(s) should be determined. This will check for the presence of any common cause failures, and conversely, if the redundant train is successfully tested, then an alternate success path will be assured. The test of the redundant train can be required to be performed at the end of the first phase of AOT, and the second phase of the AOT can be used to complete repair. To avoid any adverse effects of testing, an actual demand test may be preceded by a diagnostic checking.

- Shutdown may be needed if the repair time needed is too long to be acceptable. To avoid the risk of a long repair time in power operation in addition to the risk of shutdown, the decision to shutdown, if considered evident, should be made as soon as possible. This again is the reason to split the AOT in two phases, where the decision to shutdown can be made by the end of the first phase.

- When going to shutdown, the intent should be to reach cold shutdown state where ADHRS can be used. To minimize the risk, availability of PCS should be maintained and availability of ADHRS may be assured during the transition from full power to cold shutdown state. In addition, to reduce the risk of LOSP transients, power reduction should be initiated when the external grid is considered stable.

- For the failure conditions analyzed here, the calculated core damage frequency in the hot shutdown state is large and time in this state should be minimized. Any attempts to repair failed equipment prolonging stay in the hot shutdown state should be avoided. In principle, if and when the need for shutdown is evident, cold shutdown state should be achieved as quickly as possible. The time currently allowed in LCO requirements (a total of 36 hours) to reach cold shutdown should be reduced in these special cases.

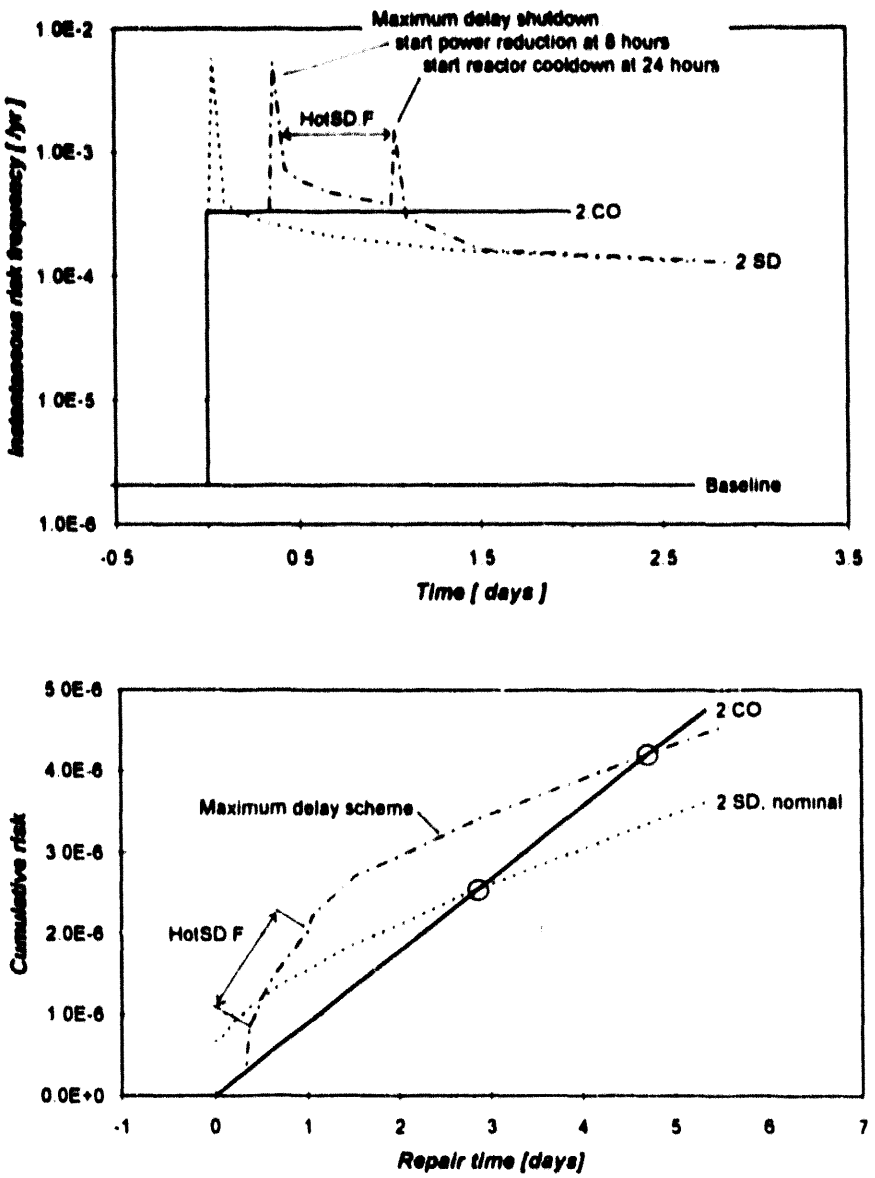


Figure 6.6. Influence of maximum delay in the stages of an LCO shutdown (requirement to reach hot shutdown within the next 12 hours and cold shutdown conditions within the following 24 hours): double failure in SSW system

7. SUGGESTED RECOMMENDATIONS FOR RISK-BASED ACTION STATEMENTS FOR RHR/SSW SYSTEMS

Our analyses of the risk impact of action statements, based on the Grand Gulf Nuclear Power Station Technical Specifications, led us to several insights regarding improvements in action statements. These insights can be summarized as follows:

a) AOT should be provided to repair at least one of the failed components when multiple failures are detected, i.e., as for a single failure, multiple failures should also have an AOT. This is different from current TS requirement of immediate shutdown in case of multiple failures in RHR/SSW systems. However, the AOT for multiple failures should be less than that for single failures.

b) The use of an AOT should be defined in the following manner (refer to Figure 7.1). A small portion of the AOT should be used to complete short repairs or to determine the repair needs. At the end of the first phase of the AOT, shutdown may be initiated if the needed repair time is considered longer than the AOT or additional tests may be performed where depending on the test outcome applicable AOT should be followed.

c) When all three trains of SSW system or both RHR trains are failed and shutdown is decided, the availability of alternate decay heat removal system should be assured and the plant should be moved to the cold shutdown state as soon as possible, whereby the alternate decay heat removal (ADHR) system can be used. This insight is applicable to plants with an ADHR system.

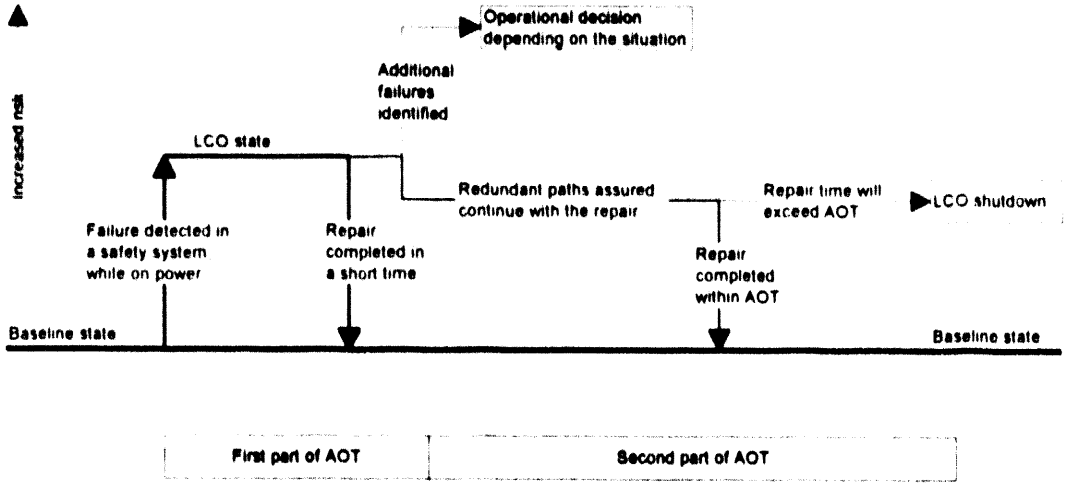


Figure 7.1 Splitting the allowed outage time (AOT) into two parts for a failure affecting risk. The first part of the AOT is to repair or diagnose the failure. Use of the second part of the AOT to complete the repair while generating power is dependent on the successful outcome of assuring redundant operation paths.

d) For these situations, the allowed time to move to hot SD and then to cold SD, a maximum of 36 hours, can be reduced to 12-18 hours. This time period is considered practical, but, at the same time, makes clear the urgency to achieve cold shutdown as quickly as possible.

e) However, if the risk impact of the failures is small, i.e., small risk is incurred for either continuing operation or plant shutdown, then the TS requirements can be relatively simple and flexible for implementation. This condition applies, for example, to failures in the RHR system of the Grand Gulf Nuclear Power Station studied in this report.

Along with these risk insights, there are a number of practical considerations that also should be taken into account in considering possible changes in these requirements.

a) If an AOT is defined, it must be of sufficient duration to allow completion of a large percentage (approximately 90%) of repair needs. This is to avoid any adverse effect of incomplete or hurried repair. Such an AOT can be established for example by defining the AOT to be at least three times the mean time to repair.

b) The AOTs chosen should follow discrete values normally used in TS; e.g., 1 day, 2 days, 3 days, 7 days, for ease of implementation. An additional reason for choosing such discrete values is the consideration of uncertainty in PSA-based results, on which the decision is based. These AOT choices are consistent with and less sensitive to PSA uncertainties.

c) Care should be taken that the relative comparison of the operation alternatives is not the only factor in defining the action requirements. If mechanically followed, this approach may result in longer AOTs for multiple failures, thus possibly providing incentives to declare multiple failures when repair for single failures cannot be completed within the prescribed AOT.

d) When AOTs for multiple failures are defined in TS, it implies that, when one failure is repaired, the action for the fewer number of failures would need to be followed. As analyzed in this study, there is a significant risk advantage to repairing one of the failures in the case of multiple failures. In principle, AOTs should reflect this risk perspective, where possible, by consistently defining longer AOTs for fewer number of failures.

e) The requirement for additional testing should take into consideration the adverse effects of testing due, for example, to test errors. If feasible, any diagnostic measure that can determine the condition of the redundant train should precede or replace need for an actual demand test.

f) AOTs defined for these situations, i.e., where either continued operation or plant shutdown is considered to be risky, are carefully decided to keep the total risk (sum of the risk in power operation plus the risk of shutting down) to a minimum. Considering the risk significance of these situations, these rules, once defined, should be followed. Thus, request for one time extensions, for example, near the end of the 2 days of AOT should not be granted. Such extensions can increase risk significantly because of the possibility of incurring the risk of shutdown along with increased risk of continued operation.

7.1 Specific Recommendations for RHR LCO Requirements

Our analysis shows that the risk impact of RHR train (A and B) failures in the Grand Gulf Nuclear Power Station for continuing operation or for shutdown are comparable, but relatively small. Given such a small impact, it is judged that the TS requirements should provide increased operational flexibility and at the same time, remain simple to implement. With this insight, the recommendations for RHR LCO requirements, as presented in Figure 7.2, are directed towards providing reasonable AOT to complete repairs for multiple failures and thereby, reducing the chance for LCO shutdown. It is not clear whether similar results, i.e., the risk impact of RHR train failures is relatively small, will be obtained for other BWRs.

a) An AOT of 7 days for a single RHR train failure appears consistent with its risk impact. This is different from current requirement of 3 days. But a change to 7 days will make this requirement the same for different modes of operation of these trans - low pressure coolant injection (LPCI), suppression pool cooling (SPC), and containment spray (CS). The reason for allowing a long AOT of 7 days is that the core damage probability impact of a single RHR train failure for 7 days is small, approximately 5×10^{-8}.

b) For double failures, an AOT of 3 days appears consistent with its risk impact. This is different from current requirements, where 8 hours or no AOT is granted for these failure combinations. As stated, the reason for allowing 3 days is that the risk impact is small, and 3 days is sufficient to complete necessary repairs to avoid plant shutdown.

c) When shutdown is required, the risk impact is also small, so there are no significant risk benefit of assuring availability of alternate trains or of reaching cold shutdown sooner than standard requirements of 12 hours to reach hot shutdown and another 24 hours to reach cold shutdown.

7.2 Specific Recommendations for SSW LCO Requirements

The recommendations for SSW LCO requirements are presented in Figure 7.3. These recommendations are different than those for the RHR system because the risk impact of SSW train failures is much larger than that of for RHR-train failures. Specific aspects of these requirements are as follows:

a) Current AOT requirements for a single SSW train failure is 3 days. Based on the results of our study, this AOT can remain the same with the additional condition that by the end of the first day redundant trains are tested to assure that there are no additional failures. If repair of the first detected failure is completed within the first day, then no additional tests are required. Also, as discussed previously, if feasible, any diagnostic measure that can determine the condition of the redundant train(s) should precede or replace need for an actual demand test.

   The recommended AOT above (of 3 days) for single SSW failure is smaller than that recommended (7 days) for similar failure in the RHR system. This is consistent with the core damage frequency impact obtained for these failure conditions; the effect of single SSW train failure is approximately a factor of 5 larger compared to single RHR train failure.

b) The SSW trains are tested relatively frequently during power operations because SSW trains are run for chemical additive mixing and to test other safety system components. The recommendation to test redundant SSW trains(s), when a failure in one SSW train is detected, item (a) above, should not result in unnecessary additional testing of SSW trains. This recommended test can be skipped, if a successful test has already been performed, for other reasons as discussed above, in the previous 72 hours, and if there is no clear indication of a latent CCF.

c) Current TS distinguishes among different double failure combinations; for example, 3 day AOT is given for failure of SSW trains A and C, and B and C; but shutdown is required for failure of SSW trains A and B. Similarly, shutdown is required for failure of all three SSW trains. Based on the results of our study, the recommended AOT for double and triple failures in SSW system is 2 days. With this change, the AOT for all double failures in the SSW system will be the same. This is justified because the core damage frequency impacts of different double failure combinations are similar.

In using this 2 days AOT for double and triple failures in the SSW system, a judgment needs to be made at the end of the first day whether repair of one of the trains can be completed by the end of the second day. If by the end of the first day it is judged that repair of one of the trains cannot be completed by the end of the second day, then shutdown should be initiated immediately.

d) For multiple failures, if the repair time is expected to exceed a total of 2 days, then shutdown should be initiated at the end of the first day and cold shutdown should be reached within the next 12 hours. The time to reach cold shutdown is different than that currently allowed (12 hours to reach hot shutdown and 24 hours to reach cold shutdown), because to minimize the risk impact, cold shutdown state, in these cases, should be reached as quickly as possible. For the Grand Gulf Nuclear Station, designed with an ADHR system that can be used during cold shutdown, the availability of this system should be assured prior to initiating a shutdown when all three trains of SSW are failed.

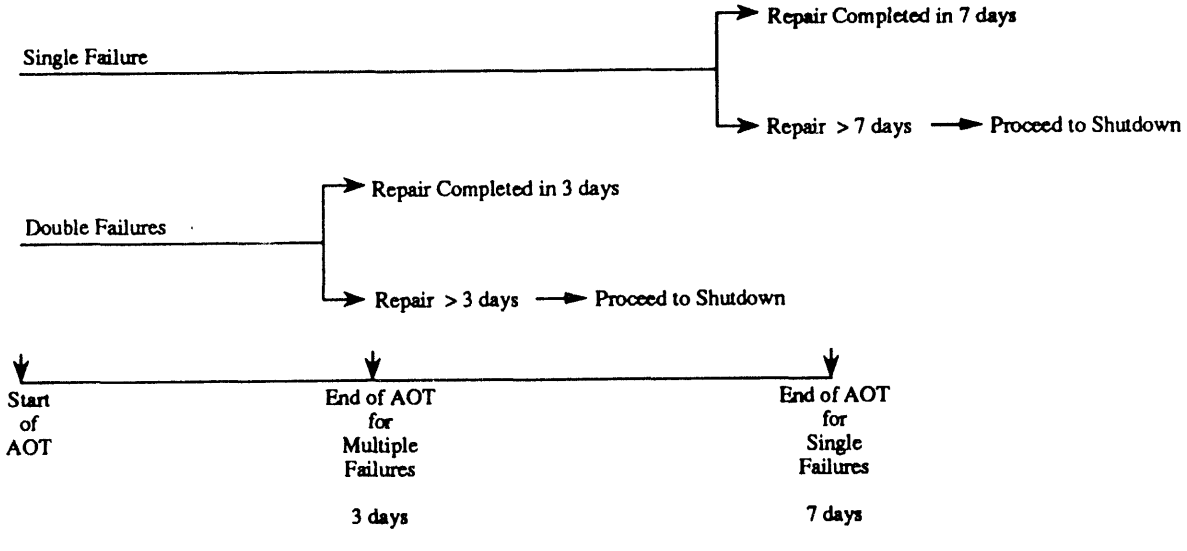


Figure 7.2 Recommendations for RHR LCO requirements (Trains A and B)

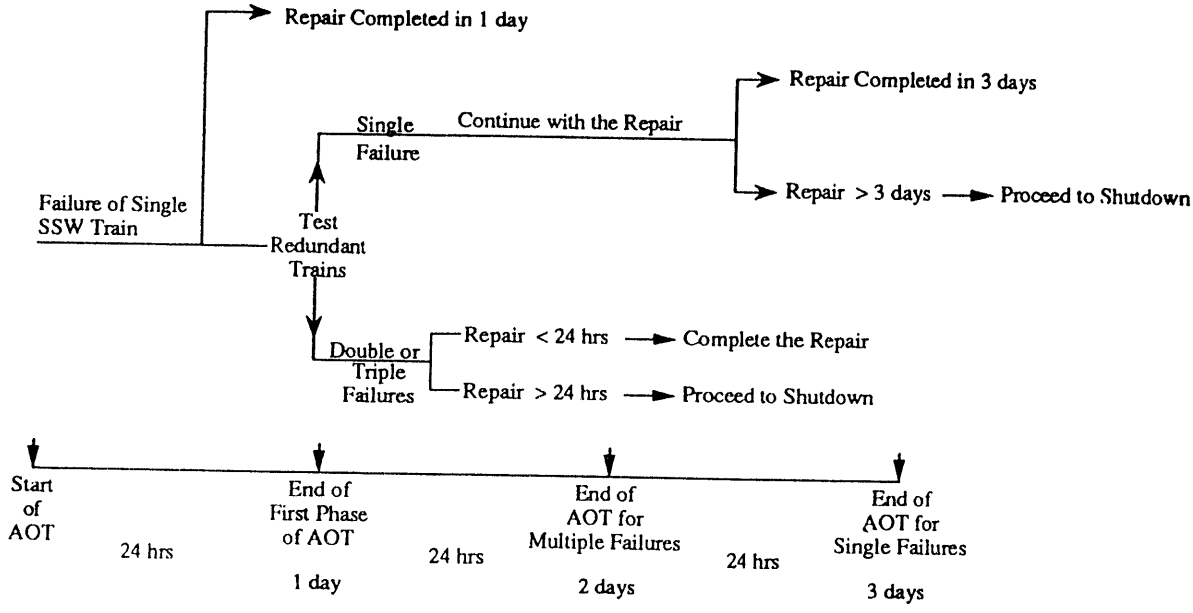


Figure 7.3 Recommendations for SSW LCO requirements

8. SUMMARY AND CONCLUSIONS

In this report, we presented a method to analyze the risk implications of limiting conditions for operation (LCOs) and associated action statements of technical specifications requiring shutdown when the plant has insufficient capabilities for removing decay heat. The method, called risk-comparison approach, allows evaluation and comparison of the risks of the basic operational alternatives (i.e., continued operation or plant shutdown) in failures of systems needed to remove decay heat. Also, it can be used for sensitivity analyses to determine risk-effective LCOs, action statements, and allowed outage time (AOT) for such failure situations. The results of this study do not reflect any position or policy of the US Nuclear Regulatory Commission on technical specifications; rather, they include recommendations that would need to be considered in light of the existing legal and regulatory requirements for technical specifications.

The approach consists of the following steps: (1) model event sequences in terms of shutdown transient diagrams (STDs) and extended event sequence diagrams (EESDs) for both a controlled LCO shutdown (SD), and continued power operation (CO) with equipment inoperable; (2) quantify the risk impact of the event sequences from the diagrams with explicit consideration of time dependencies, such as the time available for recovery actions and component repair-time distributions; (3) compare the instantaneous and cumulative risks for SD and CO alternatives for a given failure situation; and (4) determine risk-effective action requirements by evaluating various operational policy alternatives, such as testing of redundant trains or timing of shutdown, in terms of sensitivity study. As compared to conventional methods of analyzing risk, (e.g., probabilistic safety assessment (PSA) based on event tree-fault tree) this approach allows a detailed treatment of shutdown cooling phases that challenge the plant's capabilities for removing decay-heat.

The risk-comparison approach was applied to residual heat removal (RHR) and standby service water (SSW) systems of a BWR. From the risk quantification of failures in the RHR/SSW systems, we gained the following insights on the LCO risk impacts:

(1) Compared to failures in the RHR system, those in the SSW system incur much higher operating and shutdown risks because complete or partial failure of the SSW system also fails or degrades some front-line systems (i.e., the HPCS, LPCS, RCIC and RHR systems) through loss of pump and room cooling, and the support AC-power system (i.e., diesel generators) through loss of jacket cooling. This insight on the importance of service water is similar to the findings of the Risk-based Inspection Guide (RIG) Program.[17]

(2) When the SSW system is failed or degraded, the analyses show that shutdown poses a higher risk than continued operation over the mean repair time, especially for a complete failure of the system. However, the difference in risk between shutdown and continued operation may not be significant in light of uncertainties in the risk evaluation.

(3) Single or double failures in the RHR subsystems for removing decay heat (i.e., trains A and B) increase the risk only slightly above the baseline level, even if the plant continues power operation with the equipment inoperable. When the plant is shut down, the risk initially increases above the corresponding risk for the CO alternative, but declines quite rapidly as the decay heat diminishes. Considering the small increase in risk for continued operation and also the larger cumulative risk over mean repair time for shutdown compared to the CO alternative, sufficient AOTs may be given to these failures so that,

in most cases, plant personnel could restore the operability of failed equipment within the allowed downtime without shutting down the plant. The current technical specifications of Grand Gulf gives 3 days of AOT for single failures in the RHR trains for decay-heat removal, and 8 hours for double failures; the latter, especially, may need extension. Also, insufficient AOTs are given in current technical specifications of most plants, especially for multiple failure situations in important systems; some may be relaxed, based on the risk evaluations of the specific failure situations.

(4) The present AOTs for the RHR and SSW systems do not reflect the large differences in the risk impacts. For example, the LCO operating risk for SSW subsystems B and C being inoperable is almost three orders of magnitude larger than that for one of the two RHR/SPC subsystems. However, the same AOT (3 days) is given for these failures.

The evaluation of risk for failures in the SSW system, especially multiple failures, indicate that the LCO risk is considerable for both basic operational alternatives, i.e., continued operation and shutdown. To identify risk-effective LCOs and possible actions that will minimize the overall risk impact associated with the failures, sensitivity analyses were performed. Specifically, the following issues, among others, were addressed: (1) requirement for testing redundant trains, (2) guidance on the use of AOT, and (3) optimum target state of LCO shutdown.

From the sensitivity analyses, we reached the following conclusions that might be generically applicable to nuclear power plants:

(1) An additional test requirement of redundant trains may be imposed, especially when long repairs are expected. This test will allow early detection of common-cause failure (CCF) as well as better understanding of the plant's status. When CCF is detected, measures to mitigate potential adverse effect, such as checking or assurance of another success path, can be taken as quickly as possible. Alternatively, if the outcome of the test is success, a longer AOT may be given to complete the repair in the power operation state.

(2) Guidance may be given on the use of the AOT. For example, when the AOT is 3 days, the first 24 hours may be used to complete short repairs, diagnose the problem, or assess the repair time needed. If the operability of the equipment cannot be restored within the first day, then a test of redundant trains, whose status is unknown, may be conducted at the end of the first day after entering the LCO.

(3) When the failure situation is such that shutdown is inevitable, then the plant should be shut down as early as possible to avoid accumulating risk while in continued operation with equipment inoperable.

(4) For the failures analyzed, the risk in the hot shutdown state is relatively high, and so the time in this state should be minimized. By the same token, when the shutdown alternative is taken, the plant should proceed to cold shutdown, where component repairs may be made. By quickly entering this state, the benefit of diminishing decay-heat production and the possibility of using alternate paths of decay-heat removal will be maximized.

Other insights and specific recommendations to improve LCOs and action requirements for the RHR/SSW systems of the BWR plant studied also were presented in Chapter 7.

This study addressed RHR and SSW systems of a BWR. For a PWR, this method could be applied to (1) the auxiliary feedwater system which provides feedwater to steam generators to remove core heat from the primary system after reactor trip; (2) the RHR system that provides long-term removal of decay heat; (3) the component cooling water (CCW) system that provides cooling water to the RHR system; (4) the service water system that subsequently removes heat from the CCW system; and (5) the emergency power system that provides AC and DC power to safety-related components following reactor scram. In addition to the plant-specific action statements, the method also may be applied to improve the action requirements of standard technical specifications.

In conclusion, the action statements requiring shutdown, when the plant has degraded capabilities for removing decay heat, can be evaluated from a risk perspective. The method for comparing the risk of continued operation and the risk of shutdown can help to improve the bases for such technical specifications action statements.

REFERENCES

1. T. Mankamo and M. Kosonen, "Continued Plant Operation Versus Shutdown in Failure Situations of Standby Safety Systems," IAEA/TechSpec Pilot Study Program, NKS/SIK-1(91)4, August 1991.

2. T. Mankamo, "Phased Operations and Recovery Options - Advances in Event Sequence Quantification," Proc. International Topical Meeting on Probability, Reliability, and Safety Assessment, PSA '89, Pittsburgh, PA, April 1989, pp 1131-1137.

3. T. Mankamo, "Operational Decision Alternatives in Failure Situations of Standby Safety Systems Development of Probabilistic Approach and PC Program TeReLCO," Reliability Engineering and System Safety, Vol. 36 (1992), pp 29-34.

4. P.K. Samanta, S.M. Wong, and J. Carbonaro, "Evaluation of Risks Associated with AOT and STI Requirements at the ANO-1 Nuclear Power Plant," NUREG/CR-5200, BNL-NUREG-52024, August 1988.

5. B. Atefi and D.W. Gallagher, "Feasibility Assessment of a Risk-Based Approach to Technical Specifications," NUREG/CR-5742, SAIC-90/1400, Vols. 1-2, May 1991.

6. P.K. Samanta, W.E. Vesely, and I.S. Kim, "Study of Operational Risk-Based Control," NUREG/CR-5641, BNL-NUREG-52261, August 1991.

7. D.W. Whitehead, J. Darby, B. Staple, et al., "Draft Letter Report for Phase 1 of the Low Power and Shutdown Accident Sequence Frequencies Project," Sandia National Laboratories, June 1991.

8. D.W. Whitehead, et al., "BWR Low Power and Shutdown Accident Sequence Frequencies Project: Phase 2 - Detailed Analysis of POS 5," Sandia National Laboratories, August 31, 1992.

9. T.L. Chu, Z. Musicki, W. Luckas, et al., "PWR Low Power and Shutdown Accident Frequencies Program: Phase 1 - Coarse Screening Analysis," Brookhaven National Laboratory, Draft Report, June 1991.

10. T.L. Chu, G. Bozoki, P. Kohut, et al., "PWR Low Power and Shutdown Accident Frequencies Program: Phase 2 - Internal Events," Brookhaven National Laboratory, Rough Draft Letter Report, August 31, 1992.

11. J.H. Holderness, K.D. Kimball, J.D. Durham, et al., "Brunswick Decay Heat Removal Probabilistic Safety Study," Nuclear Safety Analysis Center, NSAC-83, October 1985.

12. D.C. Bley, J.W. Stetkar, L.A. Bowen, et al., "Zion Nuclear Plant Residual Heat Removal PRA," Nuclear Safety Analysis Center, NSAC-84, July 1985.

13. F.R. Hubbard III, M.A. Waller, and D.J. Wakefield, "The Use of Event-Sequence Diagrams in Probabilistic Risk Assessment," Trans. American Nuclear Society, TANSAO 60 1-792, San Francisco, CA, November 26-30, 1989, pp 407-408.

14. M.A. Stutzke, J.C. Plunkett, and E.M. Dougherty, "RIMS -- A Software Tool for IPE and Accident Management," Proc. International Conference on Probabilistic Safety Assessment and Management (PSAM), Vol. 2, Beverly Hills, CA, February 4-7, 1991, pp 1039-1043.

15. M. Drouin, J.L. LaChance, B.J. Shapiro, et al., "Analysis of Core Damage Frequency: Grand Gulf, Unit 1 Internal Events, NUREG/CR-4550, SAND86-2084, Rev. 1, Vol. 6, September 1989.

16. U.S. Nuclear Regulatory Commission, "Technical Specifications - Grand Gulf Nuclear Station Unit No. 1," NUREG-0926, Rev. 1, August 1984.

17. J. Usher and A. Fresco, "Grand Gulf Nuclear Station Unit 1 Probabilistic Risk Assessment-Based System Inspection Plans," Brookhaven National Laboratory, Technical Report A-3453-87-5, September 1987.

APPENDIX A

ACRONYMS AND INITIALISMS

AC	alternating current
ADHRS	alternate decay heat removal system
ADS	automatic depressurization system
AFW	auxiliary feedwater
AOT	allowed outage time
ATWS	anticipated transients without scram
BD	blowdown (reactor steam relief to suppression pool)
BWR	boiling water reactor
CCF	common cause failure
CCI	common cause initiator
CCW	component cooling water
CDF	core-damage frequency
CDP	core-damage probability
CDS	condensate system
CO	continued operation (of the plant)
ColdSD	cold shutdown
CoOPS	containment over-pressurization state
CoPRe	containment pressure relief
CoreD	core damage
CRD	control rod drive
CS	containment spray
CST	condensate storage tank
CVS	containment venting system
DC	direct current
DecSD	decided shutdown
DG	diesel generator
ECCS	emergency core cooling system
EESD	extended event sequence diagram
EP	emergency power
ESD	event sequence diagram
FESD	functional event sequences diagram
FrW	firewater
FrWS	firewater system
FW	feedwater
FWS	feedwater system
HotSD	hot shutdown
HPCS	high pressure core spray
HPM	high pressure mode (of reactor coolant supply)
IAS	instrument air system
IORV	inadvertent opening of relief valve
ISC	initiating event of shutdown cooling

LCO	limited condition for operation
LOCA	loss of coolant accident
LOCA.S	small loss of coolant accident
LOCA.M	medium-size (or intermediate) loss of coolant accident
LOCA.L	large loss of coolant accident
LoCC	loss of core cooling
LoEG	loss of external grid
LoFW	loss of feedwater
LoIAS	loss of instrument air system
LoPCS	loss of power conversion system
LoRHR	loss of residual heat removal
LOSP	loss of offsite power
LoSPC	loss of suppression pool cooling
LPCI	low pressure coolant injection
LPCS	low pressure core spray
LPM	low pressure mode (of reactor coolant supply)
MCS	minimal cut set
MSIV	main steam isolation valve
NMF	near mission failure
PCS	power conversion system
POS	plant operational state
PSA	probabilistic safety assessment
PTrip	plant trip
RCIC	reactor core isolation cooling
RCS	reactor coolant system
RHR	residual heat removal
RHR/CS	containment spray mode of the RHR system
RHR/SDC	shutdown cooling mode of the RHR system
RHR/SPC	suppression pool cooling mode of the RHR system
RIG	risk-based inspection guide
RPS	reactor protection system
RWCS	reactor water cleanup system
SBO	station blackout
SC	shutdown cooling
SCS	shutdown cooling system
SD	shutdown (of the plant)
SDC	shutdown cooling
SED	sequence of events diagram
SP	suppression pool
SPC	suppression pool cooling
SPMU	suppression pool makeup
SRV	safety relief valve
SSLD	safe shutdown logic diagram
SSW	standby service water

SSW-X	standby service water cross-tie
STD	shutdown transient diagram
SW	service water
TBV	turbine bypass valve
TraCSD	transfer to cold shutdown
TS	technical specifications
UnFW	feedwater unavailable

APPENDIX B

SYSTEMS FOR DECAY HEAT REMOVAL

LIST OF FIGURES

This appendix briefly describes the Grand Gulf systems dedicated to removing decay heat from the reactor or other parts of the plant, i.e., residual heat removal system and alternate decay heat removal system.

B.1 Residual Heat Removal System[1,2,5]

The function of the residual heat removal (RHR) system is to remove decay heat from the plant--specifically the reactor, containment and suppression pool--during normal and abnormal conditions. This system can be operated in four main modes: shutdown cooling, suppression pool cooling, containment spray modes, and low pressure coolant injection. Each of these is described along with the common characteristics of the RHR system.

B.1.1 Shutdown Cooling

During a reactor shutdown, reactor cooldown is accomplished initially by condensing reactor steam using the main condenser as the heat sink. When the nuclear steam temperature has decreased to a point where the steam supply pressure is not sufficient to maintain the turbine gland seal and where main condenser vacuum can no longer be maintained, subsequent cooling is accomplished with the shutdown cooling (SDC) loops of the RHR system. This SDC mode has the functional capability to remove decay and sensible heat from the reactor primary system so that the reactor outlet temperature can be reduced to 125 ^{0}F within 20 hours after the reactor is shut down. It is used as necessary to cooldown the reactor vessel water below 125 ^{0}F when the reactor vessel integrity is maintained.

Figure B.1 shows a simplified schematic of the RHR system, with the flow paths for all the operating modes indicated. Many components, including the pumps, are shared among the different modes. The bold lines indicate specifically the flow paths for the SDC mode.

As shown in the figure, the SDC loops A and B each take water through common suction valves from the recirculation loop suction line and returns the cooled water into the reactor vessel. Each suppression pool suction valve and SDC suction valve are interlocked to prevent discharge of the reactor vessel water to the suppression pool.

The SDC system is manually initiated when the reactor pressure is 135 psig or less. LPCI protection is no longer required by the time the SDC system is placed into operation. However, a low reactor water level signal will terminate shutdown cooling automatically and isolate the reactor vessel. The isolation of the RHR system from reactor coolant system will also occur whenever the primary system pressure is above the RHR system design pressure.

B.1.2 Suppression Pool Cooing

Trains A and B of the RHR system can be used to cool the suppression pool, taking suction from the pool and discharging the cooled water back to the pool. This mode of the RHR system, i.e., suppression pool cooling (SPC) mode, is needed to remove heat from the suppression pool, following momentary safety relief valve discharges, or postulated pressure vessel blowdowns or depressurizations to maintain a heat sink and pressure suppression function. The suppression pool cooling is also necessary to maintain a source of cooled water for low pressure injection and core/drywell spray.

Suppression pool cooling may be considered as part of containment cooling function along with the containment spray cooling discussed next. The SPC mode is initiated manually.

B.1.3 Containment Spray

To control temperature or pressure within the primary containment, and after the reactor water level has been restored, the RHR trains A and B may be used to spray water from the suppression pool into the containment and suppression pool vapor space to condense steam and noncondensable gases.

Under accident conditions, a low reactor water level or high drywell pressure will initiate the LPCI mode of the RHR system. Containment spray (CS) operations can be initiated manually only if the reactor water level has been restored by the LPCI operation or if this requirement is overridden by the operator. Once the drywell pressure has been decreased, the containment spray valves can be closed and the system is shut down by manual operator action.

B.1.4 Low Pressure Coolant Injection

In this operating mode of low pressure coolant injection (LPCI), the RHR system provides a safety function to restore and maintain coolant inventory in the reactor vessel at low reactor pressure during loss of coolant accident (LOCA) conditions. As such, it is part of the emergency core cooling system (ECCS). The heat exchangers of the RHR system are bypassed in this mode.

LPCI operation is automatically initiated on low reactor level or high drywell pressure. Upon receipt of a LPCI actuation signal, trains A, B and C injection valves are demanded to open, the test return valves are demanded to close, and then the three RHR pumps will start and take suction from the suppression pool and discharge into recirculation loops.

B.1.5 Common Characteristics

The various operating modes of the RHR system discussed above have common characteristics in terms of isolation from the reactor coolant system and interlocks.

The low pressure portions of the RHR system are isolated from the reactor coolant system whenever the primary system pressure is above the RHR system design pressure. The isolation valves provide protection against uncovering the core if the piping should break in the loops that are connected to the primary system. The valves also protect the piping from high reactor pressure in case of a component malfunction. The isolation valves are designed and constructed to withstand the maximum reactor vessel temperature and pressure. Should a RHR system isolation occur, the position of each isolation valve is indicated on the RHR system isolation panel in the control room.

Interlocks are provided in the RHR system for the following purposes: (1) to prevent drawing vessel water to the suppression pool; (2) to prevent opening vessel suction valves above the suction line or the discharge line design pressure; (3) to prevent inadvertent opening of drywell spray valves while in shutdown; (4) to prevent opening low pressure steam supply valve F087 when vessel pressure is above line design rating; (5) to prevent pump start when suction valve(s) are not open.

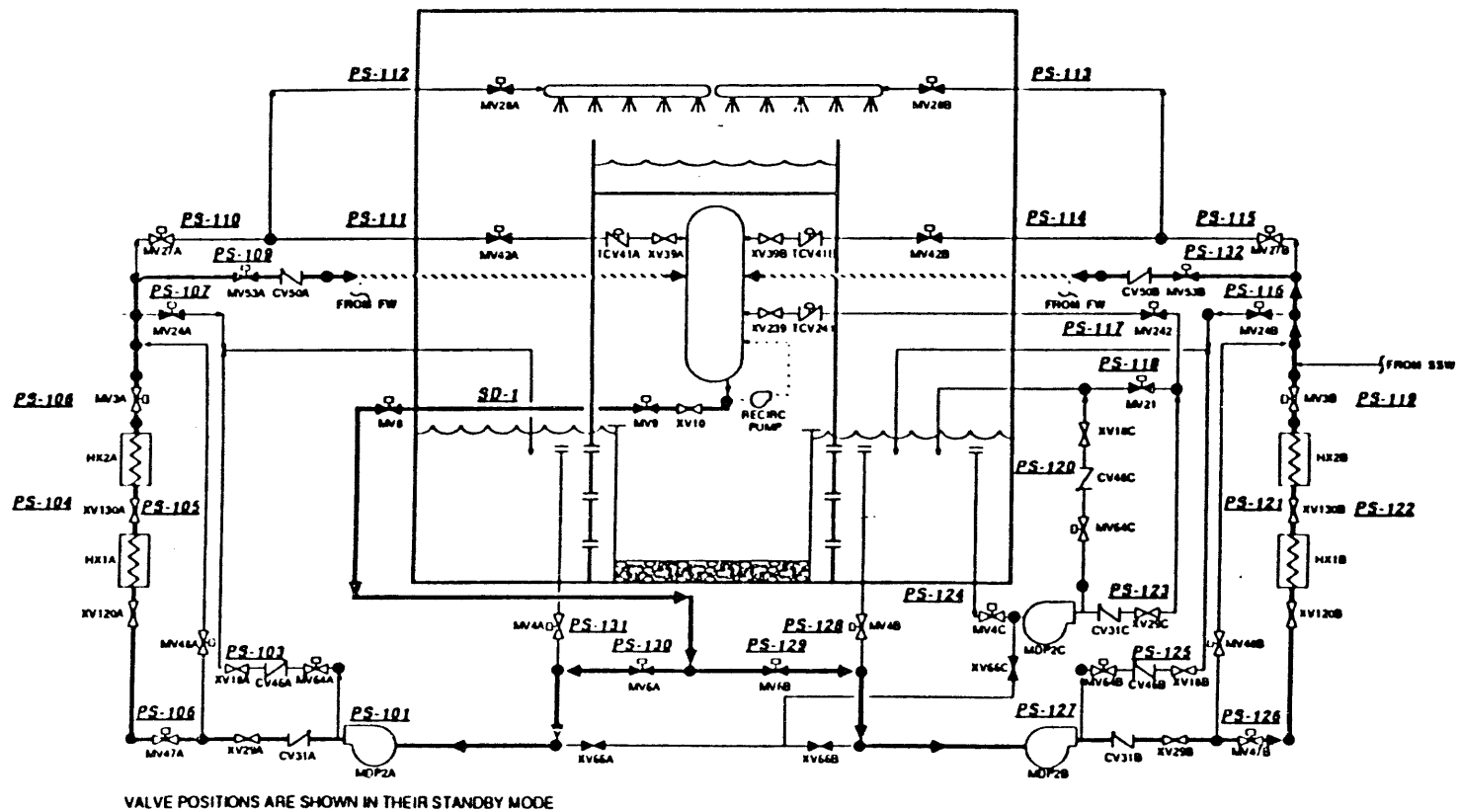


Figure B.1 Simplified schematic of the RHR system: the bold lines indicate flow paths for the SDC mode.[2]

B.2 Alternate Decay Heat Removal System[1,3,4]

The alternate decay heat removal system (ADHRS) of Grand Gulf provides an alternate method of decay heat removal during cold shutdown and refueling, when maintenance is being performed on the RHR shutdown cooling loops or associated support systems. An auxiliary cooling loop is included in the RHR system with separate pumps, heat exchangers, and controls. Piping in the RHR A, B, and C loops is utilized for suction and discharge paths, and cooling water to the ADHRS heat exchangers is supplied by the plant service water system.

The function of the ADHRS is to maintain reactor coolant temperatures below technical specification limits during cold shutdown and refueling operations. This system is important to safety, but is not safety-related because the ADHRS does not automatically mitigate the consequences resulting from accidents.

The two pumps used by the ADHRS are 50% capacity pumps which, when operated in parallel, deliver approximately 3600 gpm. Two 50% capacity heat exchangers are used in a parallel arrangement to provide the required decay heat removal. These pumps and heat exchangers are installed in the RHR C pump room.

Control for the ADHRS is remote manual from the control room. Individual manual control of pump operation with pump running status lights is provided. Flow and temperature indications are also provided in the control room for ADHRS heat exchangers.

REFERENCES

1. "Grand Gulf Nuclear Station Units 1 and 2 (GGNS) Updated Final Safety Analysis Report (UFSAR), Revision 4," December 1989.

2. M. Drouin, J.L. LaChance, B.J. Shapiro, et al., "Analysis of Core Damage Frequency: Grand Gulf, Unit 1 Internal Events, NUREG/CR-4550, SAND86-2084, Rev. 1, Vol. 6, September 1989.

3. D.W. Whitehead, J. Darby, B. Staple, et al., "Draft Letter Report for Phase 1 of the Low Power and Shutdown Accident Sequence Frequencies Project," Sandia National Laboratories, June 1991.

4. D.W. Whitehead, et al., "BWR Low Power and Shutdown Accident Sequence Frequencies Project: Phase 2 - Detailed Analysis of POS 5," Sandia National Laboratories, August 31, 1992.

5. G. Vine, T. Libs, S. Farrington, et al., "Residual Heat Removal Experience Review and Safety Analysis: Boiling Water Reactors," Nuclear Safety Analysis Center, NSAC-88, March 1986.

APPENDIX C

LIMITING CONDITIONS FOR OPERATION

LIST OF TABLES

This appendix describes the limiting conditions for operation (LCOs) and associated action requirements defined in the current Technical Specifications of Grand Gulf[1] for the systems that can be used to remove decay heat, i.e., the residual heat removal (RHR) system and the alternate decay heat removal system (ADHRS). The LCOs and action statements for the standby service water (SSW) system are relatively simple as compared to those for the RHR system, and they are described in Chapter 3 of the report.

C.1 LCOs for the RHR System

Table C.1 summarizes the LCOs and associated action statements for the various operational modes of the RHR system. For the low pressure coolant injection (LPCI), suppression pool cooling (SPC), and containment spray (CS) modes, LCOs are defined for the plant modes of power operation, startup, and hot shutdown. However, for the shutdown cooling (SDC) mode, LCOs are defined only for those plant conditions where the SDC system perform its function, namely, reactor cooldown stage below 135 psig and cold shutdown.

There are also other LCOs related to the RHR system, that is, for isolation actuation instrumentation (specification 3.3.2). These LCOs define the minimum operable channels per trip system, the trip setpoints and allowable values, and the instrumentation response time.

C.2 LCOs for the ADHRS

No LCOs are explicitly imposed on the ADHRS. This system is designed for use only during cold shutdown and refueling where the shutdown cooling loops of the RHR system or associated support systems are unavailable for maintenance or failure.

The action requirement related to the ADHRS is contained in LCO 3.4.9.2 of the Grand Gulf Technical Specifications. The LCO for residual heat removal during cold shutdown stipulates that two SDC loops of the RHR system shall be operable and, unless one recirculation pump is in operation, at least one SDC loop shall be in operation. When this condition is not met, the following actions are required to follow:

(1) With less than the required RHR SDC loops operable, within one hour and at least once per 24 hours thereafter, demonstrate the operability of at least one alternate method capable of decay heat removal for each inoperable SDC mode loop.

(2) With no RHR SDC loop in operation, within one hour establish reactor coolant circulation by an alternate method and monitor reactor coolant temperature and pressure at least once per hour.

REFERENCES

1. "Grand Gulf Nuclear Station Units 1 and 2 (GGNS) Updated Final Safety Analysis Report (UFSAR), Revision 4," December 1989.

Table C.1 Current LCOs for the RHR System

RHR Operational Mode	Plant Operational Condition(s) Applied	Inoperable RHR Sub-system(s) or Other System(s)	Operability Demonstration or Verification Required	Allowed Outage Time	Plant Operational Mode Change Required
LPCI	Power operation, Startup and Hot Shutdown	LPCI train A	No requirement for demonstration of operability; Verify the operability of ECCS divisions[a] 2 and 3 (i.e., LPCI trains B and C, and ADS)	7 days	Hot shutdown within the next 12 hours and in cold shutdown[b] within the following 24 hours
LPCI	Same as above	LPCI train A and LPCS system	Same as above	72 hours	Same as above
LPCI	Same as above	LPCI train B or C	No requirement for demonstration of operability; Verify the operability of ECCS divisions 1 and 3 (i.e., LPCI train A, LPCS, ADS and HPCS)	7 days	Same as above
LPCI	Same as above	LPCI trains B and C	Same as above	72 hours	Same as above
LPCI	Same as above	LPCI train A and either LPCI train B or C	No requirement for demonstration of operability; Verify the operability of ECCS division 3 (i.e., HPCS)	72 hours	Same as above
LPCI	Same as above	Either LPCI train B or C, and LPCS system	Same as above	72 hours	Same as above

Table C.1 Current LCOs for the RHR System (Cont'd)

RHR Operational Mode	Plant Operational Condition(s) Applied	Inoperable RHR Sub-system(s) or Other System(s)	Operability Demonstration or Verification Required	Allowed Outage Time	Plant Operational Mode Change Required
SPC	Power Operation, Startup and Hot Shutdown	Either SPC loop A or B	None	72 hours	Hot shutdown within the next 12 hours and in cold shutdown[b] within the following 24 hours
SPC	Same as above	Both SPC loops A and B	None	8 hours	Same as above
SDC	Hot Shutdown, with reactor vessel pressure less than the RHR cut-in permissive setpoint	Either SDC loop A or B	Demonstrate the availability of at least one alternate method capable of decay heat removal for each inoperable SDC loop within one hour and at least once per 24 hours thereafter.	0 hours	Cold shutdown within 24 hours
SDC	Same as above	Neither SDC loop A nor B	Initiate action to immediately restore an alternate method capable of decay heat removal within one hour	0 hours	None
SDC	Cold Shutdown	Either SDC loop A or B	Demonstrate the availability of at least one alternate method capable of decay heat removal for each inoperable SDC loop within one hour and at least once per 24 hours thereafter.	0 hours	None

Table C.1 Current LCOs for the RHR System (Cont'd)

RHR Operational Mode	Plant Operational Condition(s) Applied	Inoperable RHR Sub-system(s) or Other System(s)	Operability Demonstration or Verification Required	Allowed Outage Time	Plant Operational Mode Change Required
SDC	Hot Shutdown, with reactor vessel pressure less than the RHR cut-in permissive setpoint	Both SDC loops A and B	Demonstrate the operability of at least one SDC loop or one recirculation pump. Within 1 hour establish reactor coolant circulation by an alternate method and monitor reactor coolant temperature and pressure at least once per hour.	0 hours	None
SDC	Cold Shutdown	Same as above	Same as above	0 hours	None
CS	Power Operation, Startup and Hot Shutdown	Either CS loop A or B	None	72 hours	Hot shutdown within the next 12 hours and in cold shutdown[b] within the following 24 hours
CS	Same as above	Both CS loops A and B	None	8 hours	Same as above

[a]ECCS division 1 consists of the LPCS and LPCI subsystem "A" of the RHR system and the ADS as actuated by trip system "A". ECCS division 2 consists of LPCI subsystems "B" and "C" of the RHR system and the ADS as actuated by trip system "B". ECCS division 3 consists of the HPCS.

[b]Whenever two or more RHR subsystems are inoperable, if unable to attain cold shutdown, maintain reactor coolant temperature as low as practical by use of alternate heat removal methods.

APPENDIX D

SHUTDOWN TRANSIENT DIAGRAM AND DATA

LIST OF TABLES

LIST OF FIGURES

This appendix describes the preparation of shutdown transient diagram (STD) for Grand Gulf, and derivation of associated data. The modeling assumptions and data are based as much as possible on GG/PSA study[1] and ongoing extension of the PSA for shutdown states.[2,3]

The corresponding models of the TVO/RHRS study[4] has been utilized as a starting point, but due to differences in plant design, the selection and grouping of transients are somewhat different. The treatment of the initiating events and disturbance transients over shutdown phases has been further refined in this study to consider primary issues, such as optimum timing and target state of the LCO shutdown.

D.1 Grouping and Screening of Initiating Events

AOT considerations for the residual heat removal (RHR) and standby service water (SSW) systems are aimed at comparing the relative risks associated with failures in these systems, especially the risk comparison of the following operational alternatives:

- Continued operation (CO), staying in power operation state for the time of the repairs
- Controlled shutdown (SD) to undertake repairs in a zero-power shutdown state

Because only relative results do matter, different type of simplifications, often stronger than in PSA, are motivated and acceptable.

The initiating events considered in GG/PSA are in general applicable also to an AOT consideration of RHR systems. By making disruptions to normal power operation, they cause an automated shutdown of the plant, or a need to manually trip or promptly shut down the plant, consequently challenging the removal of decay heat.

D.1.1 Screening Criteria

In a failure situation of the RHR or SSW systems, the relative importance of initiating events may substantially differ from the average contributions analyzed in a PSA study. In general, those initiating events for which RHR function is an essential part of the plant response, increase in importance. Specially, such initiating events which are Common Cause Initiators (CCI) in regard to RHR function, i.e., both directly challenge RHR and render part of RHR systems unavailable, may increase drastically in relative importance, if it is assumed that some part of RHR systems is known to be failed initially. Very obvious CCIs in this regard are loss of offsite power (LOSP) and loss of power conversion system (LoPCS) events causing unavailability of normal power conversion system (PCS). Other potentially important CCIs may be global/local protections associated with RHR or SSW equipment or failures of AC/DC supply system, discussed later in sections D.3 and D.4.

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

D.1.2 Shutdown Cooling Mission

The modelling and quantification of the shutdown related risks includes a proper evaluation of the credit from the diminishing decay heat level after entering zero-power state in an LCO shutdown. This means that if a critical failure sequence arises, there will be increasing time margin for recovery actions as the function of time elapsed from the power reduction.

The shutdown cooling (SC) mission period is considered as a phased mission, consisting of several phases, such as reactor cooldown corresponding to so-called hot shutdown, and stable cold shutdown. Figure D.1 shows these shutdown phases and their relation with SC mission period for two basic cases:

- controlled LCO shutdown, which proceeds in a nominal, planned way
- plant trip with loss of power conversion system (LoPCS), which represents the generic type of transient scenarios

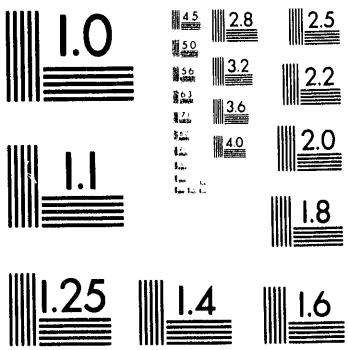
The concept of SC mission is associated with the time period in the zero-power state over which the standby RHR systems are nominally used. The SC mission phase becomes of central role in our study, because in the failure situations of RHR/SSW trains, the plant is specially vulnerable during this phase. It should be emphasized that the SC mission phase is intentionally entered in the LCO shutdown alternative (SD); however, it may also be entered in the continued operation alternative (CO), if a forced shutdown need or a transient initiator occurs during the time period concerned, i.e. during the repair time of the detected failures of RHR/SSW trains. Hence, the evaluation of the SC mission phase is relevant to both SD and CO alternatives in the risk-comparison approach.

D.1.3 Shutdown Transient Diagram

The modeling of event sequences in the phased mission approach is accomplished by the use of extended event sequence diagram (EESD), discussed in Appendix E. This modeling approach is also used to construct a master model over the transition stages from the power operation state into SC mission phase. These particular models are called shutdown transient diagram (STD), and they constitute the top level in the modeling hierarchy for event sequences.

The STDs for full-power operational state and for controlled LCO shutdown are presented in Figures D.2 and D.3, respectively. The modeling details and the relationship to the plant operational states during shutdown phases is discussed in section D.2. The principles of modeling are described more thoroughly in reference 4.

The construction of STDs for Grand Gulf (GG) is much based on the TVO/RHRS study model.[4] Due to the differences in plant design, the selection and grouping of transients are different. The most important difference is related to the PCS, which can be used to remove decay heat at Grand Gulf while staying longer in the hot shutdown state, or which can be restored as backup if normal SC path (RHR/SDC mode) becomes inoperable in the cold shutdown state. At TVO, PCS is not designed to be used at low reactor pressure and steam rate, and is unstable in that operation range: steam release to suppression pool (SP) and RHR/SPC mode need to be used later after reactor shutdown if RHR/SDC mode is unavailable. Of course, RHR/SPC mode is a viable option at Grand Gulf also, and need to be used if both PCS and RHR/SPC mode are unavailable.


1.0
1.1
1.25
1.4
1.6
1.8
2.0
2.2
2.5
2.8
3.2
3.6
4.0
4.5
5.0

2 of 2

Later in this appendix, we will discuss different initiating event classes in detail, and explain the detailed modeling assumptions used when constructing the STD, as well the derivation of data.

D.2 Relation to Plant Operational States

The definition of the plant operational states (POSs) from GG/SD/PSA[2,3] will be adopted here. The specifications are summarized in Table D.1.

D.2.1 Stages of a Controlled LCO Shutdown

In a controlled shutdown such as arising in an LCO situation with RHR or SSW trains failed, the following order of the plant state changes apply:

POS 0 -> POS 1 -> POS 2 -> POS 3 -> POS 4 -> POS 5/Repairs -> Startup

It should be emphasized, that the POSs are not actually concerned with the stable plant states but rather define operational ranges. Especially, POSs 0 and 1 cover power reduction stage up to the point where reactor is subcritical at full pressure and temperature; turbine is shut off, but the condenser is still used as a steam sink with turbine bypass valves (TBVs) on manual control, and coolant makeup is provided by condensate and feedwater pumps. The end state of power reduction is named as HotSD.F for hot shutdown state with full pressure and temperature (belongs to POS 2); this is an alternative target state of an LCO shutdown. POSs 2, 3, and 4 span over reactor cooldown stage ending with nonpressurized reactor condition, RHR/SDC in use and PCS idle. The end state of the reactor cooldown stage is named as ColdSD.N for cold shutdown state with normal shutdown cooling operating (belongs to POS 5); this is the nominal target state of an LCO shutdown

Hot and cold shutdown states oftentimes are not clearly defined. In this study, hot shutdown (HotSD) is defined as zero-power state with reactor pressurized; PCS preferably used as heat sink, but alternatively steam could be released to SP. Cold shutdown (ColdSD) is zero-power state with reactor cooled down to nonpressurized condition; RHR/SDC is preferably used for decay heat removal. Because HotSD spans over a rather wide range, staying near the full pressure is more closely denoted by HotSD.F, as discussed later.

Table D.1 also shows the behavior of the process variables of reactor coolant system (RCS), i.e., temperature and pressure, in the case of a controlled LCO shutdown. The power reduction is assumed to be performed in two steps, from 100% down to 60% and 0%, in 0.5 and 2.5 hours, respectively. The time lag of staying in HotSD is assumed negligible in the nominal LCO shutdown scenario; i.e., reactor cooldown is assumed to be started without delay after achieving zero power. A constant cooldown rate of 80 °F/hour is assumed. This means that the cooldown up to 135 psig takes about 4 hours. Thus, the minimum total time for power reduction and cooldown, in order to change over to RHR/SDC, is about 7 hours. It is assumed that, if there is at least one RHR/SDC train intact, the operations proceed according to this minimum delay scheme.

D.2.2 Target State of LCO Shutdown

The nominal target state ColdSD.N of LCO shutdown is associated with POS 5, where RHR/SDC will preferably be used for decay heat removal. The use of condenser as steam sink is ceased, and the feedwater (FW) system is placed in standby. The reactor cooldown is stopped just below 200 °F (non-

pressurized condition). Further actions of POS 5, which are relevant when going to refueling or to a special type of repair outage, are not assumed to be undertaken.

One alternative target state for LCO shutdown is associated with the hot shutdown state HotSD.F, with reactor pressure and temperature near the nominal 1000 psig and 550 °F, and TBVs/condenser used as a steam sink and FW pumps for makeup. The other alternative is to quickly proceed to POS 5 in order to use ADHRS (target state ColdSD.A). The nominal LCO shutdown scenario for the failure situations of the RHR/SSW trains follows the minimum delay scheme through the power reduction and reactor cooldown stages with ColdSD.N as the target state.

If RHR/SDC is completely disabled, e.g., due to failures of RHR or SSW trains A and B, a prolonged use of PCS as steam sink over the cold shutdown state is assumed in the nominal scenario. This may not be feasible from the operational point of view. Hence, the LCO shutdown with target state ColdSD.A is evaluated as the primary alternative in the failure situations with RHR/SDC disabled. As a secondary alternative, staying in HotSD.F is also considered.

D.2.3 STD Linking with Shutdown Scenarios

The STD for the nominal, controlled LCO shutdown (Figure D.3) includes the success path where power reduction is completed in planned way, with successful transfer to reactor cooldown stage. The likelihood of the excursion-free path is about 90%. The excursion branches represent different deviation possibilities correlated with the plant state change. They fall into same categories as the initiating events for power operation state. These events may occur also spontaneously during the time window of the power reduction stage, with a small likelihood, which is in fact incorporated in the quantification process. (Compare with the further discussion of the initiator treatment in section D.4.)

Part of the excursions are correlated with plant disturbance trip during the power reduction stage. The other part is just considered as lumped over the phase of the plant state change. The background to these categories will be discussed in section D.4.

For simplicity, excursions correlated with reactor cooldown stage are in the nominal LCO shutdown scenario superposed with the power reduction stage, and not modeled explicitly in the model for TraCSD branch. The motivation behind this is that their contribution is relatively small. In the evaluation of alternative LCO shutdown schemes, the reactor cooldown stage is handled explicitly, meaning that a similar STD model is used for it as presented for the power reduction stage in Figure D.3, and splitting the probability contributions accordingly (section D.4).

In CO alternative, the initiating events for full power operation state apply. They are represented in the STD by initiating transient events (ITR) and corresponding exit paths from the normal power operation state (Figure D.3). For completeness, and for consistency with the LCO shutdown model, the exit branch DecSD is included, representing the forced controlled shutdowns occurring during power cycle.

For the DecSD branch, the excursions associated with plant state change are presented in compact form, but are effectively identical with the STD of LCO alternative (Figure D.3). To be realistic, a branch is included, after successful power reduction, between proceeding to ColdSD and staying in HotSD state. A similar branch also is included in the PTrip event branch. For the total risk of the power operation state, the contribution of DecSD and PTrip branches are rather small, and hence these details are not very important.

In relation to SC mission period (Figure D.1), STDs describe the event scenarios from the normal power operation state down to entering SC mission. In a smoothly progressing, nondelayed controlled shutdown, the time span covered by STD is about 7 hours, as the reactor cooldown stage is in the nominal case superposed together with power reduction stage (the simplification used in the nominal LCO shutdown scenario, as discussed earlier). In transients and LOCA scenarios, the time span covered by STD is very short, including effectively reactor scram, eventual overpressure-protection response, and similar initial plant responses.

STDs end with the initiating events of SC mission (ISC). These ISC are similar to the initiating events for, or exit events from, the power operation state, although not equivalent. Instead, they are more strictly defined with respect to plant conditions; section D.5 describes more details.

D.3 Initiating Transient Events

The initiating events for full power operation are based on GG/PSA (Table D.4). The decided shutdown path is added, primarily for consistency with modeling of SD alternative, although of its small contribution to the full power operation risk, as discussed in the preceding chapter.

D.3.1 Plant Trips (PTrip)

General transients with PCS initially available, equivalent to T3A in GG/PSA, are preserved as such. Possible later loss of PCS is explicitly modeled in EESD models.

D.3.2 Loss of Feedwater (LoFW)

Loss of feedwater, with condenser initially available, is motivated to be preserved as a separate initiating event in the AOT considerations also. Possibility to realign condensate feed for reactor coolant supply in low pressure mode is considered separately, because FW pumps are then bypassed. This option is modelled in EESDs in connection with the failure of preferred coolant supply systems.

The GG/PSA mentions the FW-pump restart option for initiator T3B, but it is not actually included in the event tree analysis. This has a negligible influence for the GG/PSA results, because of so many alternative makeup systems available in T3B. This detail differs from the TVO/RHRS study model, where the manual restart of one FW pump is considered, and is a significant contributor. It should be emphasized that TVO lacks RCIC type of a diversified system for high pressure coolant supply.

D.3.3 Loss of Power Conversion System (LoPCS)

This initiating event is preserved also as such (and is presumably second in importance ranking for AOT consideration of RHR/SSW systems).

D.3.4 Loss of Instrument Air (LoIAS)

This is included as a potentially important initiating event, because it means also loss of PCS.

D.3.5 Loss of External Grid (LoEG)

This initiating event is preserved as such, and is presumably the most important. Loss of external grid is here simply associated with loss of offsite power (LOSP), i.e., including also failures of station transformers and other equipment, which impose challenge on emergency power supply from DGs. Possibility of using so called house turbine operation, when a grid failure occurs outside the plant, is not credited (beyond design). For comparison, note that, at the TVO study, it was assumed that there are 50% of chances for the successful transfer to house turbine operation in LoEG.

D.3.6 Inadvertent Opening of Relief Valves (IORV)

Inadvertent opening of relief valve(s) was observed to contribute little in PSA. Its relative importance is not much affected by RHR/SWS train failure situations; hence, IORV was considered with a crude EESD model.

D.3.7 Leakage of Primary Coolant Inside Containment (LOCAs)

LOCAs proved to contribute little in PSA, and their relative importance remains small in failure situations of RHR/SSW trains also. For general interest, they were, however, included. During the course of the study, they showed to be important contributors in failure situations of RHR pump trains, because these trains serve also LPCI function. Consequently, the models were adapted to take these connections more precisely into account.

D.3.8 Unconsidered RHR Initiators of CCI Type

There are further candidates for initiating events such as actual or inadvertent RPS (reactor protection system) actuations, or local protections, which result in trip, interlock or isolation of RHR systems. In the TVO case, most important was Y isolation, which protects against interfacing system LOCA via RHR trains, by closing the preferred SC path (corresponds to the RHR/SDC mode of the Grand Gulf plant). This kind of special initiating events were reviewed in GG/PSA, but found as small contributors. The same conclusions apply also to this study in regard to initiating transients for power operation state.

The functional consequences of spontaneous failures in AC/DC supply systems (distinct from LOSP situation) were especially checked in order to evaluate the need for their inclusion as initiating events. In the TVO/RHRS study, these were found to be important in baseline and low-order failure cases (i.e., single or double failures), but small contributors in triple/quadruple failure situations of RHR trains. Due to differences in the plant designs, these type of failures have a smaller relative contribution for the Grand Gulf plant as presented in GG/PSA screening of initiating events, and are hence excluded among the initiating transients from the power operation state. During the shutdown states, however, spontaneous failures of safety systems and their support systems/functions are handled as initiating events, which is analogous to the GG/SD/PSA models for shutdown states; this will be discussed further in section D.5.

D.4 Initiating Events During Shutdown Phases

Handling of initiating events during shutdown phases is described here also as compared with a standard PSA.

D.4.1 Definition of Initiator Categories

The accident sequence initiators are divided up into the following two categories:

(1) Spontaneous initiators, where the proximate cause is failure of an operating system or loss of a critical support function, or some other random deviation

(2) Shutdown-change-correlated triggers, or shutdown-triggered initiators, where the proximate cause may be a latent defect which has not been a problem in the preceding operation period, but becomes critical when entering a specific shutdown stage. To this category belongs also transients which are triggered by the reactor and/or turbine trip, such as loss of external grid due to an abrupt plant disconnection from the load. Critical action errors in operational deviations along the shutdown process may also be included in this category.

The spontaneous initiators are connected with self-revealed failure mechanisms (often called as monitored failures), and are quantitatively described by event rate or frequency, i.e., probability per unit of time. Generally, the frequency of a spontaneous initiator is time-dependent. Especially, it may depend on the plant operational state. Usually, an average frequency over a given plant operational state can be used, and this simplification is applied also in this study. Table D.2 summarizes the data for spontaneous initiators in different plant operational states. The background and derivation of the data are discussed in section D.7.

The shutdown-change-correlated initiators are of different stochastic nature as compared to spontaneous initiators. The total probability of a spontaneous initiator is obtained by integrating the initiator frequency over the time elapsed in the specific states. The probability of a shutdown-triggered initiator is time-independent and only connected to entering or passing through a shutdown stage.

The data for the shutdown-triggered initiators over the controlled LCO shutdown (DecSD) can be broken up into two phases: (a) power reduction phase where the plant state changes from full power operation down to HotSD.F, i.e., POS 0 -> 2, (b) reactor cooldown phase where the plant state change from HotSD.F down to ColdSD.N, i.e., POS 2 -> 5 (see Table D.1).

In the phased mission approach, the breakup of time into successive phases is usually defined in such a way that

- spontaneous initiators can be assumed constant over each phase, and
- plant/system state change correlated initiators can be associated with the phase shifts.

This scheme is applied also in this study.

It should be emphasized that the initiating event classes usually divide up into both initiator categories. For example, the spontaneous LOSP has a specific frequency in each plant state (dominated by offsite causes), but in addition there is a likelihood of losing the external grid by a disturbance transient correlated with power reduction operations. For comparison, we obtain from the data given in Tables D.2 and D.3:

$f_{LOSP|POS1-4} * a_{POS1-4|DecSD}$ = 0.13 /year * 8 hours

= 1.2E-4

$P_{LOSP|DecSD}$ = 1.0E-4

Thus these two LOSP initiator contributions are of the same order of magnitude, and therefore, both need to be considered in the risk-comparison analysis of an LCO shutdown. Handling of the two initiator categories for the event-sequence modeling will be discussed in more detail in following sections.

D.4.2 Spontaneous Initiators

During the shutdown states, spontaneous failures, which mean exit from the stable or intermediate state, are handled explicitly (as a kind of initiating events). They are modelled in detailed EESDs (Appendix E) and their data are included in module data.

D.4.3 Shutdown-Change-Correlated Triggers and Controlled Shutdown Path in STD

In the STD for controlled LCO shutdown (Figure D.3), possible deviations during the power reduction phase are represented by the transfer branches to other initiator-category paths. The transfer event, TraCSD, for the successful, decided shutdown path is defined after successful power reduction and stable hot shutdown state, HotSD.F (refer to Figure D.1 and Table D.1). The subsequent phases of this path are described in the EESD model for TraCSD (Appendix E).

Part of the initiators in the DecSD path are related to a disturbance trip: this applies to UnFW, LoPCS, IORV and LOSP, because they all are closely correlated to reactor and/or turbine trip. Other part, the more unlikely LoIAS and LOCAs are considered to be related to latent faults, which are activated/triggered during a plant shutdown process as a whole. These are simply considered equally likely per any plant trip or controlled shutdown, which sum up to about 6 per year (see Sections D.7.4 and D.7.7). This simplification for IAS, in particular, is based on the assumption that the reaction of IAS in various stages of the controlled shutdown process and transients do not differ substantially; i.e., abrupt air consumption fluctuations, and challenges imposed on IAS components and regulating functions should be about the same.

For the normal power state operation, IORV is defined as a spontaneous opening of SRVs accompanied by the failure to reclose. For the DecSD path, IORV is considered as a disturbance event correlated with and conditional on a controlled shutdown process. It seems to occur most likely in connection with a loss of PCS during the shutdown process, implying that SRVs need to operate and may then fail to reclose. The following scenarios are considered relatively unlikely: (a) pressure excursions other than loss of PCS during power reduction and reactor cooldown phases, resulting in SRV response and possibly to SRV stuck open, and (b) manual pressure relief eventually used under some circumstances to prompt pressure reduction or to get condenser sooner disconnected (or for any other reason), possibly accompanied by SRV stuck open.

All combination events with SRV stuck open and other transients or LOCA initiators are neglected as small contributors, except the above combination with LoPCS (which is reduced to the same modeling scenario as the spontaneous IORV scenario).

D.5 Initiating Events for Shutdown Cooling

STDs end with the initiating events of SC mission (ISC). These transfer events are grouped on the right hand side of the STD. They represent entry events for SC phase. The plant response in subsequent phases is modelled by EESDs (Appendix E).

As discussed earlier, the ISCs have similarities with the initiating events for, exit events from, the power operation state, but are not equivalent. Instead, they are more strictly defined with respect to plant conditions. As an example, in LoPCS, when considered as an ISC, the reactor scram and overpressure protection are assumed successful (their failure branches are not explicitly shown in STD, and their contributions neither quantified, as was discussed in connection with the boundary conditions of this study). Also, offsite power is assumed to be preserved in the ISC of LoPCS, while the combination case of initial LoPCS and turbine-trip-induced LOSP is included in the ISC of LOSP (see Figure D.2).

Drawing a limit between STDs (describing the early phase of manual shutdown or accident evolution, or the fast plant response to transient initiators) and EESDs (describing the plant/system operation over SC mission phase) is much a matter of choice. The principle used in this study attempts to cover by STDs all first-phase branching among the transient scenarios. The startup response of standby systems for decay heat removal are consistently included in EESDs. The detailed specifications for the ISC transfer events are presented in connection with the EESD models of the SC mission phases, described in Appendix E.

D.6 Plant Startup Phase

The plant startup phase is not explicitly considered. Because we are considering failure situations of the RHR/SSW systems, and decided or forced shutdowns associated with the situations, the startup is assumed to be done only after the repairs are completed. Hence, the plant configuration is safer when starting the plant as compared to the initial, known failure situation. Furthermore, the decay heat level is lower in startup conditions, which decreases the accident risk of many event scenarios.

These arguments do not hold similarly for a shutdown from the baseline state, or in a situation, where the initial failure means only a small increase in the risk level (their AOT considerations will, however, follow another path). Presumably, GG/SD/PSA will produce additional useful information for the relative significance of the startup phases.

D.7 Data for Initiating Events

This section describes how we derived the data for initiating events and other transients in the STDs, and also mean durations of the plant outage for considered shutdown classes. The derived estimates are summarized in Tables D.2 and D.3.

D.7.1 Decided Shutdowns and Plant Trips

GG/SD/PSA lists the following data during 1986-89 (Tables 11.3.3-6 and 7 in reference 2):

	Number of events	Rate [/yr]	Duration [h]
Controlled SDs to below 15%	4	1.0	224
Plant trips (scrams)	16	4.0	78
Shutdowns for refuelling		1	
Total rate of shutdowns		6.0	

The two scrams in December 1985 are excluded, as they seem to be related to early phase problems (and because it is more consistent to count full calendar years when processing plant event data).

Out of the four controlled shutdowns, three extended down to ColdSD, while one was short staying in HotSD (Tables 11.3.3-7 and 8 of reference 2). Hence, in the DecSD path of the STD for full-power operation state (Figure D.2), we obtain the branching fractions, 75% and 25%, for going down to ColdSD and staying in HotSD, respectively, as shown in the figure.

The scram events include 5 outages extending to cold shutdown (POS 4 and 5) (Tables 11.3.3-6 and 9 of reference 2). Based on this information, a branch from PTrip path to TraCSD is included in the STD, with a corresponding conditional probability of 0.3 (Figure D.2). For the power operation state, the frequency of PTrip initiator is obtained from the total scram frequency above, by subtracting LoFW and LoPCS initiator frequencies.

The plant-specific experience of Grand Gulf from 1985 through 1989 includes two events, where the reactor was scrammed during a controlled shutdown

02/12/86: feedwater pump trip at 60% power level
12/18/90: feedwater pump trip at 17% power level

When considered over 5 reactor years and about 10 controlled SDs, one during power cycle and another for annual overhaul, this would produce an estimate of about 20% likelihood for a disturbance trip per controlled shutdown. This likelihood appears very high as compared to the estimate of about 3% inferred from GG/PSA, or the TVO/RHRS study data of 1.2% (although at the TVO plant, the trip frequency in power operation is also low, about 1.0 /yr). Therefore, an estimate of

$$P_{PTrip|DecSD} = 0.1$$

will be adopted at this stage, because it appears to be closer to a generic, industry-average value. This data issue is important. To yield a broader and more confident information base for the transient profile, LERs may be extracted for reactor trips for other BWR/Mark III plants. The likelihood of trip due to shutdown-change-correlated disturbances is split into equal shares between power reduction and reactor cooldown stages, i.e., 50% for POS 0 and 1, and 50% for POSs 2 through 5 (Table D.3).

D.7.2 Loss of Feedwater (LoFW)

GG/PSA data of 0.76/yr for initiating event T3B is used. The mean duration of this event is assumed to be the same as for scrams, i.e., 80 h. Manual realignment to use condensate feed is assumed to succeed with 90% probability (GG/PSA uses a screening value of 0).

The probability of introduced FW pump trip during controlled shutdown, including failure to realign condensate feed, is assumed to be the same as at TVO, 1% per disturbance trip. Excluding LoPCS as shown in Figure D.3, this gives:

$$P_{LoFW|DecSD} = 0.01*(1-P_{LoPCS|PTrip})*P_{PTrip|DecSD} = 6.3E\text{-}4$$

This likelihood is all associated with power reduction stage, i.e., 100% for POS 0 and 1 as shown in Table D.3.

D.7.3 Loss of Power Conversion System (LoPCS)

GG/PSA data of 1.6/yr for initiating event T2 is used. The mean duration of the associated plant outage is assumed to be the same as for scrams, i.e., 80 h. For the probability of introduced loss of PCS during controlled shutdown, a screening value, $P_{LoPCS|DecSD} = 0.035$ (Figure D.3), is used. It is based on GG/PSA value 0.37 for event Q2, representing the fraction of transient initiating events involving loss of PCS (Table 5.1.2 of reference 1). At TVO, this probability is 0.85, reflecting the instability of condenser at a low steam flowrate as well as the normal way of performing the tail part of RCS pressure reduction by regulated steam relief to SP, which enables to start maintenance at the turbine plant earlier. The likelihood of shutdown-change-correlated LoPCS is split into equal shares between power reduction and reactor cooldown stages, in the closer breakdown (Table D.3).

D.7.4 Loss of Instrument Air (LoIAS)

GG/PSA frequency of 8.1E-4/yr for initiating event TIAS was derived from a simple system model by neglecting CCFs. It concerns the loss of both normally running instrument air compressors and the standby service air compressor. This value appears under-estimated considering the operating experience of Grand Gulf which is discussed in connection with IAS module data. By adding an estimate of CCF contribution, a frequency of $f_{LoIAS} = 3.3E\text{-}3$/yr is obtained, and adopted in this stage. Assuming that a fraction of 10% would be latent faults, revealed at shutdown progress when air consumption varies, we obtain by use of 6 shutdowns per year:

$$P_{LoIAS|DecSD} = 0.1 * 3.3E\text{-}3/yr * (1/6)\ yr = 5.5E\text{-}5$$

In comparison, GG/SD/PSA uses a frequency of 0.5/yr for LoIAS in POSs 1 through 7. When calculated over a cooldown period of 4 hours, this would give:

$$P_{LoIAS|CoolDown} = 0.5\ /(8760\ h) * 4\ h = 2.3E\text{-}4$$

This seems pessimistic, and is in fact based only on two experienced events at Grand Gulf caused by specific maintenance actions, not fully relevant to LCO shutdown. Therefore, the adapted data as explained above are used in the nominal calculations, but a sensitivity analysis was made to see the influence of using the substantially higher values of GG/SD/PSA. The likelihood of shutdown-change-correlated LoIAS is split into equal shares between power reduction and reactor

cooldown stages, in the closer breakdown (Table D.3). Mean duration of the associated plant outage is assumed to be the same as for scrams, i.e., 80 h.

D.7.5 Loss of External Grid (LoEG)

The GG/PSA data of 0.11/yr for the frequency of loss of offsite power has been substituted by 0.07/yr from GG/SD/PSA, because this apparently reflects more recent experiences. In fact, the latest NSAC compilation gives a mean LOSP frequency of 0.059 per site year.[5] These data values include also events caused by spontaneous transformer failures and other failures during normal power operation. Possible transfer to house turbine operation (HTO) is not credited, because the Grand Gulf plant is not designed to allow that. Thus, the data for LOSP can be approximately associated with the loss of external grid connections (LoEG). This results in small overcounting in the STD, because LOSP induced by plant trips is explicitly included for the most likely transient events (Figure D.2). This is, however, accepted to avoid rather complex, detailed modeling of offsite power supply paths.

GG/SD/PSA uses a higher LOSP frequency of 0.13/yr while in shutdown states, i.e., POSs 2 through 7. A look at the NSAC compilation of LOSP events qualitatively confirms this feature, and indicates in fact an even higher conditional LOSP frequency during POSs 1 to 4, constituting in a way non-stationary conditions for power supply. This issue is discussed in association with module data, and a sensitivity analysis was made to see the influence of this data on the risk evaluation.

The probability of LOSP induced by a plant trip (with abrupt load disconnection) is assumed to equal to the generic value of 1E-3.[5] GG/PSA used ASEP data of 2E-4, which seems rather small compared to 4E-3 used in TVO/RHRS study, because on the other hand the LoEG frequency for TVO was assessed as 0.04/yr for longer than 10 min, and as 0.025/yr for longer than 30 min LOSP durations. This is presumably one of the important data values, and may be refined in the continuation.

The induced LOSP is explicitly taken into account for the most likely transients, i.e., PTrip, LoFW and LoPCS, but not for others as such event combinations are small contributors. However, LOSP during SD outage period is taken into account in the EESD models, as discussed in section D.5. Because the likely disturbance transients roughly sum up to be about 10% per DecSD, we obtain:

$$P_{LOSP|DecSD} = 1E\text{-}3 * P_{PTrip|DecSD} = 1E\text{-}4$$

This likelihood is all associated with power reduction stage, in the closer breakdown between power reduction and reactor cooldown stages (Table D.3). The average of 2.2 hours was assumed here for the time to restore offsite power.[5] The mean outage time of the plant in LOSP situation is assumed to be 80 h as for the scrams.

D.7.6 Inadvertent Opening of Relief Valves (IORV)

GG/PSA data of 0.14/yr for initiating event IORV is used. The mean duration of the associated plant outage is assumed to be the same as for scrams, i.e., 80 h. The conditional probability of 0.04 (per pressure relief into SP) is used in this stage for the stuck open SRV (GG/PSA event P1, Table 5.1.2). This failure mode is mainly associated with loss of PCS situations. Thus, a likelihood of

$$P_{IORV|DecSD} = 0.04 * P_{LoPCS|DecSD} = 1.5E\text{-}3$$

per DecSD is derived (Figure D.3). Compare with the derivation of $P_{LoPCS|DecSD}$ in Section D.7.3. The likelihood of shutdown-change-correlated IORV is split into equal shares between power reduction and reactor cooldown stages, in the closer breakdown (Table D.3).

D.7.7 Leakage of Primary Coolant Inside Containment (LePCi)

LOCA events are handled as in GG/PSA, by grouping the events into the following classes and their corresponding frequencies of

LOCA.S (Small LOCA): 3E-3/yr
LOCA.M (Medium size LOCA): 3E-4/yr
LOCA.L (Large LOCA): 1E-4/yr

These are modeled distinctly due to different success criteria and influences of RHR pump trains via LPCI function. The small-small LOCA (recirculation pump seal leakage) has not been considered due to its minor contribution.

The estimate for the SD-triggered LOCA is based on the fraction of 10% of LOCA risk related to plant shutdown/startup changes, as compared to spontaneous LOCA events during power operation state. Using a 5% fraction for shutdown changes and frequency of 6 controlled shutdowns/scrams per year, the following conditional probability estimates are obtained:

$$P_{LOCA.S|DecSD} = 0.05 * 3E\text{-}3/yr / (6/yr) = 2.5E\text{-}5$$
$$P_{LOCA.M|DecSD} = 0.05 * 3E\text{-}4/yr / (6/yr) = 2.5E\text{-}6$$
$$P_{LOCA.L|DecSD} = 0.05 * 1E\text{-}4/yr / (6/yr) = 8.0E\text{-}7$$

These likelihoods are all associated with reactor cooldown stage (which includes the pressure and temperature changes), in the closer breakdown between power reduction and reactor cooldown stages (Table D.3). These estimates belong to the uncertain data values, but are less important to this study, because the contribution of LOCA scenarios remains less than about 1% in all cases. The mean duration of the plant outage in LOCA scenarios is assumed be 10 days, 240 hours.

D.7.8 Remarks on Grouping of the Initiating Events

The derivation of data, as well as the closer definition of the initiating events, is here based on the standard principle of considering first order events only as initiating events. Combination events arising independently or due to a causal relation, such as LOCA and LOSP, or LOSP and failure of IAS, are considered in the EESDs (corresponding to the detailed event-trees/fault-trees in the conventional PSA approach).

D.8 Summary of Main Uncertainties, Sensitivity Analysis Needs

In summary from the preceding sections, the following items are identified as main uncertainties in connection with the STD modeling and data:

(1) In a controlled LCO shutdown when both RHR pump trains A and B failed, whether to stay in HotSD for repairs or proceed to POS 5 in order to align ADHRS or RWCU for RHR

(2) Influence of the high likelihood for loss of IAS in shutdown states as derived from GG/SD/PSA

(3) Influence of the high likelihood of LOSP induced by plant trip, and also the high LOSP frequency in shutdown states from GG/SD/PSA

REFERENCES

1. M. Drouin, J.L. LaChance, B.J. Shapiro, et al., "Analysis of Core Damage Frequency: Grand Gulf, Unit 1 Internal Events, NUREG/CR-4550, SAND86-2084, Rev. 1, Vol. 6, September 1989.

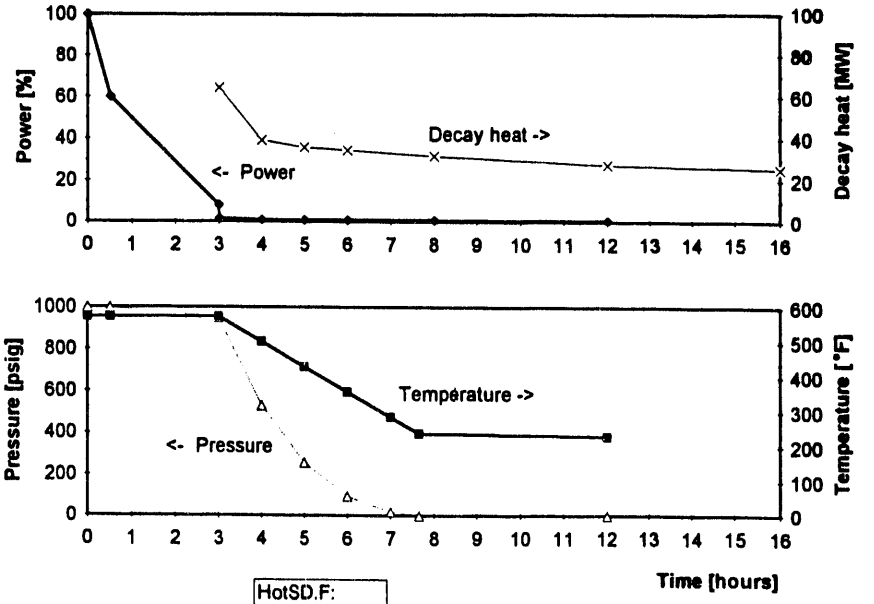
2. D.W. Whitehead, J. Darby, B. Staple, et al., "Draft Letter Report for Phase 1 of the Low Power and Shutdown Accident Sequence Frequencies Project," Sandia National Laboratories, June 1991.

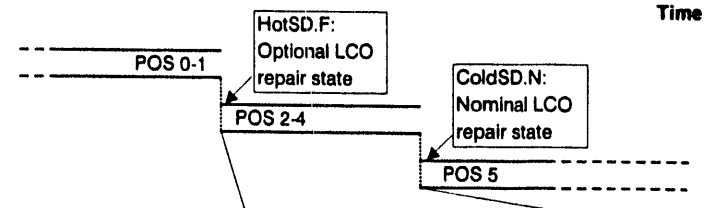
3. D.W. Whitehead, et al., "BWR Low Power and Shutdown Accident Sequence Frequencies Project: Phase 2 - Detailed Analysis of POS 5," Sandia National Laboratories, August 31, 1992.

4. T. Mankamo and M. Kosonen, "Continued Plant Operation Versus Shutdown in Failure Situations of Standby Safety Systems," IAEA/TechSpec Pilot Study Program, NKS/SIK-1(91)4, August 1991.

5. H. Wyckoff, "Losses of Off-Site Power at U.S. Nuclear Power Plants: Through 1989," NSAC-147, Nuclear Safety Analysis Center, March 1990.

Table D.1 Plant Operational States (POSs) and Variation of Reactor Power, Decay Heat Level, and Temperature and Pressure of Reactor Coolant System during Controlled LCO Shutdown





State	POS 0-1	POS 2	POS 3	POS 4	POS 5
Description	Power operation reduction, stages 1, 2	Reactor cooldown, 1st stage	Reactor cooldown, 2nd stage	Reactor cooldown, 3rd stage	Cold shutdown RHR/SDC in operation
P thermal	Relative power POS 0: 100 .. 15% POS 1: 15% -	Decay heat < ~ 60 MW	Decay heat < ~ 40 MW	Decay heat < ~ 35 MW	Decay heat < ~ 30 MW
Pressure, temperature	1000 psig 550 °F	950 - 500 psig 540 - 490 °F	500 - 100 psig 490 - 360 °F	100 - 0 psig 360 - 240 °F	0 psig < ~ 200 °F
Remarks	PCS used, TBVs open below P < 20%	PCS used, TBVs in manual control	Changeover to RHR/SDC at ~135 psig	RHR/SDC used, TBVs shut at ~100 psig	RHR/SDC used PCS idle

Notes: 1. Conditional frequency is defined as the probability of event per unit of time. It is expressed here in the unit of per year for convenience of general comparison.

2. The same frequencies are conservatively used for the stable cold shutdown state as for the pressurized states (i.e., the baseline full-power state and the low power and hot shutdown state).

Table D.2 Conditional Frequencies of Spontaneous Initiators with Ratios of the Frequencies for Low Power and Hot Shutdown State, and Stable Cold Shutdown State to the Frequencies for Baseline Full-Power State

		Conditional frequency [/yr]				Relative to baseline state		
		Baseline full power POS 0	Low power and HotSD POS 1-4	Stable ColdSD POS 5		Baseline full power POS 0	Low power and HotSD POS 1-4	Stable ColdSD POS 5
0	DecSD	1	NA	NA		1		
1	PTrip	1.6	1.6	NA		1	1	
2	LoFW	0.76	0.76	NA		1	1	
3	LoPCS	1.6	1.6	NA		1	1	
4	LoIAS	3.3E-3	1.40E-02	1.40E-02		1	4.24	4.24
5	LOSP	0.07	0.13	0.13		1	1.86	1.86
6	IORV	0.14	0.14	NA		1	1	
7	LOCA.S	3.0E-3	3.0E-3	3.0E-3	*2*	1	1	1
8	LOCA.M	3.0E-4	3.0E-4	3.0E-4		1	1	1
9	LOCA.L	1.0E-4	1.0E-4	1.0E-4		1	1	1

Notes: 1. The total probabilities in the right hand side column do not take into account the definition of the initiators as mutually disjoint. The actual probability estimates are shown on the STDs (Figures D.2 and D.3)

2. The same LOCA frequencies are conservatively used in the ColdSD as in the pressurized state. This is intended to compensate for the modelling limitation, e.g., that RTR flow diversification possibilities in the ColdSD are not explicitly modelled.

Table D.3 Relative Fractions, Conditional Probabilities, Total Probabilities of Shutdown-Triggered Initiators for Power Reduction Stage (POSs 0 and 1) and Reactor Cooldown Stage (POSs 2 to 5)

	Relative fraction		Conditional probability in		Total probability over		/*Note 1*/
	Power reduction POS 0/1	Reactor cooldown POS 2/5	Power reduction POS 0/1	Reactor cooldown POS 2/5	Power reduction POS 0/1	Reactor cooldown POS 2/5	DecSD to ColdSD POS 0/5
PLANT TRIP CORRELATED INITIATORS							
PTrip	50%	50%	0.05	0.05	0.05	0.05	0.1
LoFW | PTrip	100%		0.02	NA	0.001		0.001
LoPCS | PTrip	50%	50%	0.37	0.37	0.0185	0.0185	0.037
IORV | LoPCS	50%	50%	0.04	0.04	7.40E-4	7.40E-4	1.48E-3
LOSP | PTrip	100%		0.002	NA	1.00E-4		1.00E-4
SHUTDOWN CHANGE CORRELATED INITIATORS							
LoIAS	50%	50%			2.75E-5	2.75E-5	5.50E-5
LOCA.S		100%				2.50E-5	2.50E-5
LOCA.M		100%				2.50E-6	2.50E-6
LOCA.L		100%				8.00E-7	8.00E-7

Notes: 1. The total probabilities in the right-most column do not take into account the definition of initiating event classes as mutually disjoint. They are presented in connection with the STD for controlled LCO shutdown (Figure D.3).

Table D.4 Initiating Events for Full Power Operation - Comparison with NUREG/CR-4550 PSA for Grand Gulf[1]

NUREG/CR-4550 PSA			This Study	
Initiator Nomenclature	**Description**	**Mean Frequency (per year)**	**Corresponding Identifier**	**Remarks**
T1	Loss of Offsite Power (LOSP) transient	0.11	LOSP	Preserved as such
T2	Transients with loss of the Power Conversion System (PCS)	1.62	LoPCS	Preserved as such
T3A	Transients with PCS initially available	4.51	PTrip	General transients/plant trips, PCS initially available
T3B	Transients involving Loss of Feedwater (LOFW) but with the steam side of the PCS initially available	0.76	LoFW	Included (crudely due to a small contribution)
T3C	Transient caused by an Inadvertent Open Relief Valve (IORV) on the reactor vessel	0.14	IORV	Included (crudely due to a small contribution)
TIAS	Transient caused by loss of instrument air	8.1E-4	LoIAS	Included (crudely due to a small contribution)
A	Large Loss of Coolant Accident (LOCA)	1.0E-4	LOCA.L	Leakage of primary coolant inside containment is explicitly inciuded due to interference with RHR/LPCI function
S1	Intermediate LOCA	3.0E-4	LOCA.M	
S2	Small LOCA	3.0E-3	LOCA.S	
S3	Small-small LOCA (recirculation pump seal LOCA)	3.0E-2	-	Not explicitly covered due to small contribution
V	Interfacing system LOCA (failure of a high/low pressure interface in the primary system)	(see Section 4.4.15)	-	
R	Vessel Rupture	(see Section 4.4.16)	-	

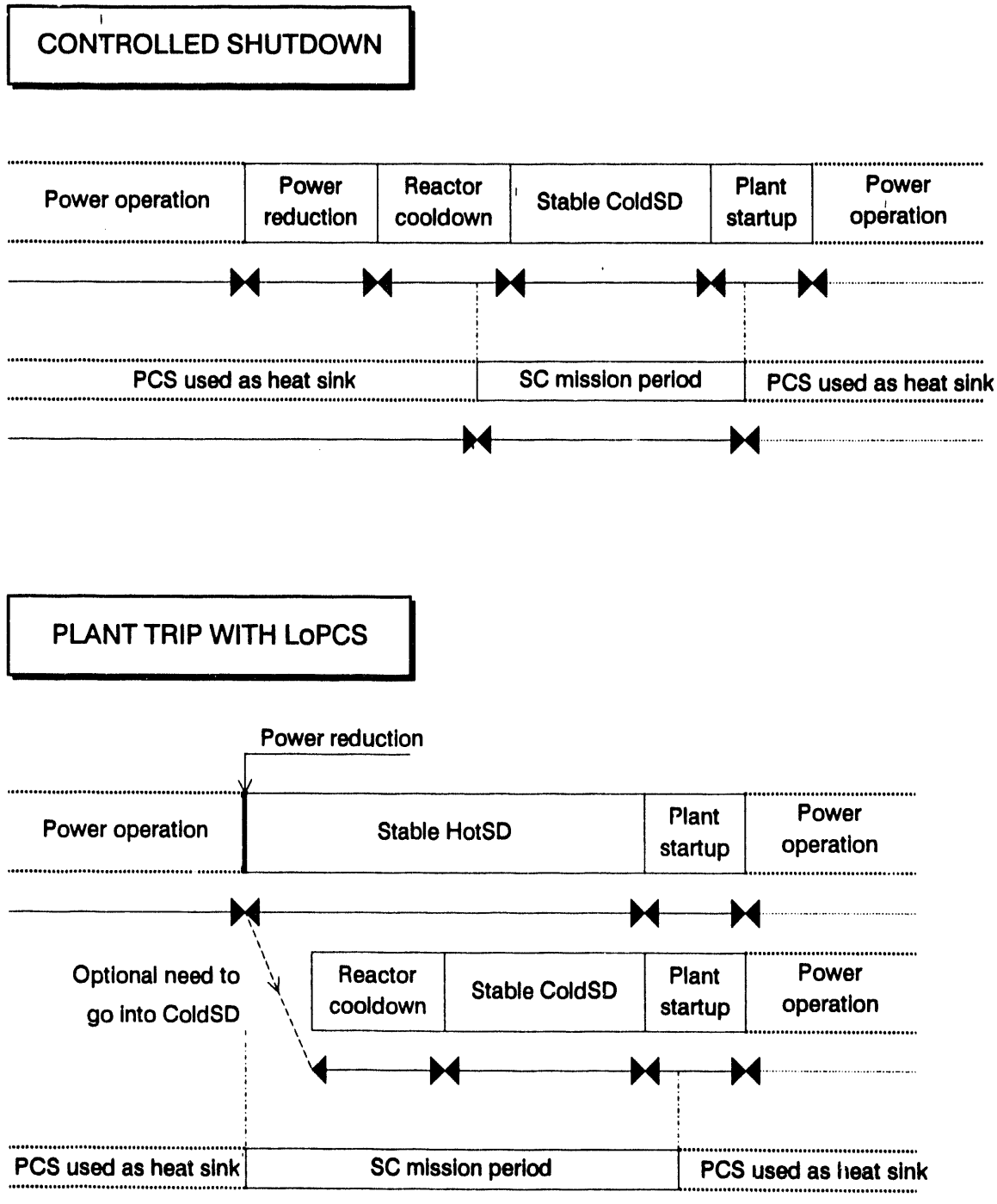


Figure D.1 Shutdown phases and their relation with shutdown cooling (SC) mission period for two basic cases: controlled shutdown and plant trip with loss of power conversion system (LoPCS) transients

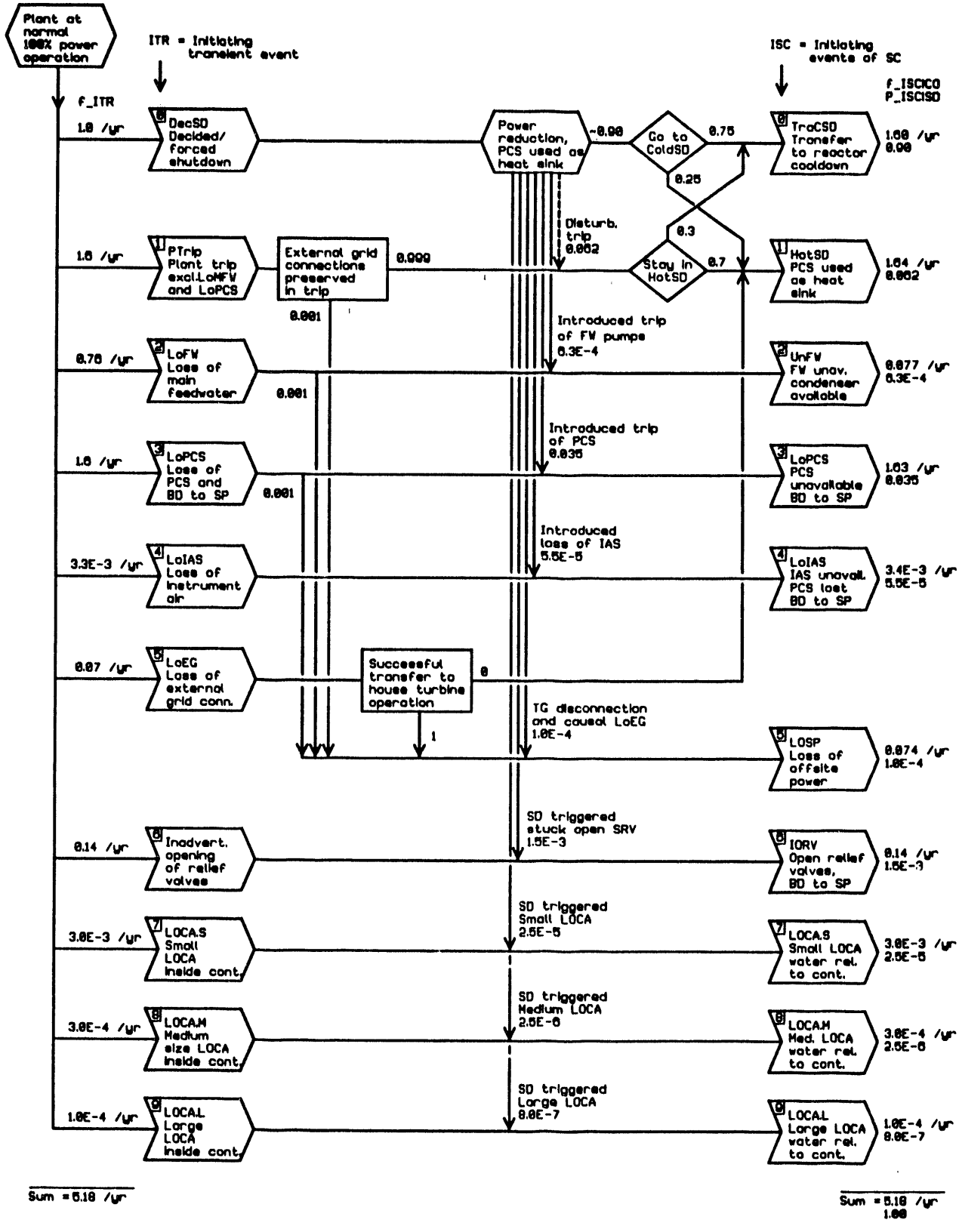


Figure D.2 Shutdown transient diagram (STD) for full-power operational state

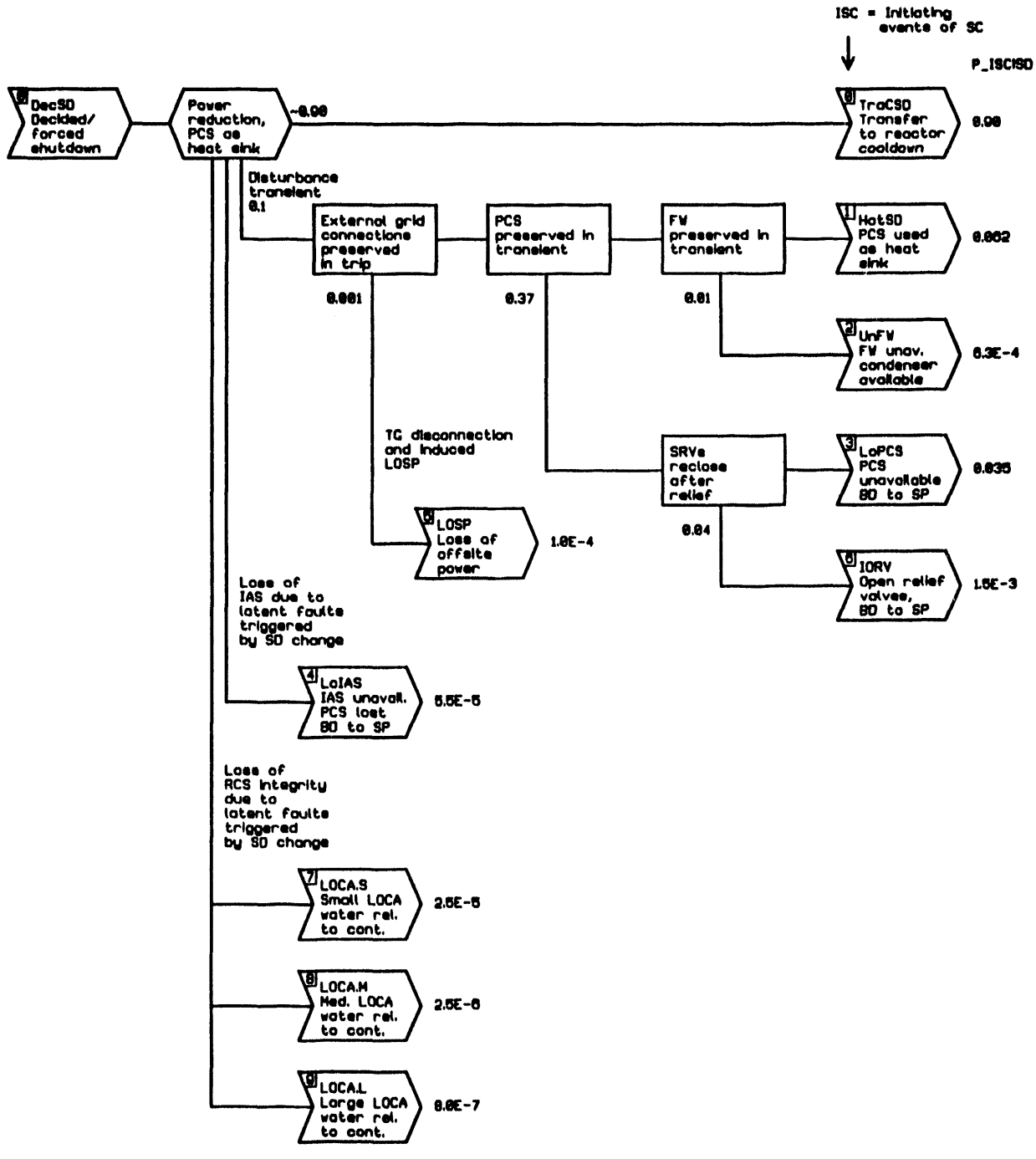


Figure D.3 Shutdown transient diagram (STD) for controlled LCO shutdown

APPENDIX E

EXTENDED EVENT SEQUENCE DIAGRAMS

LIST OF TABLES

LIST OF FIGURES

This appendix describes the preparation of extended event sequence diagrams (EESDs) to describe plant response to the RHR challenge events, which were discussed in connection with shutdown transient diagrams (STDs) in Appendix D. Assumptions on the plant behavior are based on the information from the GG/PSA study.[1] The primary emphasis is put on the LOSP scenario, because this presumably is the most important contributor. The EESD models for other RHR challenge events are then either reduced to the LOSP model or selectively worked out in regard to principal differences. The EESD models of the TVO/RHRS study[2] are used as a starting point.

E.1. General Principles Of EESD Modeling

E.1.1 Modeling Syntax of EESD

The approach of modeling event sequences using EESD is described in Chapters 2 and 4 of this report, and in more detail in reference 2. It is important to emphasize that the EESD model is laid out according to the following rules:

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

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

E.1.2 Connection to System Models

EESD models would become overly extensive if drawn down to the fine level of system detail. It is hence desirable to use functional entities in analogy to the event tree headings of PSA. An example of such a functional entity is reactor coolant supply while in pressurized state (High Pressure Mode), which can be accomplished by a successful operation of High Pressure Core Spray (HPCS) or Reactor Core Isolation Cooling (RCIC) functions. (In some sequences, also feedwater pumps or control rod drive system can be used for high pressure injection; these are not included in the simple example discussed below.)

The loss of HPM implies, thus, failure of both HPCS and RCIC, which is described, according to the usual convention, by the following Boolean event expression:

HPM = HPCS * RCIC

In an EESD model, the quantification is based on evaluating transition rates or probabilities of failure paths. This failure event could be described in terms of fault tree models down to combinations of system/component failures and other corresponding basic events. An equivalent presentation by use of Boolean Event Expression is, however, preferred in connection with EESD models, necessitating strong modularization of system models.

In this approach the contributors to loss of HPM are expanded as:

HPCS = HCS + AC/DC.3 + SSW.C + CST + SWO/SP

RCIC = RCI + DC.1 + SSW.A + CST + SWO/SP

The system modules, HCS and RCI, representing respective pump trains are examples of typical system modules, which can be used as basic entities in EESD model treatment. On the contrary, the AC/DC supply entities above need to be further expanded into presentation in terms of offsite power supply, diesel generators, station batteries, bus equipment, etc., to properly take into account hardwired and functional dependencies. These types of expansions for system modules are described in Reference 2.

E.1.3 Grouping of Cut Sequences

After the failure path elements are expanded into presentations by basic system entities, a MCS (minimal cut set) presentation for the whole path can be derived. Each MCS represents a possible event sequence, which realizes the failure path. Hence, in connection with EESD models, they are called Cut Sequences. The attribute "minimal" is dropped, because often partial losses of a safety function also need be considered in addition to total failures (as mutually exclusive cases). It also should be noted that for Cut Sequences, specific operational details may be necessary to take into account along with the general dependencies described in the overall EESD model.

E.1.4 Loss of Room/Component Cooling Sequences

The room/component cooling for coolant supply systems, i.e., HPCS, RCIC, LPCS, and LPCI, is a critical function served by SSW trains, and thus crucial for this study. It is assumed in this stage that the associated heatup times, i.e. the time margins available for recovery in room/component cooling cases, are constant, independent of the time elapsed from reactor shutdown and of the status of suppression pool (Appendix F). This assumption may not be fully realistic, but is very convenient as it allows consideration of the room/component cooling failures as independent MCSs not directly coupled with other sequences associated with plant states. These MCSs are evaluated in connection with function and system structures.

E.2. Operational States and Preferences

E.2.1 Operational Combinations

The operational states for possible combination of coolant supply systems and residual heat removal paths are outlined in Table E.1. They are arranged crudely in the order of operational preference (e.g., RHR/SDC is a preferred path compared to RHR/SPC, and RCIC is preferred to HPCS). It is assumed that in normal transfer to cold SD state, PCS is used until changeover to RHR/SDC at 135 psig; i.e., steam release to SP does not normally occur.

The operational preference of Table E.1 was followed in modeling event sequences with the following refinement:

- RCIC and HPCS are both assumed to be started, if operable, in demand situations, and both are assumed to be kept in the operation state over the whole mission period

- LPCS is preferred to LPCI; i.e., LPCI is considered as a backup system which is called for only when LPCS does not succeed

- In the low pressure state, switchover to RHR/SDC is preferred, and assumed to be undertaken, even if LPM coolant supply and RHR/SPC would be successfully started and operated over the early stage of the SC mission

Furthermore, in regard to the use of backup coolant supplies requiring special manual operations, the following operational preference of manual alignment/restart is assumed: (1) SSW cross-tie, (2) CDS feed, and (3) firewater system. It was assumed in this stage that one and only one of the three is credited (corresponding to the assumption that, if alignment fails for the first option attempted, then it is likely that further attempts will also fail).

E.2.2 Operational Dependencies

The operational dependencies of selected systems on initiating events of shutdown cooling are shown in Table E.2, based on the information inferred from the assumptions in the event trees of GG/PSA.[1] For the inadvertent opening of relief valves (IORV), there is some ambiguity in regard to loss of condenser and related implications. In this study, it is consistently assumed that IORV generates similar isolations as LOCAs; i.e., PCS, CDS and IAS will be lost.

E.2.3 Implications of Containment Venting

In the pressure reduction at containment venting, RCIC will be tripped due to the loss of suction head. However, HPCS will survive containment venting.

E.2.4 Implications of Reactor Depressurization

After automatic or manual depressurization, condenser is assumed unavailable as steam sink (SP is used instead). Possible repressurization of the reactor to return to high pressure mode, and restoration of PCS as steam sink, are not considered. In high pressure mode, PCS is assumed to be the preferred steam sink, if available. The use of condenser as steam sink is assumed independent from the operability of main feedwater.

E.3. Loss of Offsite Power (LOSP)

E.3.1 General Structure of LOSP Cases

The LOSP transfer event from the STD (Figure D.2 of Appendix D) is first structured into several subcases in Figure E.1. As a boundary assumption, the sequences concerning failure of reactor scram or loss of overpressure protection are not evaluated in detail. But, the cases where the safety/relief valves (SRV) are stuck open need to be considered as they pose a different type of challenge both on coolant supply function and suppression pool cooling.

It seems appropriate to use the model structure presented in Figure E.1, meaning that separate detailed EESDs are prepared for the cases according to the number of SRVs failing to reclose. The failure of controlled steam release to SP in hot shutdown state is not taken into account as it is effectively backed up by overpressure protection/ADS function (refer to the boundary assumption discussed above).

The possibility to manually reclose a SRV (in the case where it is stuck open due to a pilot fault, for example), was not credited in GG/PSA. The case of three or more SRV stuck open is not considered in the GG/PSA. These cases give anyway only a small contribution, and therefore, they are not considered in this stage in connection with LOSP.

E.3.2 EESD for LOSP_P0

Figure E.1 shows the detailed EESD for LOSP scenario with proper reclosure of SRVs.

E.3.2.1 *Normal Path of Operation*

In LOSP due to isolation of PCS, HPCS and RCIC are automatically started for reactor coolant inventory control. Steam is dumped to SP, and operators manually start RHR/SPC. If these systems operate successfully, meaning that adequate DG power supply is available, a stable HotSD state is entered. It is assumed that, if no additional failures occur, the plant is kept in this state, while efforts are concentrated on the recovery of offsite power (OSP).

E.3.2.2 *Failure of RHR/SPC Sequences*

If RHR/SPC fails at startup or during mission time prior to OSP/PCS recovery, the operators proceed to manually depressurize the reactor in order to use RHR/SDC (part 2 of Figure E.1). If depressurization does not succeed, SP will begin to warm up, while reactor is in HotSD state. If this continues without recovery and intake is from SP, then RCIC will be lost due to loss of suction head at containment pressure relief (CoPRe), which is undertaken at 17.25 psig (255°F), or at SP temperature of about 265°F.[1] However, HPCS will survive containment venting.

When CST is depleted to a specific level, the switchover to SP intake is needed. The early injection phase from CST are for simplicity included in the startup of HPM function. If the depressurization is successful, but coolant supply from the low pressure systems, i.e., LPCS, LPCI or SSW Cross-Tie, fails, the possibility of repressurization and returning to HPM is not considered as discussed in section E.2.

RHR/CS could be used for SP and containment cooling, in specific failure combinations of RHR/SDC. There are also many other rearrangement options, depending on the failure situation. For example, it would help in getting at least slower warmup, if LPCI water would be directed via RHR heat exchangers. As a backup resort, SPMU and depleting warm water away from SP might be used. It is difficult to figure out to what extent this kind of resorts could be assumed manageable. Possible influences need to be checked in regard to the conclusions, specially for AOT situations where RHR/SDC is fully inoperable, implying that special type of shutdown operations are necessary.

E.3.2.3 *Loss of High Pressure Coolant Supply*

If high pressure coolant supply systems fail, then with ADS or manual depressurization, low pressure systems can be used to enter a stable ColdSD state as shown in Figure E.1 (part 3). This submodel is similar to the low pressure option part in Figure E.1 (part 2), except that now the high pressure coolant supply systems are failed, and hence repressurization possibility is not relevant.

If depressurization fails in connection with failure of high pressure coolant supply systems, the final resort is the use of enhanced CRD injection for coolant inventory control (part 4 of Figure E.1).

With an operating RHR/SPC, a stable HotSD state then can be entered. If RHR/SPC fails in this path, and recoveries are not successful until CoPRe, CRD will be lost at containment venting. Here also, some special resorts might be available to prolong SP warmup.

E.4. Loss of PCS Transients

The EESD models for RHR challenge transients with PCS initially lost, i.e., LoPCS and LoIAS, are only drafted in this stage, as they resemble much the LOSP scenario.

E.4.1 LoPCS

Figure E.2 shows the EESD for loss of power conversion system (LoPCS). In the first stage, LOSP model can be used with appropriate modifications of MCS presentations concerning the initial availability of OSP (and DGs in standby).

E.4.2 LoIAS

Figure E.3 shows the EESD for loss of instrument air system (LoIAS). In the first stage, the similar approach as for LoPCS can be followed, and the LOSP model can be used with appropriate modifications of MCS presentations concerning the initial availability of OSP (and DGs in standby), and initial inoperability state for CRD and FWS.

E.5. LOCA Events and IORV

The EESD models for LOCA events resemble the LOSP and LoPCS scenarios because PCS will be initially lost. However, the success criteria for coolant supply systems as well as the role of ADS change as the function of LOCA size as discussed below. In medium and large LOCA, suppression pool makeup (SPMU) is needed to use HPCS, LPCS or LPCI. However, SPMU is not needed if SSW cross-tie is used.

E.5.1 Small LOCA

Figure E.4 shows the EESD for small loss of coolant accident (LOCA.S). In the first stage, the transient models can be used as a framework. In fact, small LOCA is in many respects identical to LoIAS with respect to initial conditions.

E.5.2 Medium Size LOCA

Figure E.5 shows the EESD for medium-size loss of coolant accident (LOCA.M). As a remarkable difference compared to small LOCA, SPMU is necessary except the case where SSW-X is used. RCIC is assumed to be inoperable according to GG/PSA assumptions. ADS/manual depressurization is necessary in order to use LPM coolant supply. In medium as well as in large LOCA situations, RHR/SPC is not so critical as compared to loss of coolant supply, and hence not described in detail in the EESD.

E.5.3 Large LOCA

Figure E.6 shows the EESD for large loss of coolant accident (LOCA.L). ADS/manual depressurization is not needed to use LPM coolant supply. This is the only remarkable difference as compared to medium-size LOCA. HPCS is designed to function in a Large LOCA, but RCIC will be lost.

E.5.4 IORV

This reduces effectively to LOCA scenarios, depending on how many SRVs open and do not reclose (see assumptions for initial conditions in Table E.2). In this stage, only the most likely case of one SRV opening and failing to reclose is included, and handled as a small-LOCA case.

E.6. Normal Shutdowns and Plant Trips

The EESD models for RHR challenge events with PCS initially available, i.e., TraCSD, HotSD and UnFW, are only drafted in this stage.

E.6.1 TraCSD

Figure E.7 shows the EESD for transfer to cold shutdown (TraCSD). Up to the point of successful RHR/SDC, the scenarios of HotSD apply. In ColdSD state, the applicable transient/LOCA initiators as well as failure of RHR/SDC are considered.

E.6.2 HotSD

Figure E.8 shows the EESD for hot shutdown. In the first stage, HotSD state is handled as the power operation state in regard to possible initiating events and sequence scenarios.

E.6.3 UnFW

Figure E.9 shows the EESD for loss of feedwater (UnFW). It reduces to HotSD and TraCSD scenarios, except for the initial need of HPCS/RCIC startup, from which similar failure sequences as in LOSP/LoPCS are developed.

E.7. Boundaries, Limitations and Unresolved Issues of Transient Modeling

As discussed in the preceding sections, many simplifications were made in modeling event scenarios, as well as remarkable boundary assumptions. Their significance may be further checked in the continuation. The following issues seem most important:

- inclusion of coolant diversion paths (plus flooding and fire) in association with a LCO repair outage due to failures in RHR/SSW trains

- manual realignment to use special paths for coolant supply and RHR, either as a backup resort in specific transient/failure combinations, or in the case of LCO shutdown due to complete failure of the RHR/SDC function

- optional staying in hot shutdown with use of PCS versus proceeding to POS 5 to use ADHRS or RWCU, in complete failure of the RHR/SDC function

REFERENCES

1. M. Drouin, J.L. LaChance, B.J. Shapiro, et al., "Analysis of Core Damage Frequency: Grand Gulf, Unit 1 Internal Events, NUREG/CR-4550, SAND86-2084, Rev. 1, Vol. 6, September 1989.

2. T. Mankamo and M. Kosonen, "Continued Plant Operation Versus Shutdown in Failure Situations of Standby Safety Systems," IAEA/TechSpec Pilot Study Program, NKS/SIK-1(91)4, August 1991.

Table E.1 Operational States for Possible Combination of Coolant Supply Systems and Residual Heat Removal Paths

Coolant supply \ RHR path	PCS/ condenser	RHR/ SDC	RHR/ SPC	RHR/ CS	Filtered venting CVS
HPM High pressure modes					
PCS/FWS	Normal power operation state	RHR/SDC is a low pressure system	FWS can be used as backup in these RHR modes		
RCIC	Applicable in the loss of FWS		Steam relief to suppression pool (SP)	Steam/water release to containment (LOCA scenarios)	RCIC lost in venting situation
HPCS					Steam relief to containment
CRD					
LPM Low pressure modes		Coolant recirculated			
LPCS	In LPM, hot water can be released from RCS to condenser, special alignments required	RHR/SDC is preferred in the LPM state, no makeup required	Successful pressure reduction or ADS presumed, steam dumped to SP		LPM systems may be used in venting situation, assuming sufficient pressure reduction
LPCI					
SSW-B-X crosstie					
Fire water system					

Table E.2 Operational Dependencies of Selected Systems on Initiating Events of Shutdown Cooling

Initiating event of SC		System status or implications				
		PCS	CDS	IAS	FrWS	CRD
0	TraCSD	Idle	Standby	Operating	Standby	Standby
1	PTrip/HotSD	Operating	Operating	Operating	Standby	Operating
2	UnFW	Available as steam sink	Lost	Operating	Standby	Standby
3	LoPCS	Lost	May be restarted	Operating	Standby	Standby
4	LoIAS	Lost	Lost	Lost	Lost	Lost
5	LOSP	Lost	Lost	Degraded	Affected via IAS	Affected via IAS
6	IORV	Isolated /*Note 1*/	Isolated /*Note 1*/	Isolated /*Note 1*/	Inoperable due to LoIAS	Inoperable due to LoIAS
7 8 9	LOCA.S, LOCA.M, LOCA.L	Isolated	Lost	Isolated: LOCA + CONT-ISO-S /*Note 2*/	Inoperable due to LoIAS	Inoperable due to LoIAS

Notes: 1 Based on GG/PSA, the LOCA situation implications are applied also to LoIAS
2 CONT-ISO-S is containment isolation signal

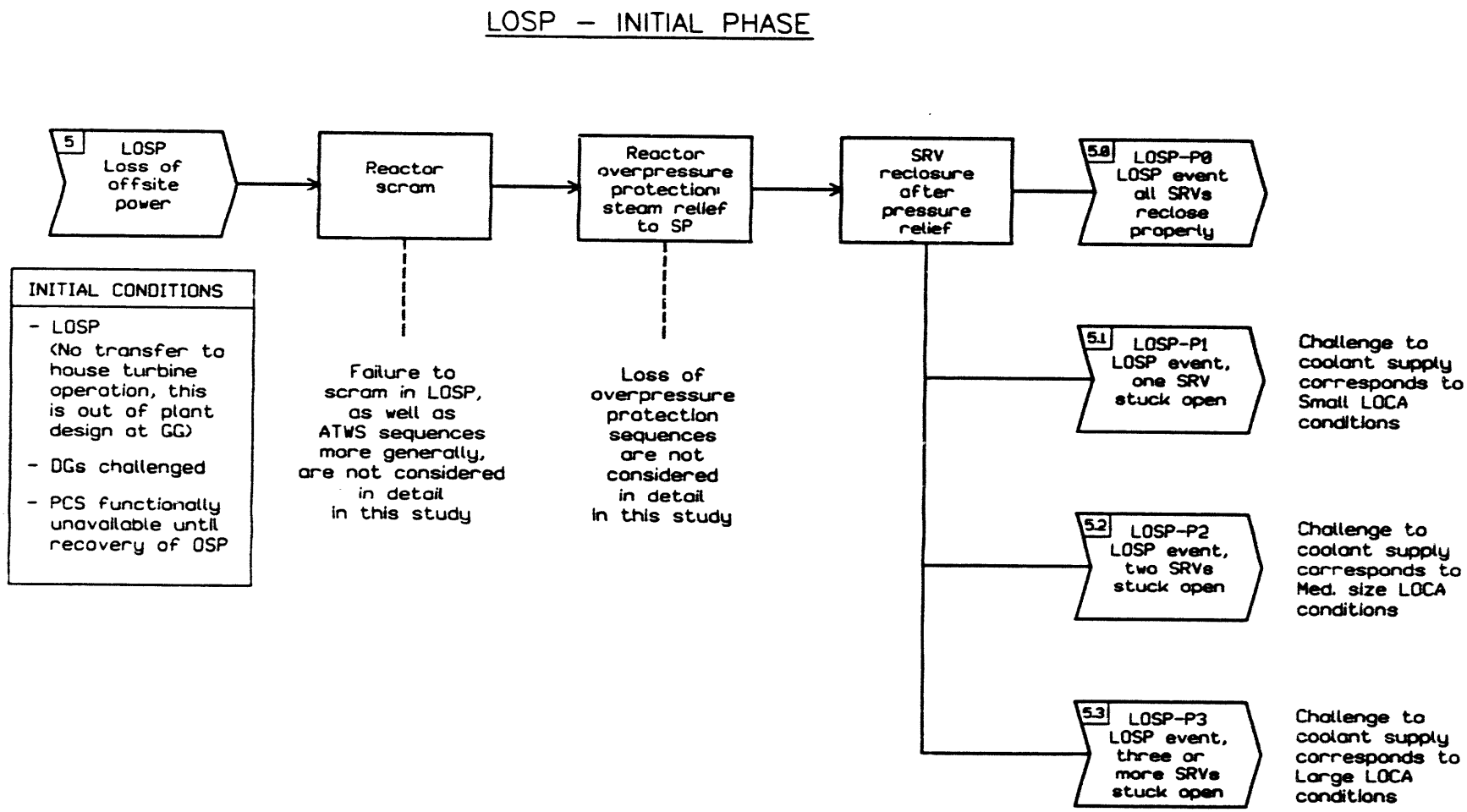


Figure E.1 Extended event sequence diagram (EESD) for loss of offsite power (LOSP) (part 1 of 4)

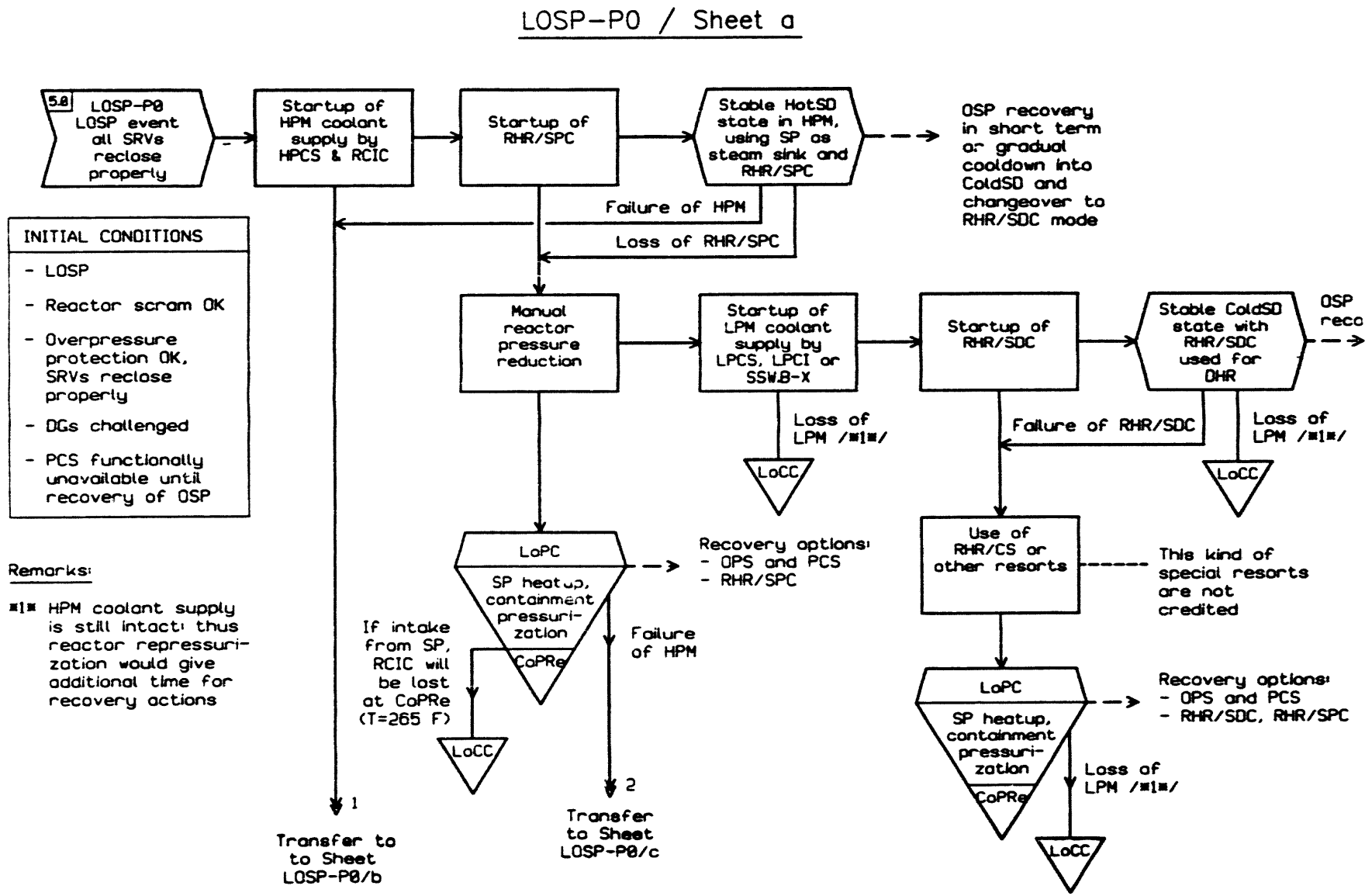


Figure E.1 Extended event sequence diagram (EESD) for loss of offsite power (LOSP) (part 2 of 4)

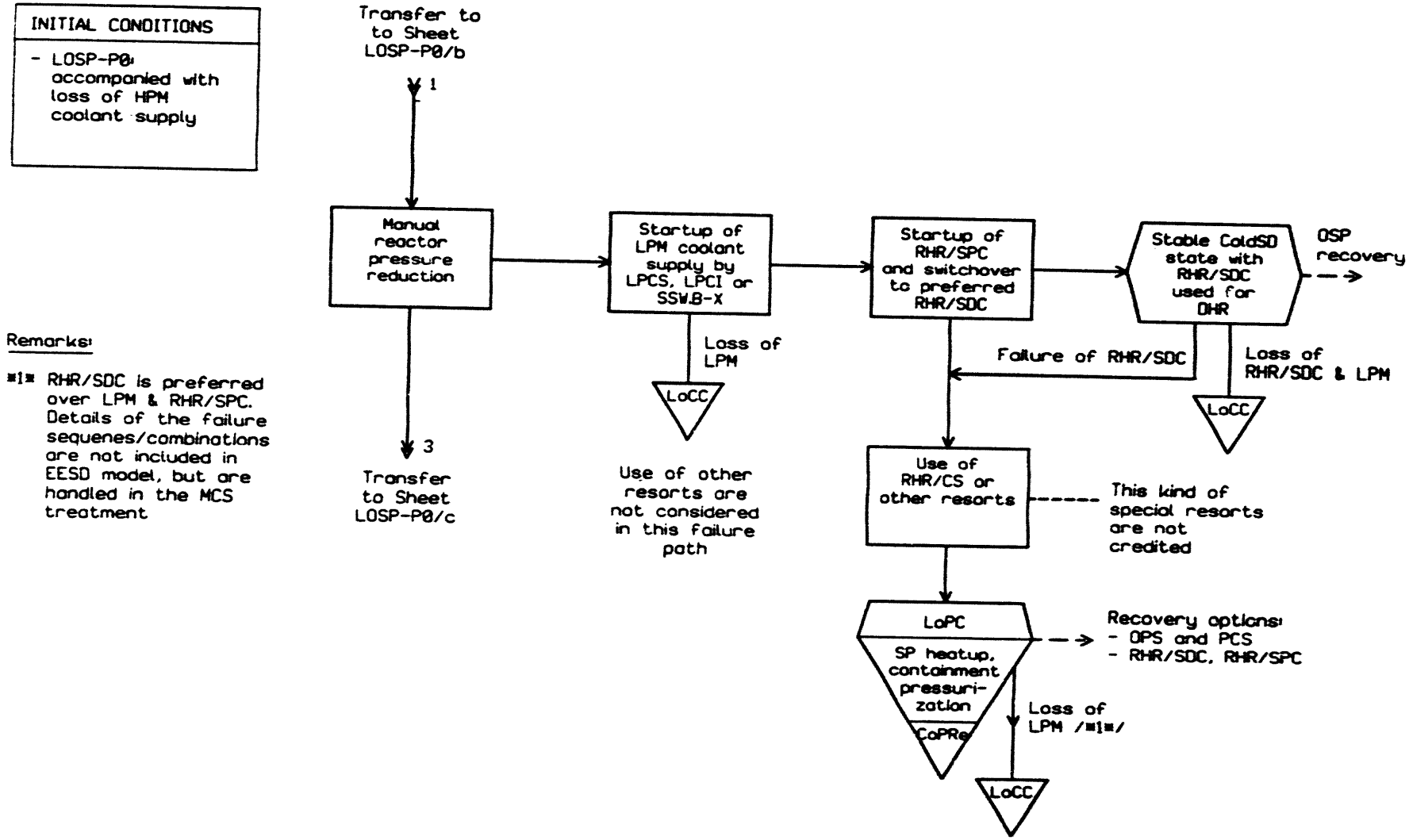


Figure E.1 Extended event sequence diagram (EESD) for loss of offsite power (LOSP) (part 3 of 4)

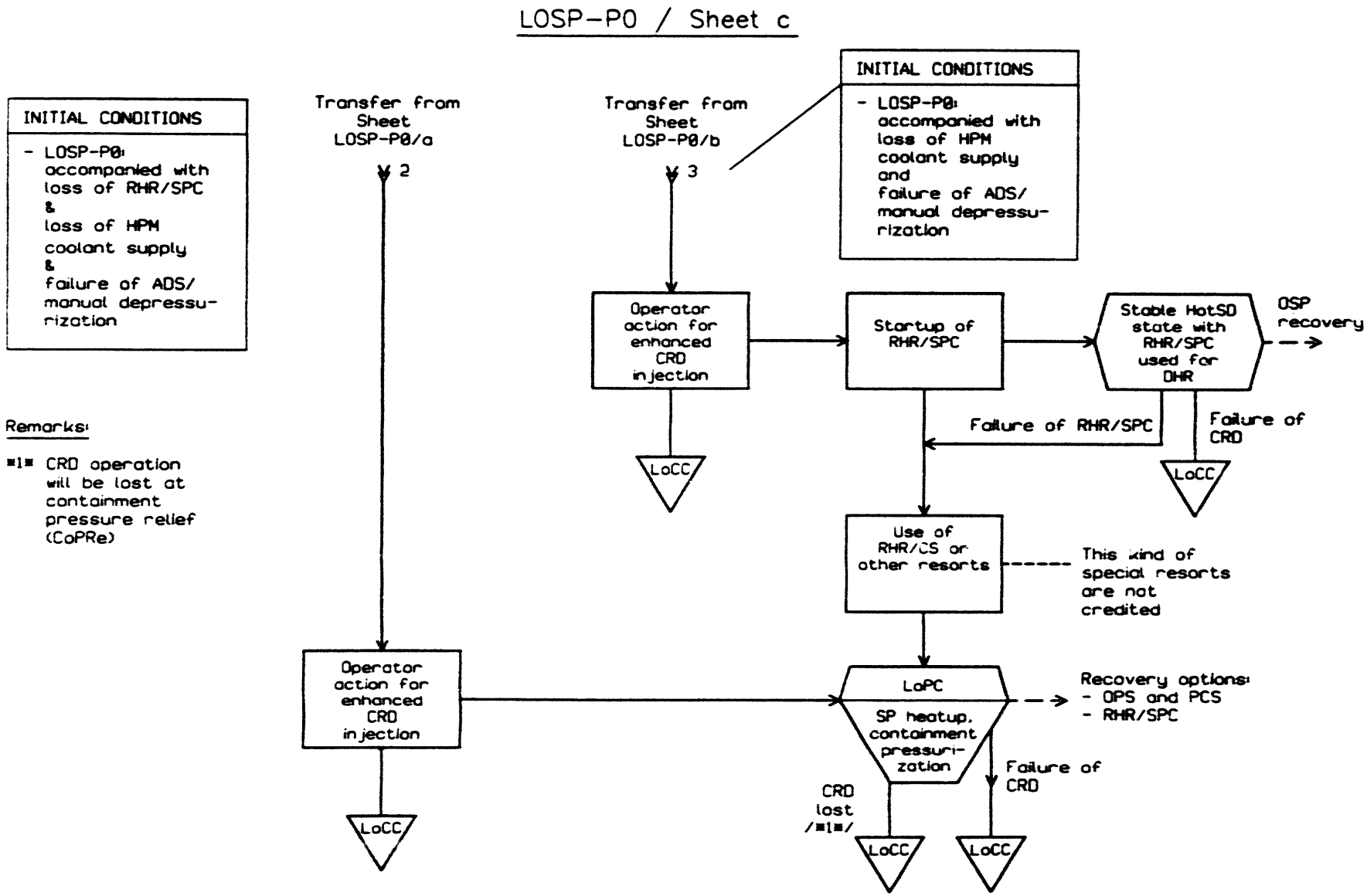
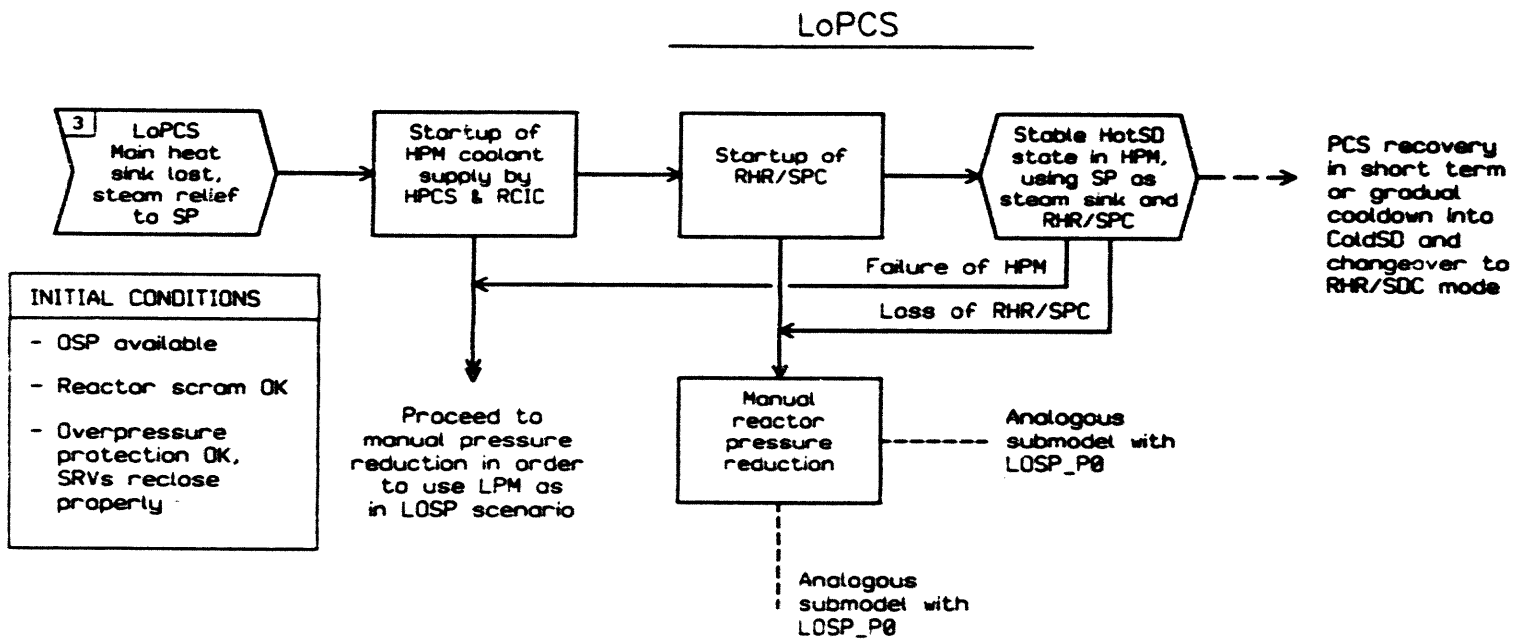


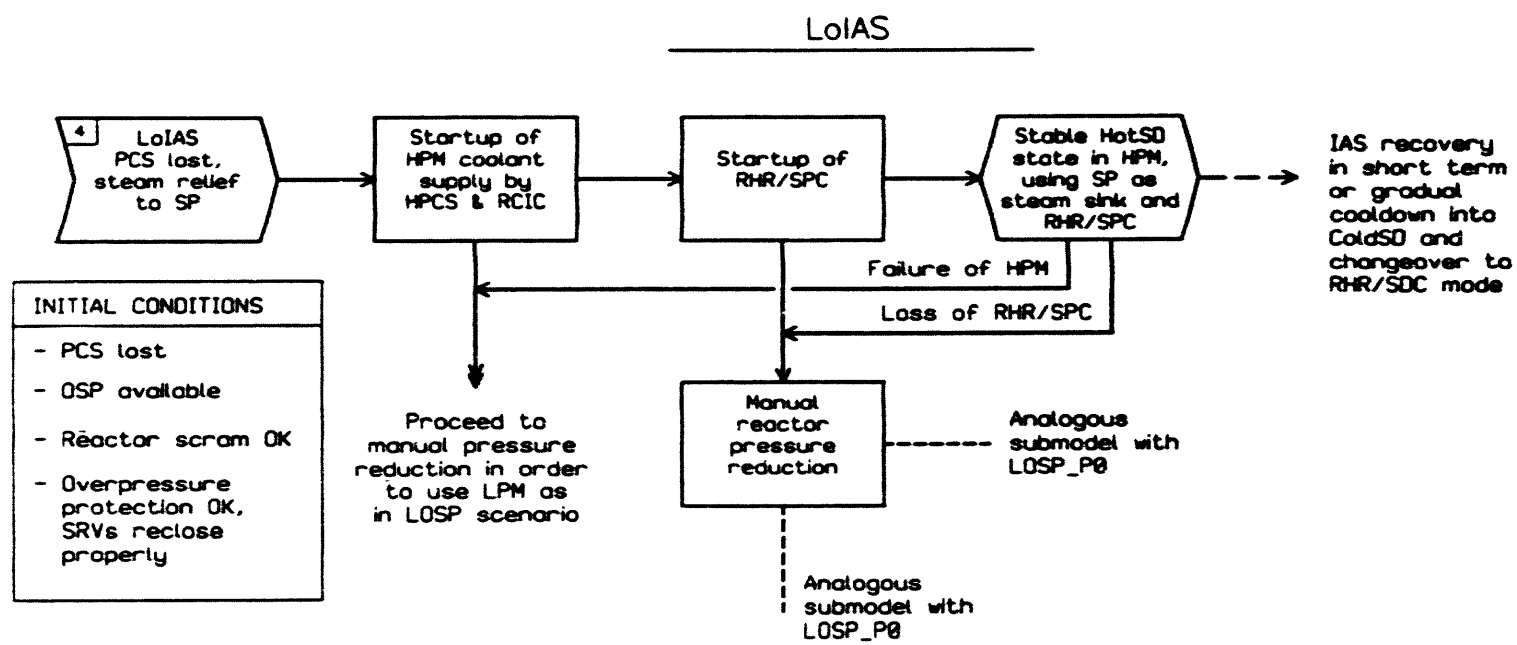
Figure E.1 Extended event sequence diagram (EESD) for loss of offsite power (LOSP) (part 4 of 4)



Remarks:

[1] Pilot study calculations are done with the same selected Cut Sequences as for LOSP case, with the distinction, that OSP is initially available.

Figure E.2 Extended event sequence diagram (EESD) for loss of power conversion system (LoPCS)



Remarks:

1 Pilot study calculations are done with the same selected Cut Sequences as for LOSP case, with the distinction, that OSP is initially available.

Figure E.3 Extended event sequence diagram (EESD) for loss of instrument air system (LoIAS)

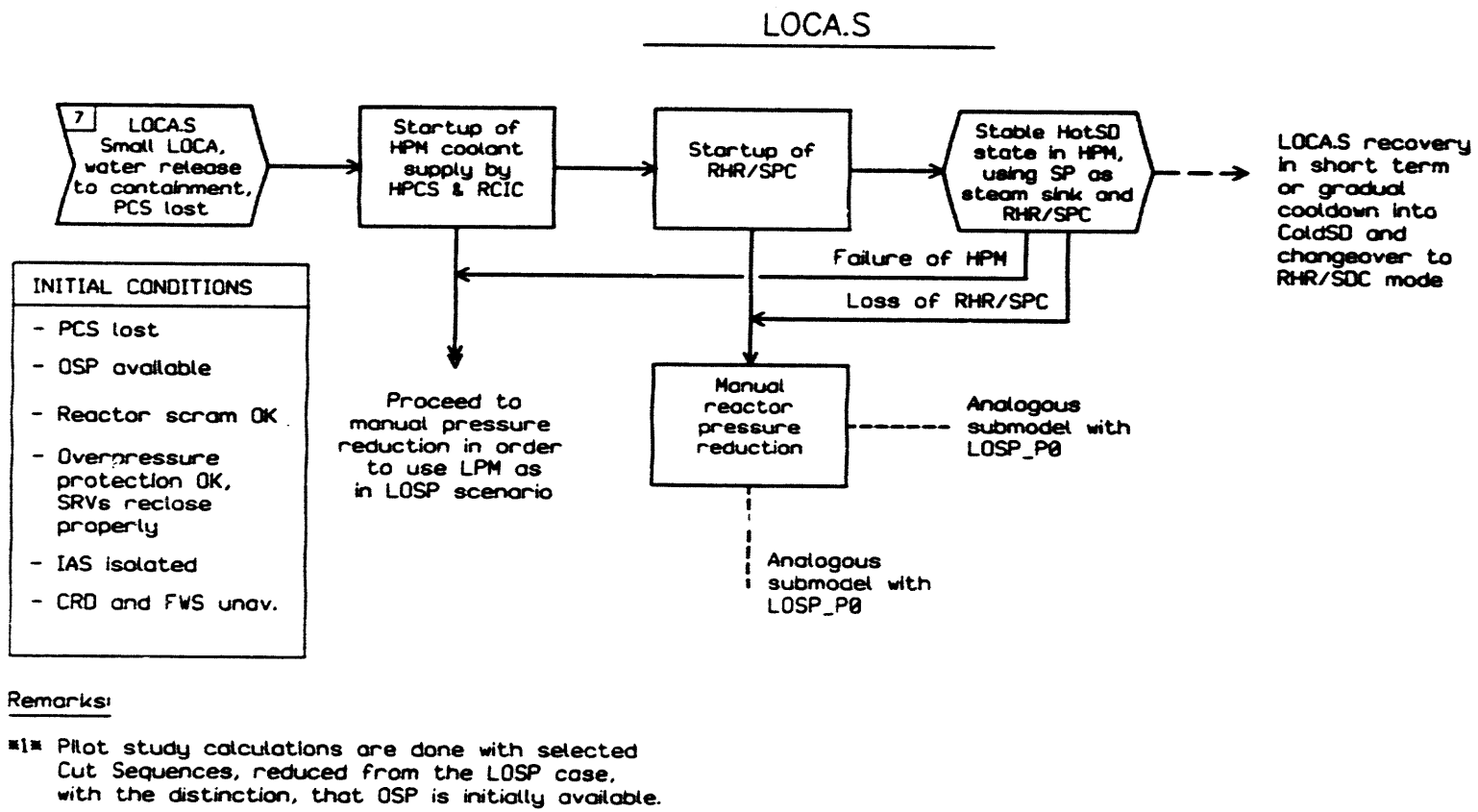


Figure E.4 Extended event sequence diagram (EESD) for small LOCA (LOCA.S)

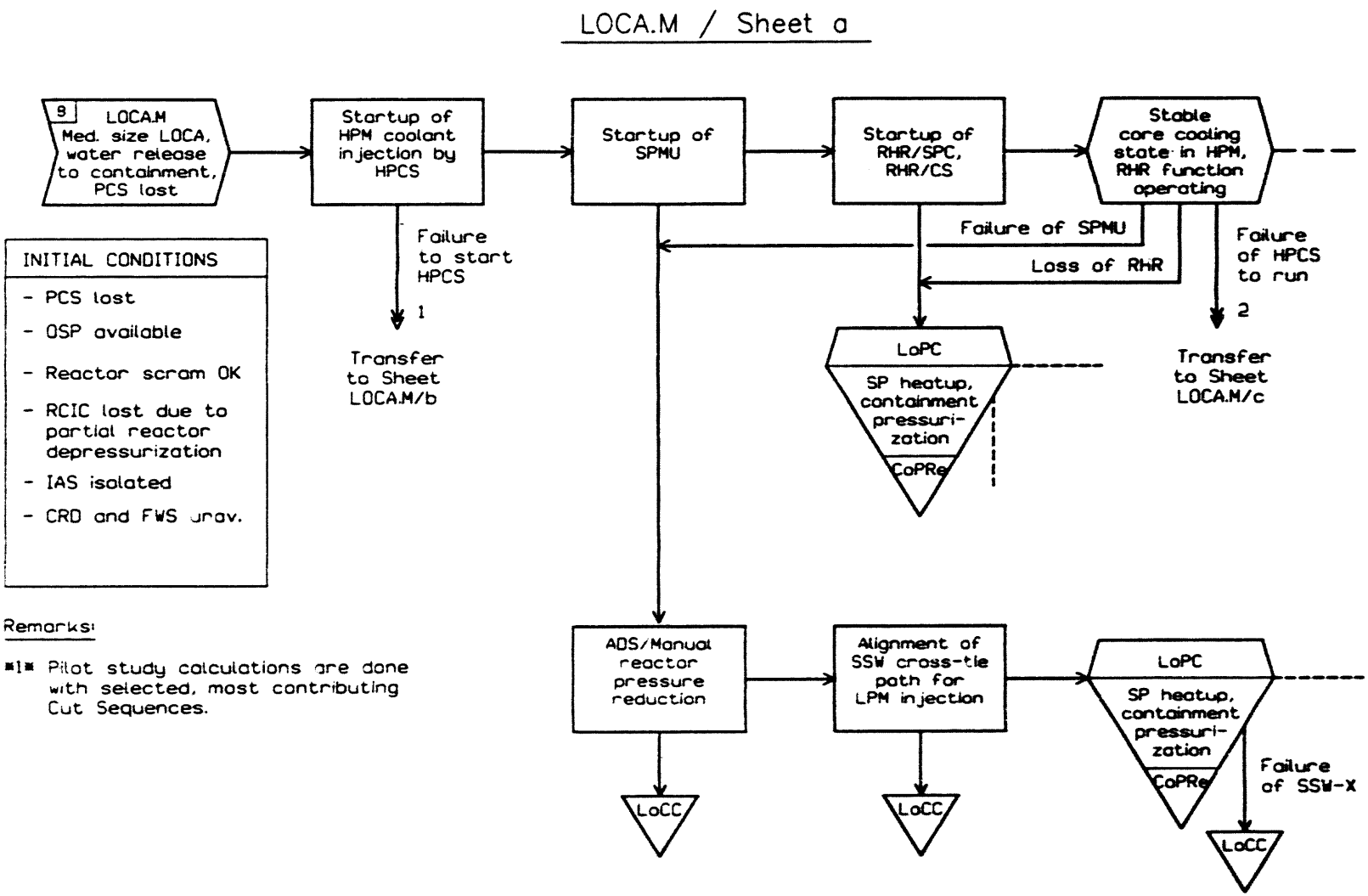


Figure E.5 Extended event sequence diagram (EESD) for medium-size LOCA (LOCA.M) (part 1 of 3)

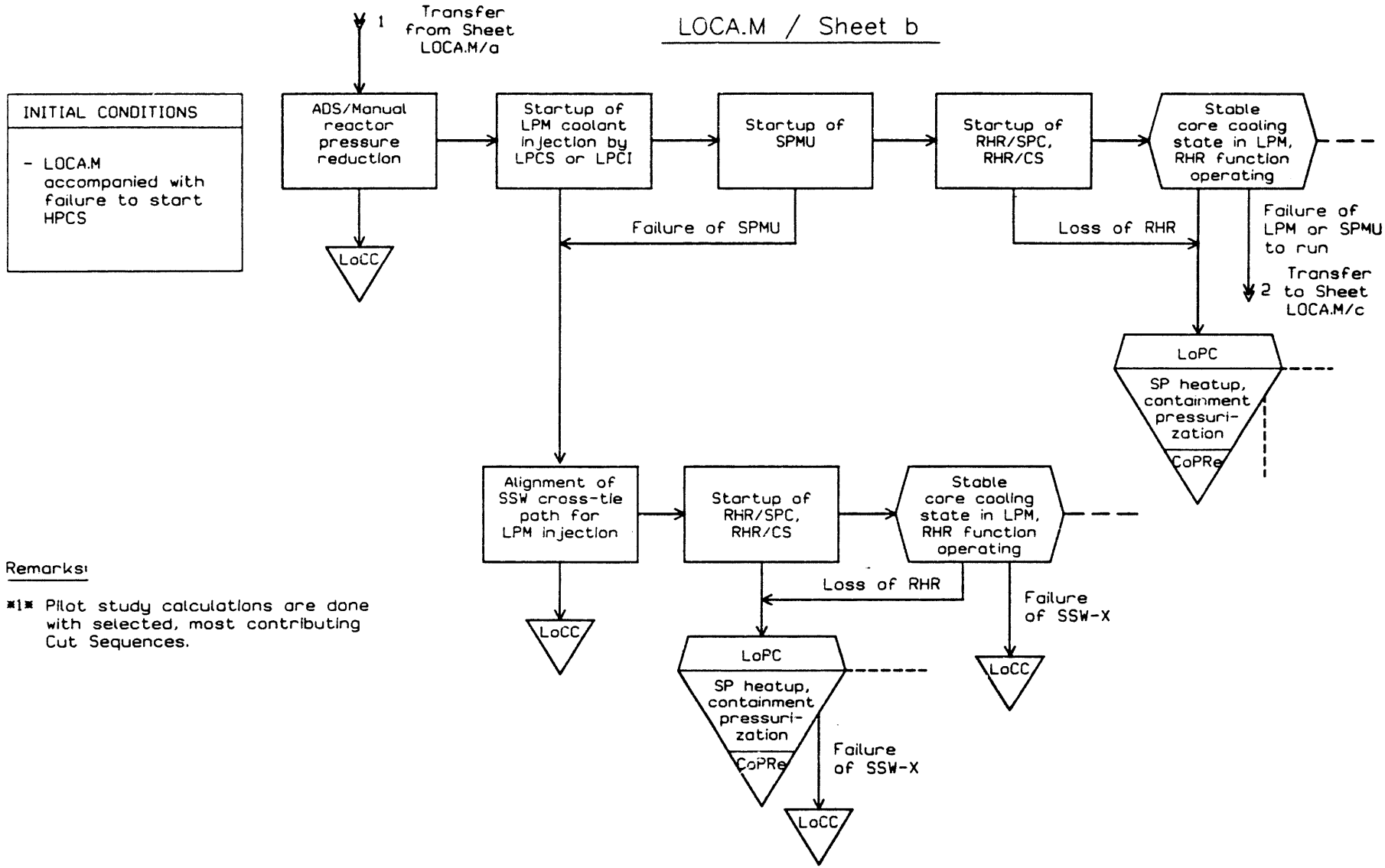


Figure E.5 Extended event sequence diagram (EESD) for medium-size LOCA (LOCA.M) (part 2 of 3)

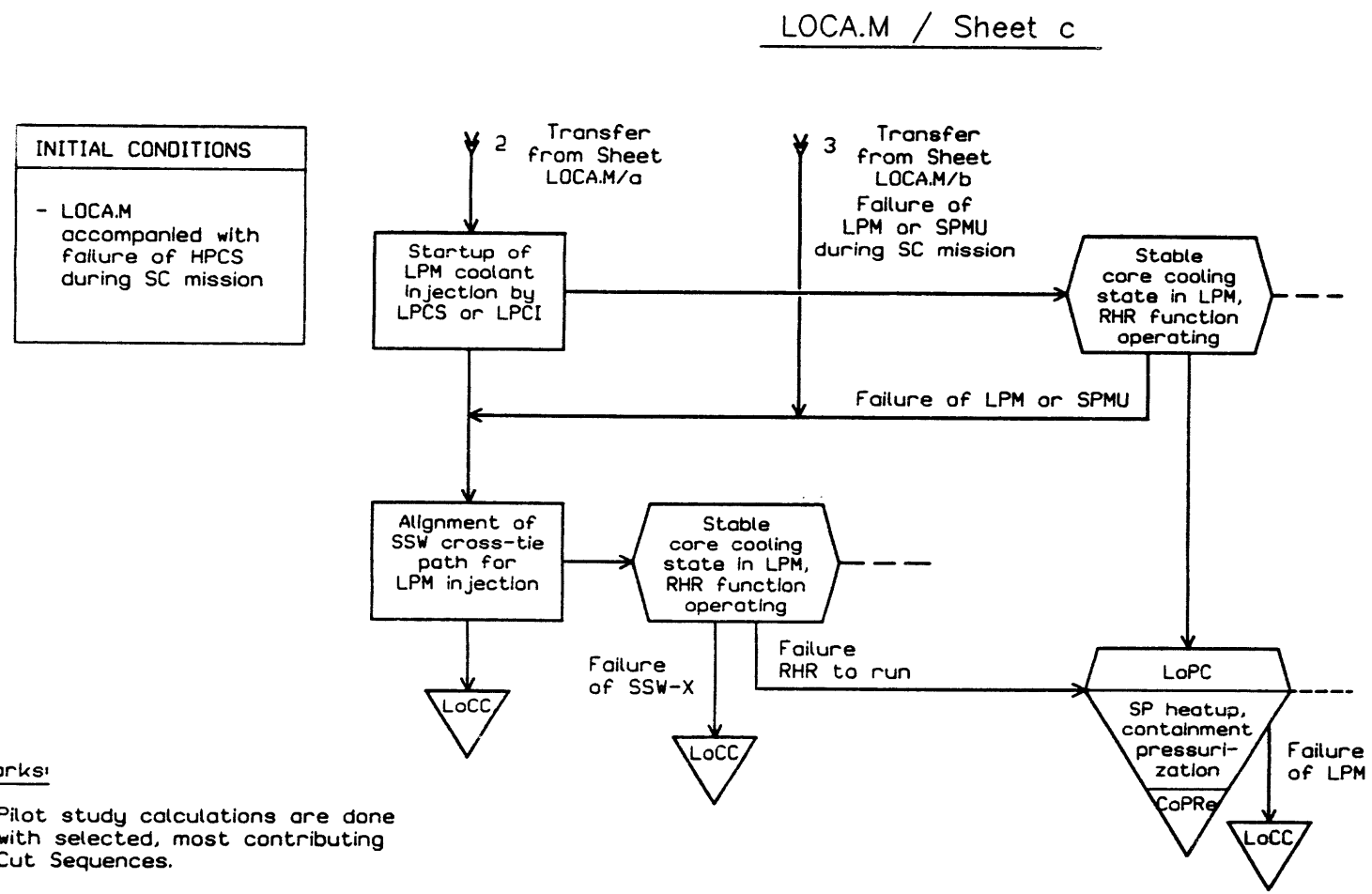


Figure E.5 Extended event sequence diagram (EESD) for medium-size LOCA (LOCA.M) (part 3 of 3)

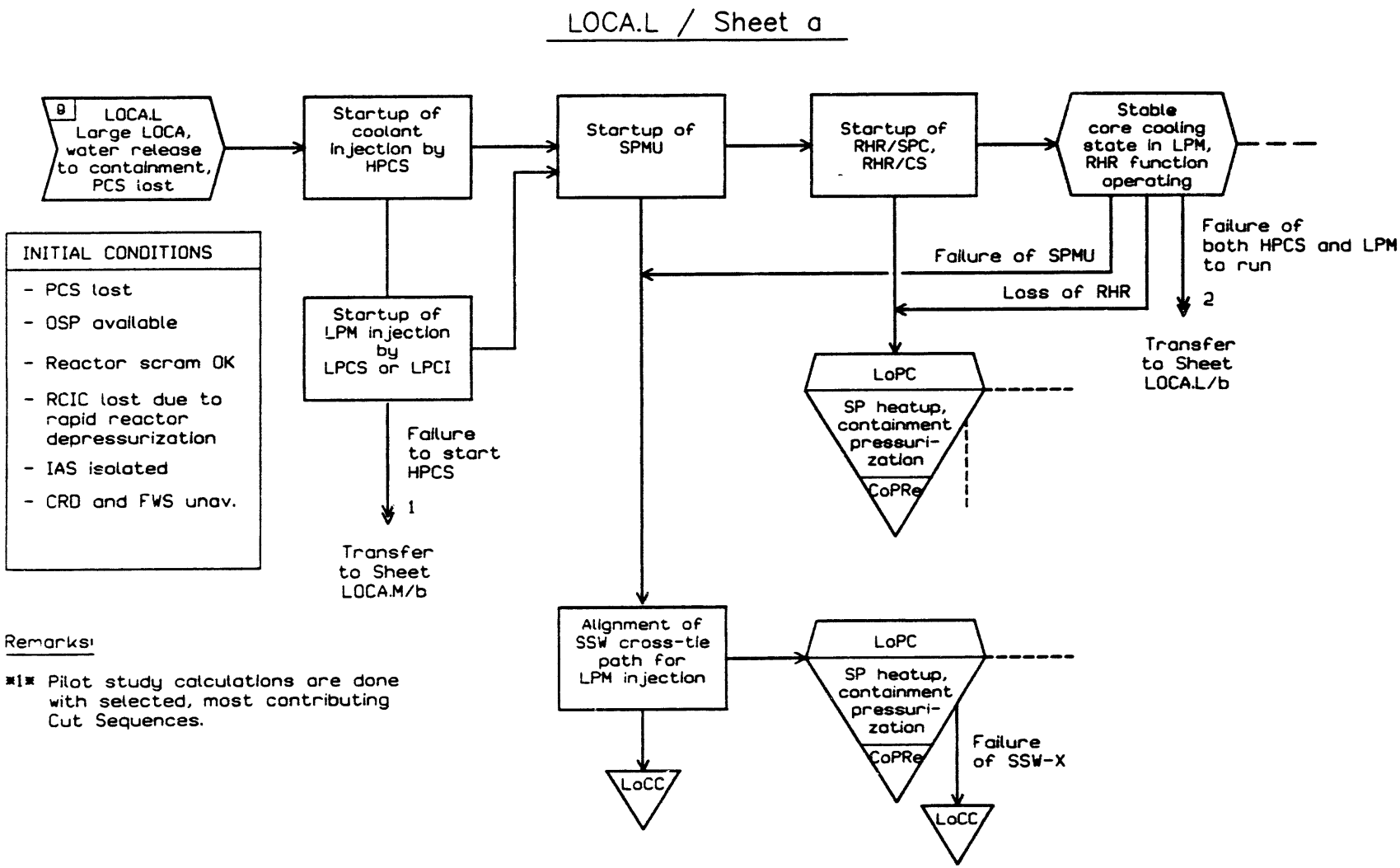


Figure E.6 Extended event sequence diagram (EESD) for large LOCA (LOCA.L) (part 1 of 2)

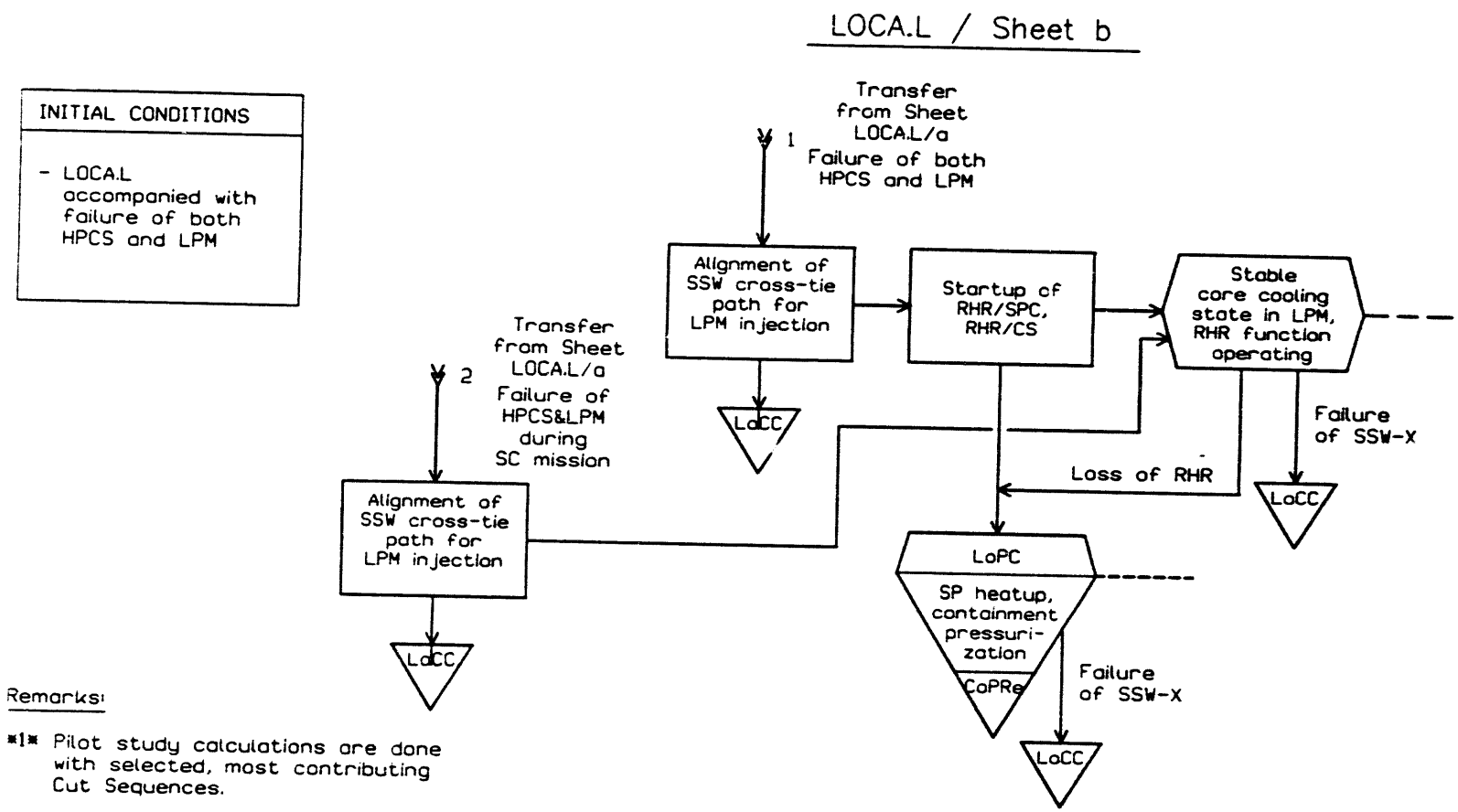


Figure E.6 Extended event sequence diagram (EESD) for large LOCA (LOCA.L) (part 2 of 2)

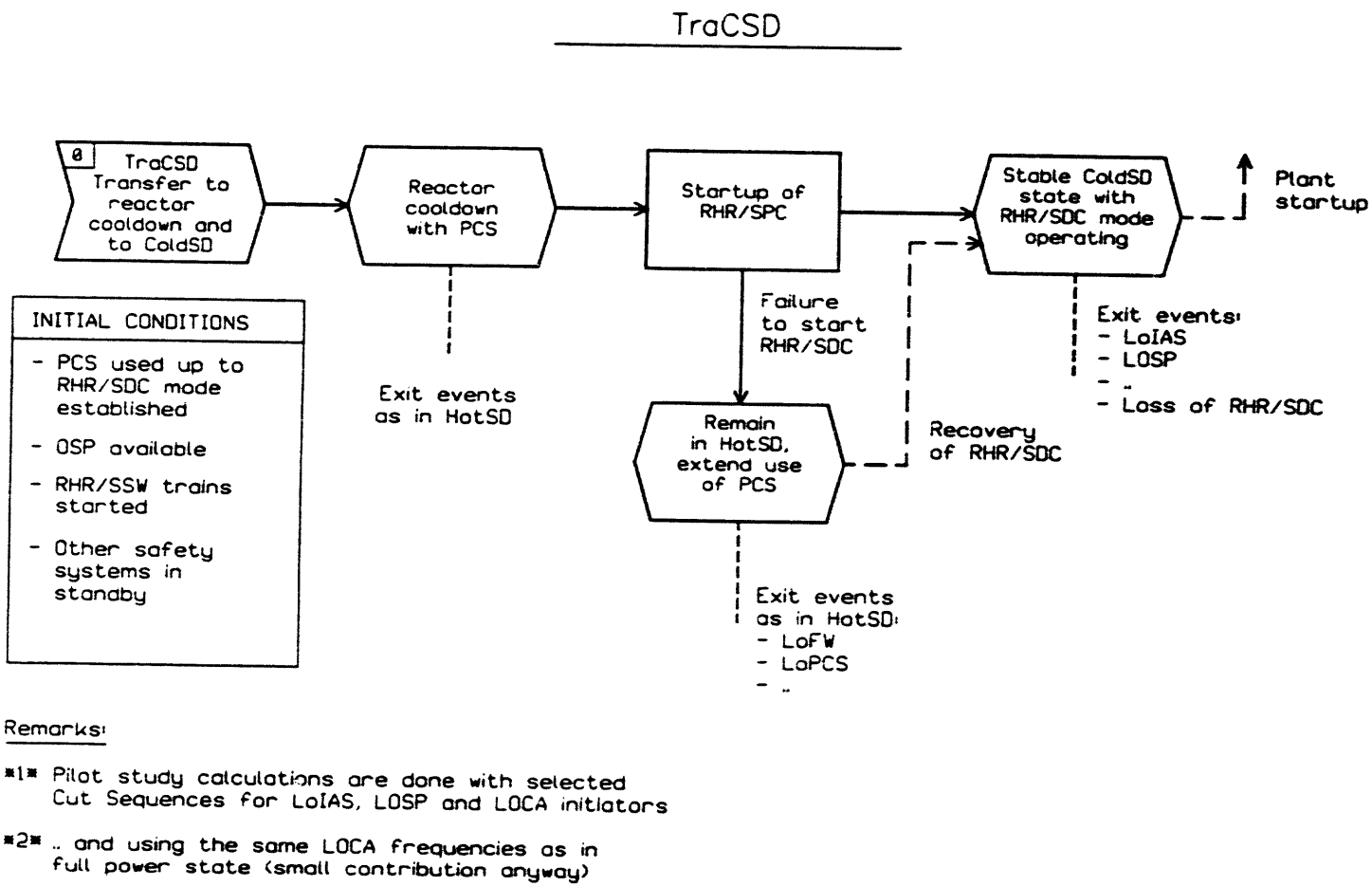


Figure E.7 Extended event sequence diagram (EESD) for transfer to cold shutdown (TraCSD)

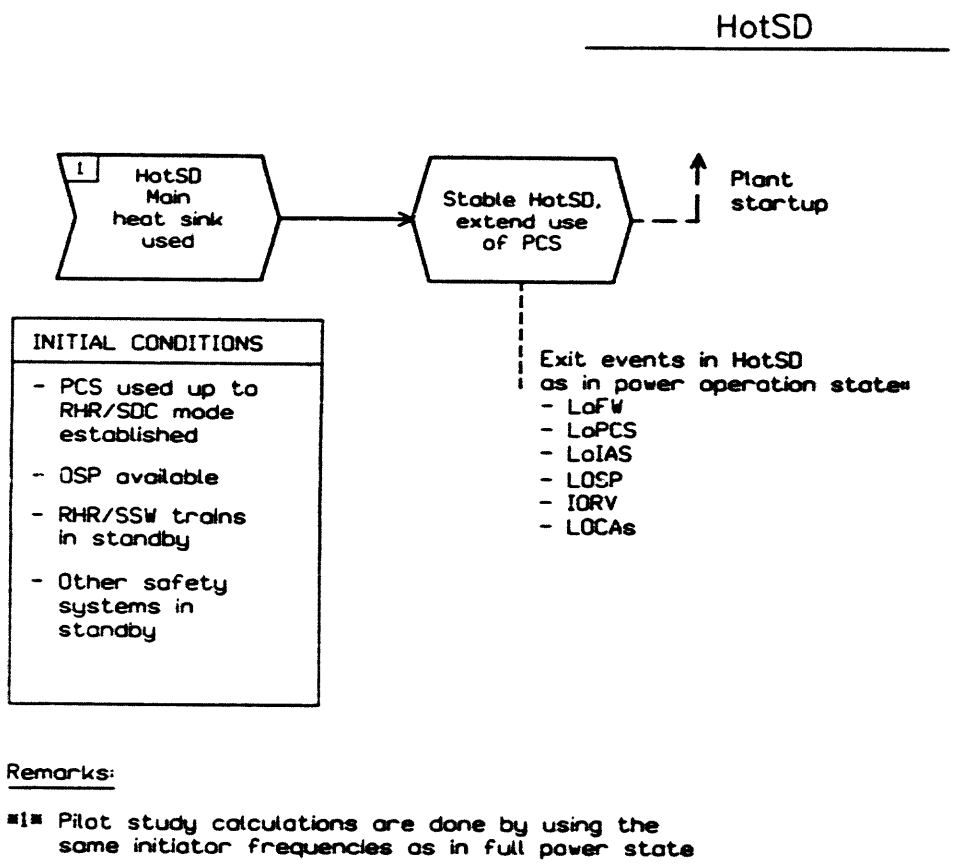
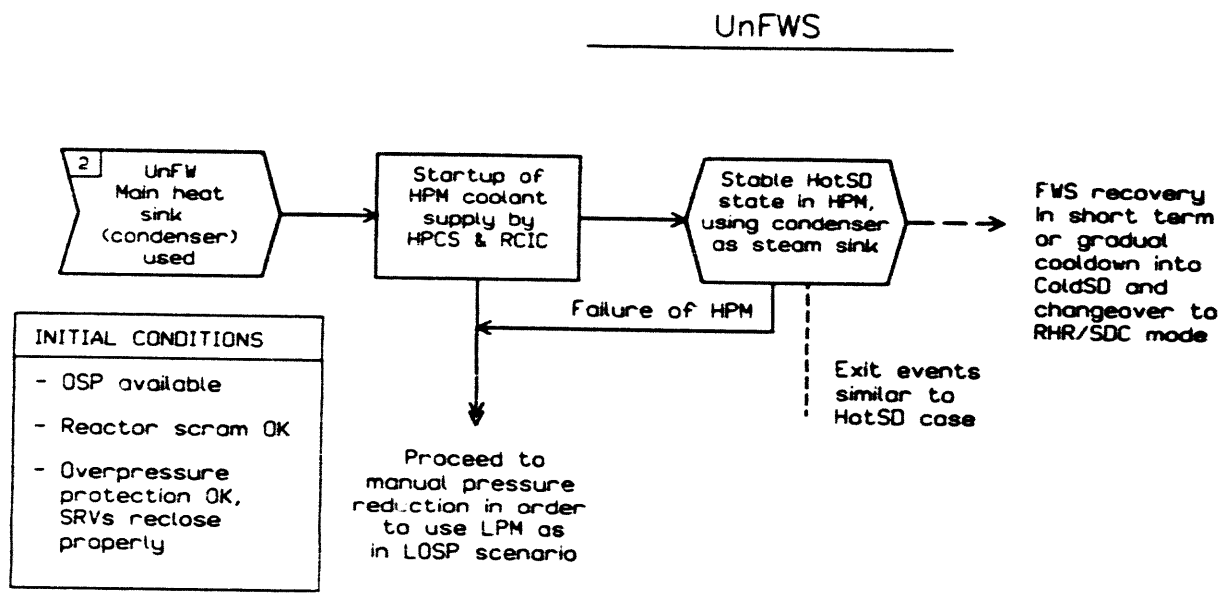


Figure E.8 Extended event sequence diagram (EESD) for hot shutdown (HotSD)



Remarks:

1 Pilot study calculations are done with the same selected Cut Sequences as for LOSP case, with the distinction, that OSP is initially available.

Figure E.9 Extended event sequence diagram (EESD) for loss of feedwater (UnFW)

APPENDIX F

ANALYSIS OF SUPPRESSION POOL HEATUP

LIST OF TABLES

LIST OF FIGURES

This appendix describes heatup scenarios, i.e., classification of plant responses used to consider recovery from Near Mission Failure (NMF) states. Assumptions on the plant behavior are based on the PSA for Grand Gulf.[1] Using the corresponding data of the residual heat removal study for the TVO plant as a starting point,[2] the heatup data were extracted from the work material of the low-power and shutdown PSA for Grand Gulf, scaling the TVO information to the Grand Gulf plant with crude approximations.

F.1 Scenario Approach

F.1.1 Available Time to Recovery

When entering an NMF state, there is a time margin until actualization of an undesired end event, such as core damage in the case of loss of reactor cooling. This time margin for recovery will be called "heatup time". This margin is determined by delaying buffers such as the following:

- heatup of the suppression pool in the case of loss of RHR, but coolant supply and steam relief functions retained
- decrease of reactor water level in the case of loss of coolant supply
- AC/DC supply from station batteries for vital instrumentation in the case of station blackout

In the current version of TeReLCO, recovery from NMF states is handled by arranging process delay behavior cases into principal scenarios. Event sequences are then associated for quantification with the most relevant scenario.[3]

F.1.2 Discretization of Mission Time

The time variable is discretized with logarithmic steps, because the details of time-dependent phenomena are important during the first hours after SD. A maximum mission period is limited to about 10 days. This period is sufficient, because at that time point from an initiating event, it is likely that the plant state has been stabilized, and implications of initial deviations removed.

F.2 Undesired Consequence States

F.2.1 Undesired End Events

In analogy to the RHR study for TVO, the following two undesired end events are considered:

CoreD = Core damage due to prevailing loss of coolant supply and reactor core cooling

CoPRe = Containment pressure relief with venting system due to prevailing loss of RHR function

CoreD is of primary importance, while CoPRe will be considered for additional interest.

F.2.2 Near Mission Failure States

The Near Mission Failure (NMF) state is a state where a critical safety function is lost and an undesired consequence state will occur if no recovery is made. The specific period between an NMF state and an undesired end state corresponds to the available time to recovery, or "heatup time", as discussed above.

The following NMF states are defined:

LoCC = Loss of reactor coolant supply and core cooling endangered

LoRHR = Loss of RHR function, which means that heat transport from the reactor core to an ultimate heat sink is inoperable

LoSPC = Loss of suppression pool (SP) cooling: a subset of LoRHR, which has a central role as the pool water is an important delay buffer

These are listed in the order of descending importance. In some event sequences they may be causally related. In an overlap, the more important NMF state is considered as determining the heatup time for the specific sequence.

F.2.3 System Operability in Heatup States

According to the PSA for Grand Gulf, the following are assumed regarding system operability in heatup states:

- The RCIC and CRD systems will be lost in reactor depressurization as well as at containment venting (i.e. at CoPRe threshold).

- The HPCS, as well as the LPCS and RHR pumps in all modes, can continue operation with increases of temperature in the suppression pool, and also will survive containment venting.

These assumptions are also adopted in our analysis of heatup scenarios.

The operability of the backup coolant supply systems pumping water from the outside basins, such as the SSW cross-tie, condensate system (CDS), and firewater system, are affected only by the RCS pressure. Only the CDS is capable to inject in the high pressure mode.

F.3 Available Time to Recovery in Pool Heatup Cases

Table F.1 defines various scenarios for the heatup of the suppression pool. The steam sink and the systems for maintaining the reactor coolant inventory also are shown in the table.

Figure F.1 depicts the SP temperature behaviors for the heatup scenarios defined in Table F.1, based on the scheme of the corresponding TVO study as adapted to the specific design data of Grand Gulf, explained in more detail below. In the figure, the SP heatup is shown for three example cases. Two of them, IH0 and LH0, are related to LoSPC at time zero for transient and LOCA scenarios, respectively, providing time margins of 9.2 and 7.7 hours before crossing the CoPRe threshold. The third

example, IH1:16, shows a LoSPC situation during shutdown cooling at 16 hours, while in transient scenario IH1, we have a time margin of 10.8 hours before crossing the CoPRc threshold.

The time data for the selected SP heatup scenarios are shown in Table F.2, along with those for the reactor coolant boil-off scenario in the case of loss of reactor coolant supply. These times, based on a simplified heat balance model discussed below, agree qualitatively with those obtained in the TVO study, when operability states of 4,2,0 RHR trains at TVO are compared with operability states of 2,1,0 RHR/SPC trains at Grand Gulf, respectively.

For the calculation of SP temperature and heatup times, a simple heat balance model was constructed, made up of the following entities:

- the decay heat rate as a function of the time from reactor shutdown[3,4]
- the amount and release rate of the latent heat stored in the reactor system, deduced from the temperature difference of about 21°F between no depressurization and depressurization with ADS at about 0.5 hours, in station blackout (SBO) (Figure 2.1 of Reference 4).
- the SP heat capacity based on the assumption of 100 % efficiency of temperature mixing
- the heat transfer rate of RHR/SPC trains, assumed to be a linear function of the temperature difference between the SP and the SSW basin, as determined by the overall heat transfer coefficient and the effective surface of the RHR heat exchangers (page 5.4-66 of Grand Gulf Updated UFSAR[5]).

A nominal SSW basin temperature of 80°F is assumed to be coherent with the assumed nominal SP temperature of 90 °F. The seasonal fluctuations should be considered for more detailed analysis.

The following simplified heat transfer model was used in this study to analyze the SP temperature behaviors:

$$dT_{SP} = dt/C_{SP} \, (P_{DH} + P_{LatH} - P_{RHR})$$

$$P_{RHR} = n_{RHR} \, G_{RHR} \, (T_{SP} - T_{US})$$

$$P_{LatH} = W_{LatH} / a_{CoolDown}$$

where,

T_{SP} = temperature of the suppression pool
T_{US} = temperature of the ultimate heat sink = 80°F (for SSW basin)
G_{RHR} = cooling capacity of one RHR/SPC train = 4.46×10^6 Btu/hr-°F
= 0.73 MW/°C
n_{RHR} = number of the operating RHR/SPC trains
P_{DH} = decay heat rate at the end of the power cycle
P_{LatH} = latent heat release rate
W_{LatH} = latent heat energy = 187 GJ = 177×10^6 BTU
$a_{CoolDown}$ = reactor cooldown time
C_{SP} = heat buffer of suppression pool with 100% mixing = 16 GJ/°C

$\approx 8.42 \times 10^6$ Btu/^{0}F

The reactor cooldown time, which determines the release rate of the latent heat, is assumed to be 4 hours in a controlled shutdown, 24 hours if staying in hot shutdown and 0.5 hours in LOCA scenarios.

F.3.1 Controlled SD

This is the basic scenario of a controlled shutdown from power operation into ColdSD state. It is assumed that PCS is used during reactor cooldown up to the point where the RHR/SDC can be used, i.e., about 135 psig. Thus, the SP temperature is retained at the nominal, about 90°F (i.e., 32°C as compared to 20°C at TVO).

F.3.2 HotSD Scenarios

This class, IH and IC, is associated with the loss of PCS cases with regulated steam-dump to SP. After the initial blowdown, it may be possible to switch over to RHR/SDC and stop the steam-dump to SP. This change to RHR/SDC is assumed to be made at about 4 hours. The IC scenarios are divided into IC1 and IC0, depending upon whether it is possible to continue SP cooling with one RHR train or not, respectively. Prevailing steam dump scenarios are denoted as IHk.

F.3.3 Depressurization Scenarios

This class, LH, is associated with LOCAs, and other situations where ADS is used to allow the use of low pressure injection systems. In contrast to the HotSD scenarios, the latent heat from RCS is rapidly burst into SP, which means a larger increase in SP temperature at the beginning of the scenarios. It is assumed that in these LH scenarios, no switch-over would be made to RHR/SDC in the early hours of the SC mission (compare the LCk and ICk curves in Figure F.1).

F.3.4 Loss of Component/Room Cooling Scenarios

As in the PSA for Grand Gulf, we assumed that the low pressure ECCS pumps fail within four hours after loss of the associated room cooling that results from failure in the emergency ventilation system (EVS.L). The HPCS and RCIC pumps are assumed to fail within twelve hours after loss of room cooling (EVS.H). It is also assumed in this study that these critical times do not depend on the SP temperature or other conditions. The scenarios, EVS, in Table F.2 account for the loss of component/room cooling.

F.3.5 Reactor Coolant Boil-Off Scenarios

This class, FW0, is concerned with the loss of coolant supply to the reactor core, i.e., loss of feedwater (LoFW), resulting in a gradual boil-off and decrease in water level. The level decrease to the top of the core was calculated from the nominal water volume above the core, assuming saturated conditions at LoFW[3,4] (see Table F.2 for the corresponding reactor coolant boil-off times).

REFERENCES

1. M. Drouin, J.L. LaChance, B.J. Shapiro, et al., "Analysis of Core Damage Frequency: Grand Gulf, Unit 1 Internal Events, NUREG/CR-4550, SAND86-2084, Rev. 1, Vol. 6, September 1989.

2. T. Mankamo and M. Kosonen, "Continued Plant Operation Versus Shutdown in Failure Situations of Standby Safety Systems," IAEA/TechSpec Pilot Study Program, NKS/SIK-1(91)4, August 1991.

3. "Thermodynamics Calculations for Grand Gulf," Work Material, SEA, May 1991.

4. "GGNS Station Blackout Analysis," MS194/SERISB01, March 1989, pp 7-9.

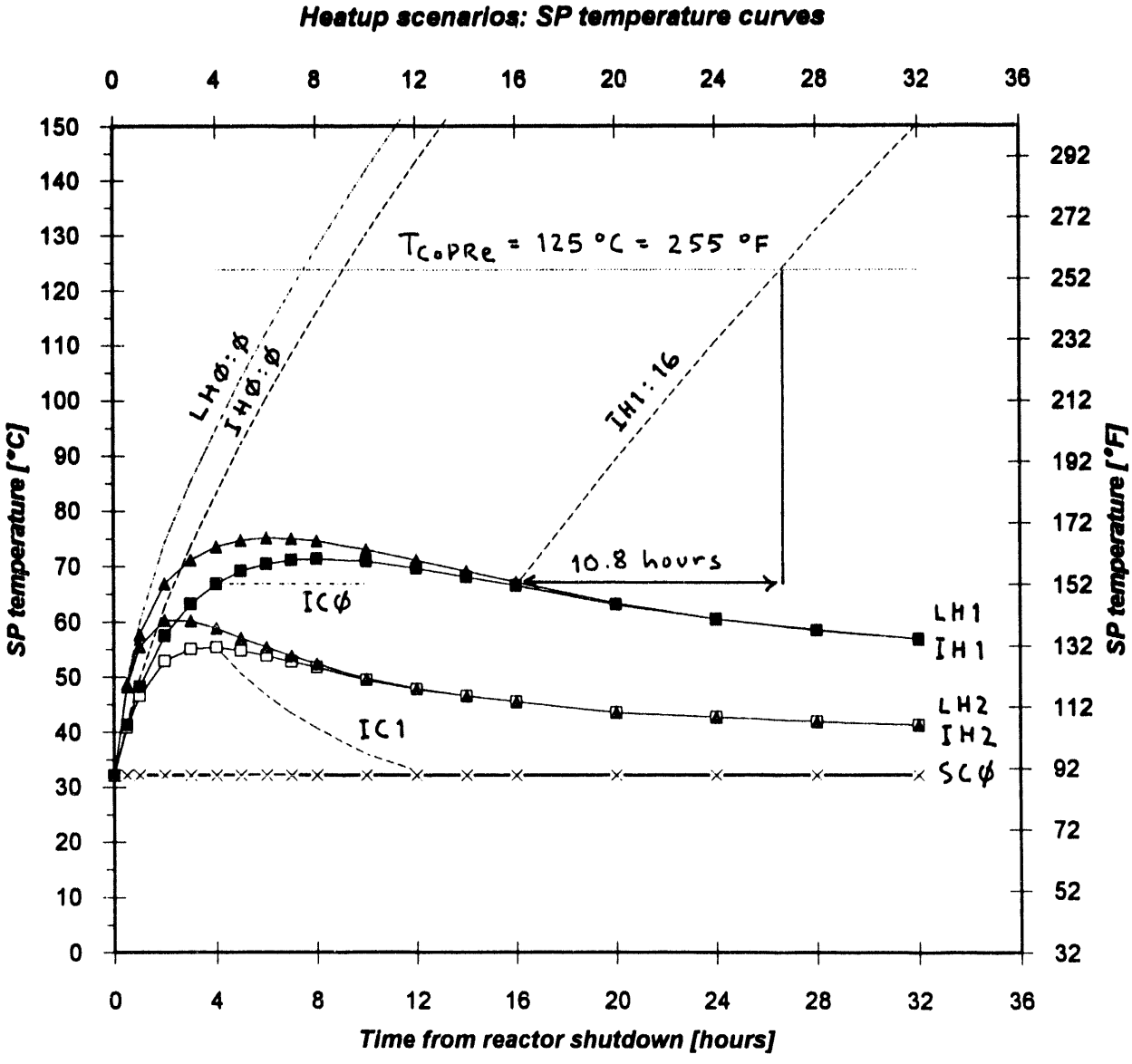
5. "Grand Gulf Nuclear Station Units 1 and 2 (GGNS) Updated Final Safety Analysis Report (UFSAR), Revision 2," Section 5.4.7.1.1.3 Suppression Pool Cooling Mode, December 1987, pp 5.4-66.

Table F.1 Scenario Classes for the Heatup Cases of the Suppression Pool

Scenario class		Steam sink	Reactor coolant inventory control
S	Smooth cooldown: successful transfer into ColdSD state	Turbine condenser used up to changeover to RHR/SDC	FWS during cooldown then RHR/SDC recirculation
I	Initial, regulated steam blowdown into SP	SP, PCS isolated, RCS pressurized	High pressure injection systems RCIC HPCS FWS CRD
IH	Prevailing regulated steam dump to SP		As above
IC	Changeover to RHR/SDC after initial blowdown		RHR/SDC recirculation
L	Automatic/manual, rapid depressurization or LOCA	SP, PCS isolated, RCS nonpressurized	Low pressure injection systems LPCS LPCI SSW cross-tie Condensate system Firewater system
LH	Prevailing steam release to SP		As above
LC	Changeover to RHR/SDC after initial blowdown		RHR/SDC recirculation

Table F.2 Time Data for Heatup Scenarios Based on a Simple Heat Transfer Model

Time step	0	1	2	3	4	5	6	7	8	9
Time from reactor shutdown [hours]	0	2	3	4	8	16	32	64	128	256
Scenarios	Heatup time from entering NMF state until critical core condition [hours]									
Pool heatup scenarios										
Smooth SD: successful transfer to ColdSD										
1 SC0.0	9.2	11.9	12.7	13.2	15.3	17.6	21.3	26.4	32.5	39.7
Initial, regulated BD										
2 IH2.0	9.2	8.6	8.9	9.5	11.7	15.1	19.0	23.5	31.0	39.2
3 IH1.0	9.2	7.9	7.7	7.7	8.0	10.8	15.4	20.7	30.6	38.9
4 IC1.0	9.2	8.6	8.9	9.5	13.6	17.4	21.1	26.2	32.2	39.7
5 IC0.0	9.2	7.9	7.7	7.7	8.8	10.7	12.9	15.1	20.6	33.9
Initial, rapid BD										
6 LH2.0	7.7	7.6	8.2	8.9	11.5	15.1	19.0	23.9	31.5	39.5
7 LH1.0	7.7	6.6	6.6	6.6	7.7	10.6	15.4	20.7	30.6	38.9
Loss of room/component cooling										
8 EVS.H	12.0	12.0	12.0	12.0	12.0	12.0	12.0	12.0	12.0	12.0
9 EVS.L	4.0	4.0	4.0	4.0	4.0	4.0	4.0	4.0	4.0	4.0
Reactor coolant boil-off scenarios										
Loss of reactor coolant supply										
10 FW0.0	0.7	1.5	1.7	1.9	2.2	2.8	3.5	4.4	5.8	7.7



ASk	Coding	
k	= Number of operating RHR/SPC trains	
S	= Reactor shutdown mode:	H = HotSD C = ColdSD
A	= SC initiation state:	S = Smooth (successful transfer to ColdSD mode) I = Initial regulated steam relief to SP L = LOCA, ADS (rapid steam relief to SP)

Figure F.1 Behaviors of the suppression pool temperature for various heatup scenarios

APPENDIX G

EXAMPLE QUANTIFICATION

LIST OF TABLES

LIST OF FIGURES

This appendix exemplifies the quantification of LCO risks for two basic operational alternatives, i.e., plant shutdown and continued operation, in a failure situation of SSW trains A and B. LOSP (loss of offsite power) sequences are used for this example quantification because of their dominant contribution to the plant risk.

G.1. Definition of the Example Case

The example quantification considers LOSP sequences starting at power operation state or during power reduction stage, when a controlled shutdown is going on. These are handled in this study on an equal basis as the same Initiating event of Shutdown Cooling mission (ISC=5, see Figure 4.2 in Chapter 4). Entering SC mission via LOSP (ISC=5) occurs in SD and CO alternatives with the following likelihood or frequency (Appendix D):

$P_{LOSP|SD}$ = 10^{-4}/controlled shutdown
$f_{LOSP|CO}$ = 0.07/yr (in power operation state)

Our primary interest is the exemplification of the SD risk evaluation, but in parallel, the CO alternative also will be considered.

The failure of SSW Trains A and B is chosen as the example situation, because this failure situation is perhaps the most interesting from the AOT point of view. The SSW trains are important support systems, especially serving jacket cooling of DGs. Their failure state in case of LOSP implies wide functional consequences, as will be discussed in Section G.1.2.

G.1.1. Initial Conditions

In accordance with the analysis boundary conditions in connection with the LOSP initiator:

- reactor scram is assumed successful
- overpressure protection is assumed to operate, and all SRVs reclose properly after initial steam relief
- regulated steam relief to the suppression pool (SP) is assumed to operate over the whole SC mission

The failure branches of these functions after the LOSP initiator are not considered because they are relatively small contributions, and affect little the SD/CO risk comparison results for the LCO situations (Appendix D).

The failure situation SSW.AB (SSW Trains A and B) has been detected just before the LOSP initiator. This assumption has a specific influence on the predicted repair time and its distribution for the initial failure.

G.1.2. Function Implications

LOSP means loss of PCS, and in conjunction with the SSW.AB failure situation, there will be the following functional implications:

- DG.A and DG.B are inoperable because of the lack of jacket cooling which should be served by SSW Trains A and B; the dedicated DG.C is however not affected, and if successfully started, it will supply power to HPCS

- All RHR modes, i.e., RHR/SDC, RHR/SPC, and RHR/CS, are inoperable because AC buses A and B are lost, and also because heat removal path via SSW Trains A and B is not available

- Low pressure coolant supply mode (LPM) is severely impacted, because

  -- LPCS and LPCI lack power supply (connected to AC buses A and B)

  -- SSW.B-X crosstie is inoperable due to SSW Train A failure

  -- CDS is inoperable because of LOSP

The other, last-resort LPM paths are not credited in this study (Appendix E).

- High pressure coolant supply mode (HPM) is less affected, because

  -- HPCS receives dedicated diesel power from DG.C and component cooling from SSW Train C

  -- RCIC will be lost at containment venting (CoPRe) because heat cannot be removed from SP and containment, if recovery of RHR is not successful before that time point; RCIC lacks also component cooling because SSW Train A is failed, but this is assumed to be critical only after 12 hours, which is longer than the time to containment venting in the first, more critical part of SC mission period

  -- CRD pumps are inoperable because they are connected to AC buses A and B

Because of so many systems are functionally unavailable, the success paths are strongly reduced, as will be discussed in the following section.

G.2. Success and Failure Paths

Taking into account the functional implications of the SSW.AB failure situation, only the following success paths remain:

- use of HPM coolant supply with HPCS and/or RCIC (both will start automatically in LOSP)

- release of steam to SP, which will gradually heat up, and use of containment venting in the later stage of containment pressurization, if recovery of RHR is not successful before the SP temperature reaches 255 °F (this takes about 9.2 hours, see Appendix F).

Consequently, the following functional failure paths exist, resulting in direct loss of core cooling (LoCC) situation:

- failure to start HPM (HPCS and RCIC system functions)
- failure of HPM during SC mission period
- delayed LoCC at containment venting, if HPCS is inoperable at that time point (RCIC will be lost due to loss of suction head at containment venting)

The corresponding minimal cut sets (MCSs) are presented in Table G.1. Note that offsite power is initially lost, i.e., OSP=1.

In addition, HPM may be lost because of loss of component cooling. RCIC lacks initially component cooling, because SSW.A is failed. Thus, RCIC would be lost at 12 hours because of component heatup. Cooling of HPCS is served by SSW Train C, and is initially intact. Table G.1 also presents the heatup scenarios for the event sequences (refer to Appendix F).

G.3. Quantification of Sequences

Table G.2 shows the most essential steps of the quantification process for SC phased-mission probability entities and SD/CO risk measures. The variables for cut sequences in the last column of this table are of the following meaning:

pch(s)	=	Probability of failure to enter SC mission at the initial challenge for a given sequence, s
fsc(s; a)	=	Failure frequency during the SC mission for a given sequence, s, as the function of time, a, elapsed from the beginning of mission
a	=	Time variable from the beginning of the SC mission
psc(s)	=	Expected failure probability during the SC mission (integrated with respect to recovery from the initial repair state)
pmp(s)	=	Total, expected failure probability over the SC mission phase for a given sequence, s

The variables for initiators, denoted with index i, have the same meaning as the variables for cut sequences, denoted with index s.

Tables G.3 and G.4 show the major steps to quantify the SC mission failure probabilities. Table G.3 indicates how the probabilities of failure to enter SC mission can be calculated for the failure situation under consideration, i.e., LOSP initiator occurs just after SSW trains A and B are detected failed. Table G.4 indicates how the failure rates during SC mission period can be estimated for the same failure situation.

The probability of failure to enter SC mission at the initial challenge, and the failure rate during, SC mission period are calculated for a given cut sequence, s, as follows:

$$pch(s) = \prod_{X \in SBQ(s)} una_X(0).pnr_{ch}(s;0)$$

$$fsc(s;a) = \sum_{X \in SBQ(s)} fra_X(a). \prod_{Y \in SBQ(s), Y \neq X} una_Y(a).pnr_{fo.X}(s;a)$$

where

$una_X(a)$	=	Projected unavailability of system module, X, at time point, a
$fra_X(a)$	=	Failure rate (loss of operation during SC mission) of system module, X, at time point, a
$pnr_{ch}(s; 0)$	=	Probability of nonrecovery from NMF, when entered at the beginning of SC mission due to cut sequence, s
$pnr_{fo.X}(s; a)$	=	Probability fo nonrecovery from NMF, when entered during SC mission due to cut sequence, s, and system module, X, failing to operate at time point, a

The derivation of the probability of nonrecovery from the NMF state is illustrated in Figure G.1 for the dominant sequence, OSP*DGC*RCI. The SRCF (shortest repair class first) model is used in this study, assuming that repair efforts in multiple failure situations are prioritized starting from the component whose expected recovery time is assessed shortest. For comparison, the distribution for independent parallel repair (traditional, very optimistic assumption) is also shown in the figure.

G.4. Construction of Risk Frequency Diagram

The quantification results are summarized in Table G.5, and presented graphically in Figure G.2.

G.4.1. Probability Entities for SC Mission

The entities related to the initial repair state, SSW.AB, are the following:

prs(a)	=	Complementary distribution of the repair time for the initial failure state (until the completion of first repair)
a_rec	=	Mean time to repair for the initial failure state (time to first repair)

The variables describing the contribution of a given cut sequence or a whole sequence group for a given initiator over SC mission are the following (Part I of Table G.5):

a_scp	=	Time variable from the beginning of the SC mission
pch	=	Probability of failure to enter the SC mission
fsc(a)	=	Failure frequency during the SC mission
psc	=	Expected failure probability during the SC mission (integrated with respect to the probability distribution for first repair of the initial failure state)

$$= \int_{a\_scp=0}^{\infty} da\_scp \cdot fsc(a\_scp) \cdot prs(a\_scp)$$

pmp = Total, expected failure probability over the SC mission
= pch + psc

G.4.2. Risk of SD Alternative

For SD alternative, the corresponding risk variables, rsd and fsd, for the failure to enter SC mission and failure frequency during mission time (used in Part II of Table G.5 and to obtain the risk curves in Figure G.2), are obtained by summing up the SC mission entities for all initiators, i, and then multiplying by the initiator likelihood:

$$R_{SD.ch} = rsd\_ch = \sum_i P_{i|SD} \cdot pch(i)$$

$$f_{SD.sc}(a) = fsd = \sum_i P_{i|SD} \cdot fsc(i; a)$$

In the risk frequency presentation, the risk mass of $R_{SD.ch}$ is presented by a triangle peak superposed over $f_{SD.sc}$ as explained in reference 1. The cumulative risk over predicted repair time, r, is obtained from:

$$C_{SD}(r) = R_{SD.ch} + \int_{a=0}^{r} da \cdot f_{SD.sc}(a)$$

The expected risk per failure situation can be assessed from:

$$R_{SD} = R_{SD.ch} + \int_{a=0}^{\infty} da \cdot f_{SD.sc}(a) \cdot prs(a)$$

The value of R_{SD} is assessed to be 9.63E-7 for the example failure situation, as shown in Table G.5. The contribution of LOSP initiator is 4.16E-7, i.e., about half of R_{SD}.

G.4.3. Risk of CO Alternative

The risk frequency for CO alternative is obtained from:

$$f_{CO} = \sum_i f_{i|CO} \cdot pmp(i)$$

The cumulative risk over predicted repair time, r, and expected risk per failure situation are obtained from:

$C_{CO}(r) = f_{CO} \cdot r$
$R_{CO} = f_{CO} \cdot a\_rec$

Figure G.2 also shows the risk frequency and the cumulative risk over predicted repair time for all initiators so that they can be compared with the corresponding contributions from the LOSP sequences under consideration.

REFERENCES

1. T. Mankamo and M. Kosonen, "Continued Plant Operation Versus Shutdown in Failure Situations of Standby Safety Systems," IAEA/TechSpec Pilot Study Program, NKS/SIK-1(91)4, August 1991.

Table G.1 Minimal Cut Sets for the Example Case with Heatup Scenarios

Sequence category	MCS	Heatup scenario
Direct LoCC	OSP *DGC *RCI OSP *HCS *RCI OSP *SSW.C *RCI	FW0
Delayed LoCC at CoPRe due to loss of RCIC at containment venting	OSP *DGC OSP *HCS OSP *SSW.C	IC0
Loss of component/room cooling sequences	OSP *SSW.C	EVS.H

System modules:

SSW.C	SSW Train C, common elements of the train
DGC	Diesel generator C with auxiliaries, dedicated Div. 3
HCS	High pressure core spray system
RCI	Reactor core isolation cooling system
OSP	Offsite power supply

Table G.2 Main Steps in the Quantification Process for Phased-Mission Probability Entities and SD/CO Risk Measures

Input	Quantification step	
Cut sequence presentations: MCSs and heatup scenarios; system module data	For each Cut Sequence (s): evaluate the probability entities of the SC mission failure	$pch(s) = \ldots$ $fsc(s; a) = \ldots$ $psc(s) = \int_{a=0}^{\infty} da.fsc(s; a).prs(a)$ $pmp(s) = pch(s) + psc(s)$
	Sum up Cut Sequences over the Sequence Group SGR(i) for each initiator (i)	$pch(i) = \sum_{s \in SGR(i)} pch(s)$ $fsc(i; a) = \sum_{s \in SGR(i)} fsc(s; a)$ $pmp(i) = \sum_{s \in SGR(i)} pmp(s)$
Data for ISCs: link to STDs	Construct risk frequency presentations for the SD and CO alternatives	$R_{SD.ch} = \sum_i P_{i\|SD} . pch(i)$ $f_{SD}(a) = \sum_i P_{i\|SD} . fsc(i; a)$ $f_{CO} = \sum_i f_{i\|CO} . pmp(i)$

Table G.3 Quantification of Probabilities of Failure to Enter Shutdown Cooling Mission for the Example Failure Situation (Occurrence of LOSP Just After SSW Trains A and B are Detected Failed)

Cut sequence Projected unavailability of sequence elements			Recovery data Scenario pnr	 a_hup	Sequence contribution pch
Direct LoCC					
OSP	*DGC	*RCI	FW0	0.7 hours	
1	3.80E-2	5.40E-2	0.583		1.20E-3
OSP	*HCS	*RCI	FW0	0.7 hours	
1	1.70E-2	5.40E-2	0.583		5.36E-4
OSP	*SSW.C	*RCI	FW0	0.7 hours	
1	9.30E-3	5.40E-2	0.583		2.93E-4
Delayed LoCC at CoPRe due to loss of RCIC at containment venting					
OSP	*DGC		IC0	9.2 hours	
1	3.80E-2		0.0283		1.08E-3
OSP	*HCS		IC0	9.2 hours	
1	1.70E-2		Screened out in the pilot phase calculations		
OSP	*SSW.C		IC0	9.2 hours	
1	9.30E-3		0.0291		2.71E-4
Loss of component/room cooling sequences					
OSP	*SSW.C		EVS.H	12 hours	
1	9.30E-3		0.0156		1.45E-4
In total				pch(LOSP) =	3.52E-3

Table G.4 Quantification of Failure Rates During Shutdown Cooling Mission for the Example Failure Situation (Occurrence of LOSP Just After SSW Trains A and B are Detected Failed)

Cut sequence =		OSP*DGC*RCI		Recovery data		Sequence contribution
Time	Transition to NMF	Projected unavailability of the		Scenario	a_hup	
a_scp	Rate	other sequence elements		pnr		fsc
	DGC	*OSP	*RCI	FW0	2.2 hours	
8 hours	2.00E-3 /hour	5.74E-2	5.77E-2	0.603		3.99E-6 /hour
	RCI	*OSP	*DGC	FW0	2.2 hours	
8 hours	5.00E-3 /hour	5.74E-2	2.42E-2	0.618		4.29E-6 /hour
8 hours	In total			fsc(LOSP; 8 hours) =		8.29E-6 /hour
					=	7.26E-2 /year

Table G.5 Conditional Failure Probability/Rate Entities and Risk Contributions for LOSP Sequences When SSW Trains A and B are Failed

I. Conditional probability/rate entities for LOSP sequences

	Dominant *DGC*RCI	All LOSP seq.	Probability of repair state prs(a_scp)
pch	1.20E-3	3.52E-3	
fsc [1/hour]			
a_scp = 0	1.74E-4	3.10E-4	1
2	3.69E-5	1.06E-4	0.727
3	2.53E-5	8.27E-5	0.629
4	1.87E-5	6.59E-5	0.550
8	8.29E-6	2.80E-5	0.352
16	2.34E-6	6.88E-6	0.195
32	2.91E-7	7.01E-7	0.0856
64	1.16E-8	2.57E-8	0.0203
128	5.71E-9	1.01E-8	2.90E-3
256	4.35E-9	5.33E-9	6.26E-4
psc	2.80E-4	6.48E-4	a_rec [hours]
pmp	1.48E-3	4.16E-3	12.1

II. Risk contribution for LOSP sequences

	Dominant *DGC*RCI	All LOSP seq.	All initiators
rsd_ch	1.20E-7	3.52E-7	5.74E-7
fsd [1/hour]			
a_scp = 0	1.74E-8	3.10E-8	8.25E-8
2	3.69E-9	1.06E-8	4.61E-8
3	2.53E-9	8.27E-9	4.10E-8
4	1.87E-9	6.59E-9	3.75E-8
8	8.29E-10	2.80E-9	3.01E-8
16	2.34E-10	6.88E-10	2.37E-8
32	2.91E-11	7.01E-11	1.84E-8
64	1.16E-12	2.57E-12	1.46E-8
128	5.71E-13	1.01E-12	1.20E-8
256	4.35E-13	5.33E-13	1.04E-8
rsd_sc	2.80E-8	6.48E-8	3.89E-7
rsd	1.48E-7	4.16E-7	9.63E-7

Fractions of repair time classes zr

kc	rtc	SSW^2	OSP	DGC	RCI	Sequence
1	1		0.75			0.75
2	2					0
3	4	0.598	0.15	0.64	0.3	0.2398696
4	8		0.1			0.0101304
5	20	0.39392			0.6	0
6	40			0.34		0
7	100	0.00808		0.02	0.1	0
	hours					

Repair time distributions - probability of nonrecovery pnr

ka	apr	SSW^2	OSP	DGC	RCI	*Shortest repair class first* Seq|SRCF	*Model of independent repairs* Seq|IndR
0	0	1	1	1	1	1	1
+	0.7	0.890	0.590	0.891	0.931	0.583	0.2540
1	2	0.727	0.270	0.731	0.823	0.255	0.0301
2	3	0.629	0.177	0.637	0.755	0.158	8.44E-3
3	4	0.550	0.130	0.562	0.698	0.108	3.02E-3
4	8	0.352	0.0573	0.383	0.535	0.0364	1.51E-4
+	9.2	0.316	0.0468	0.353	0.500	0.0273	7.12E-5
+	12	0.253	0.0298	0.301	0.433	0.0142	1.40E-5
5	32	0.0856	1.88E-3	0.168	0.194	2.66E-4	1.39E-9
6	64	2.03E-2	3.36E-5	7.92E-2	7.72E-2	3.43E-6	1.43E-14
	hours						

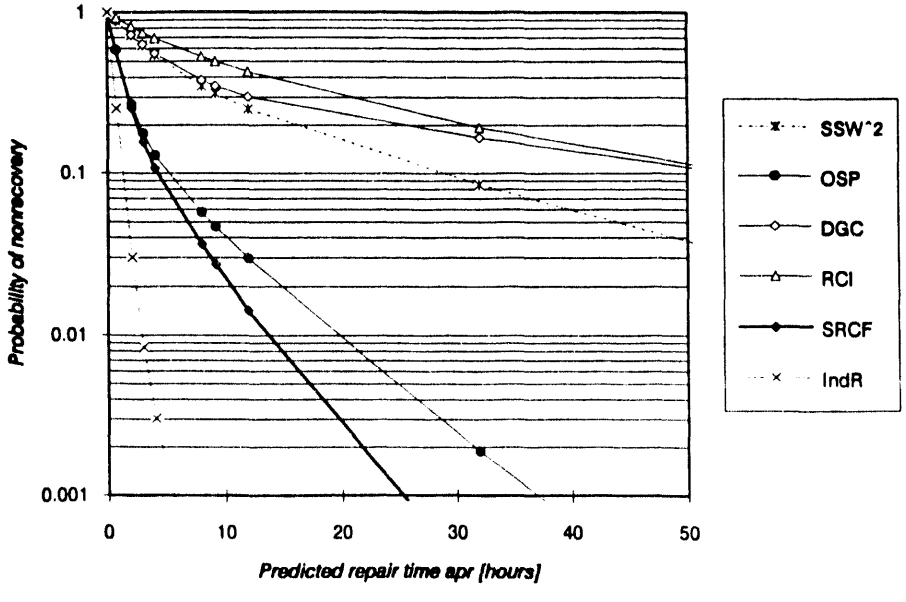


Figure G.1 Repair-time distribution for the elements in the dominant sequence of OSP*DGS*RCI in the example failure situation and the probability distribution for nonrecovery from the Near Mission Failure state based on the SRCF (shortest repair class first) model

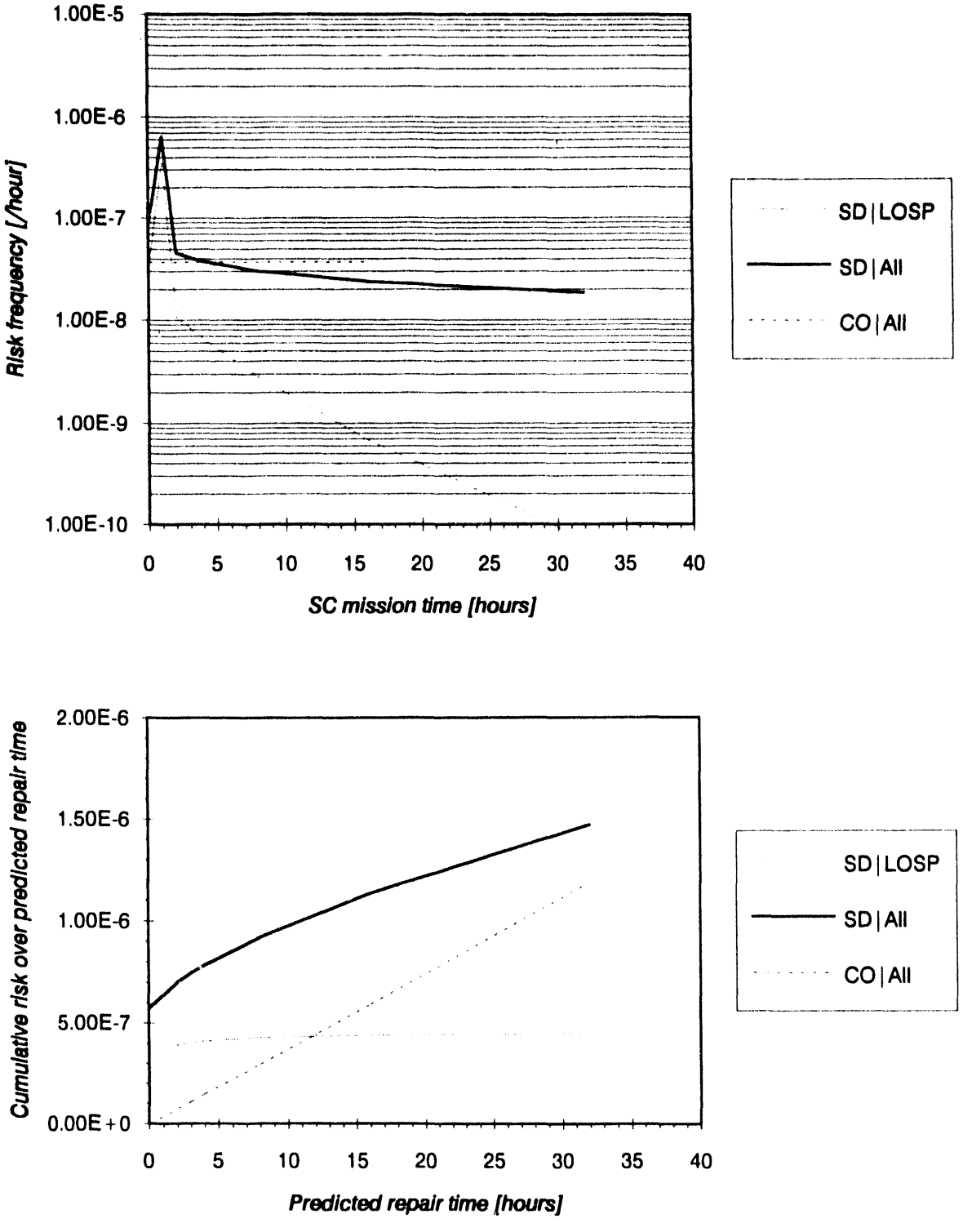


Figure G.2 Risk Frequency and Cumulative Risk over Predicted Repair Time for the LOSP Scenario in Failure of SSW Trains A and B with the Corresponding Risk Measures for All Initiators for Comparison

DATE
FILMED
1/12/94
END