ornl

OAK
RIDGE
NATIONAL
LABORATORY

UNION
CARBIDE

NUREG/CR-2678
ORNL/TM-8314

Flood Risk Analysis Methodology Development Project Final Report

D. P. Wagner
M. L. Casada
J. B. Fussell

Prepared for the U.S. Nuclear Regulatory Commission
Office of Nuclear Regulatory Research
Under Interagency Agreement DOE 40-550-75

OPERATED BY
UNION CARBIDE CORPORATION
FOR THE UNITED STATES
DEPARTMENT OF ENERGY

Printed in the United States of America. Available from
National Technical Information Service
U.S. Department of Commerce
5285 Port Royal Road, Springfield, Virginia 22161

Available from
GPO Sales Program
Division of Technical Information and Document Control
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555

NUREG/CR-2678
ORNL/TM-8314
Distribution Category RG

Contract No. W-7405-eng-26

Engineering Physics Division

FLOOD RISK ANALYSIS METHODOLOGY DEVELOPMENT PROJECT
FINAL REPORT

D. P. Wagner*
M. L. Casada*
J. B. Fussell*

NRC Monitor: P. K. Niyogi
Risk Methodology & Data Branch
Division of Risk Analysis

Manuscript Completed: December, 1981

Date Published: June 1982

This Work Performed For
Nuclear Regulatory Commission
Under
DOE Interagency Agreement 40-550-75
NRC FIN No. B0436

Work Performed Under
ORNL Subcontract No. 85B-13860C

*JBF Associates, Inc.
1630 Downtown West Boulevard
Suite 108
Knoxville, Tennessee 37919

OAK RIDGE NATIONAL LABORATORY
Oak Ridge, Tennessee 37830
operated by
UNION CARBIDE CORPORATION
for the
DEPARTMENT OF ENERGY

ACKNOWLEDGMENTS

We gratefully acknowledge the support given to this project by the Division of Risk Analysis, U. S. Nuclear Regulatory Commission. Dr. W. E. Vesely and Mr. S. R. Sturges deserve special thanks for their assistance throughout this two-year effort. Sincere thanks is given to Dr. G. F. Flanagan of the Oak Ridge National Laboratory for his support and advice. We also wish to thank the personnel at the Surry Power Station for their cooperation and assistance during our plant visit.

We also appreciate the contributions of Mr. Jim Rooney and Mr. Ben Ellison of JBF Associates, Inc. for their assistance in various phases of the work. Special thanks are given to Ms. Beth Davenport, Ms. Karen Rogers and Mr. Scott Johnston for their skill and patience in preparing the final document.

PREFACE

This report is the final documentation of a two-year effort to develop a methodology for assessing the impact of floods on nuclear power plant risk. Determining the flooding level versus probability at a particular plant site is beyond the scope of this work; however, these are treated in a separate study being carried out at the Idaho National Engineering Laboratory for the Nuclear Regulatory Commission.

The methodology presented in this document is consistent with conventional fault tree/event tree risk assessment techniques and is intended for application as a part of an overall probabilistic risk assessment (PRA). The methodology also satisfies many of the requirements for flood analysis identified in the Nuclear Regulatory Commission's recent Draft PRA Procedures Guide (NUREG/CR-2300).

The project also resulted in two computer programs that aid in portions of the flood analysis. These computer programs represent a major effort of the project and are fully described in a separate document that is the user's manual for both computer programs. These computer programs are used extensively in the example applications discussed in the appendices of this report.

We expect that work in the area of flood risk analysis will continue as the application of PRA techniques expands. This will result in further refinements and extensions to the methodology presented herein as application experience grows. In its present form, the methodology retains substantial flexibility so that future extensions will not alter the basic concepts of the methodology.

This report assumes the reader is familiar with fault tree/event tree terminology and conventional probabilistic risk assessment techniques.

ABSTRACT

This document presents the concepts and methodology necessary to perform flood risk analysis for nuclear power plants, once the flooding level versus probability is known. The methodology is consistent with accepted probabilistic risk assessment (PRA) techniques and is usable either during the normal course of a PRA or as an "add on" analysis for an existing PRA. The methodology fulfills many of the requirements for flood analysis suggested by the Nuclear Regulatory Commission's recent PRA Procedures Guide (NUREG/CR-2300).

The basic inputs to the methodology are:

- accident sequences and their consequence categories,
- fault trees for the events that comprise the accident sequences,
- occurrence probabilities for the accident sequences and the events that comprise the accident sequences,
- basic event failure data,
- basic event vulnerability elevations for flood events, and
- flood occurrence probabilities.

The flood analysis procedure allows screening of the accident sequences to determine the accident sequences that are potentially significant contributors to risk due to flooded effects. A qualitative flood simulation identifies flooded minimal cut sets and critical flood levels for system failures using the system fault trees. The quantitative analysis uses these results to calculate the flood's contribution to:

- system failure probability,
- accident sequence occurrence frequency, and
- consequence category occurrence frequency.

The Appendices to this report describe two example applications of the flood risk methodology to systems of the Surry Power Station, the pressurized water reactor (PWR) used in the Reactor Safety Study (WASH-1400). The first application considers an external flooding scenario and the second application considers an internally generated flood. The results include the contributions of these floods to the Reactor Safety Study results as a function of flood probability.

Additional results of the project are two computer programs that aid in the accident sequence screening and qualitative flood simulation segments of the flood risk analysis. These programs are described in a separate report.

TABLE OF CONTENTS

TABLE OF CONTENTS (Continued)

Section **Page**

LIST OF TABLES

LIST OF FIGURES

LIST OF FIGURES (Continued)

LIST OF FIGURES (Continued)

FLOOD RISK ANALYSIS

METHODOLOGY DEVELOPMENT PROJECT

FINAL REPORT

1. INTRODUCTION

This document is the final report of the Flood Risk Analysis Methodology Development Project. The project is directed toward development of a methodology for analyzing the effects of floods on nuclear power plant systems.

The Reactor Safety Study(1) and the Lewis Committee Report(2) identify floods as external hazards that warrant further investigation in assessing the risk associated with nuclear power plants. The importance of floods results from their potential to produce multiple component failures by submerging individual components. These multiple component failures are called common cause failures(3). These component failures can result in system failures which contribute to the overall risk from nuclear power plants. Thus, consideration of common cause failures due to floods is an important aspect of the overall risk assessment of nuclear power plants.

1.1 Purpose and Scope of the Project

The purpose of this project is to develop a formal basis for assessing the impact of floods on nuclear power plant systems. No attempt is made to identify the source of the flood or the probability associated with the occurrence of the flood. The project considers only the effects of a specified flood on the plant. The methodology identifies system components which are failed (or degraded) by a flood and describes the impact of these component failures on the system failure probability. The methodology is demonstrated by application to existing nuclear reactor systems.

1.2 Project Organization

The Flood Risk Analysis Methodology Development Project was performed in three phases. These three phases were defined to enhance management and control of the project and to assure effective performance throughout the project.

Phase 1 tasks included defining the scope and requirements for Phase 2 of the work. In addition to specifying the required inputs and scope of the computer-aided methodology, an illustrative example problem was defined. Specific information and input data for the example problem were collected, categorized and stored. Phase 1 also included preliminary computer program development. Phase 1 was completed in February 1980.

Phase 2 of the project encompassed development and implementation of the methodology and performance of the example problem analysis and evaluation. The first version of a computer program, called NOAH, was used to implement the flood risk analysis methodology and to perform the example problem analysis. The analysis results were evaluated and areas needing further development and study were identified. Phase 2 was completed in September 1980.

The purpose of Phase 3 of the project was to continue development and application of the methodology and the NOAH computer program, and to perform an additional application of the flood risk methodology. This additional application experience and the resulting modifications to the NOAH computer program resulted in an analysis tool that is directly useful in the licensing of nuclear power plants. Phase 3 was completed in December 1981.

1.3 Objectives of the Project

The overall objective of the Flood Risk Methodology Development Project is to develop a methodology for assessing the impact of floods on nuclear power plant risk. Specific objectives include:

- provide the capability to screen accident sequences to determine those sequences that are potentially significant contributors to risk due to floods,
- provide the capability for detailed flood effects analysis for individual nuclear power plant safety systems,
- provide methods for quantifying flood effects on safety system failure probability and plant risk, and

- demonstrate the methodology by application to existing reactor systems.

In addition, the methodology is structured so that it can be applied as an add-on analysis to existing risk assessments or be included from the beginning of a risk assessment effort. The remaining sections of this document describe the flood risk analysis methodology that is the result of accomplishing these objectives.

1.4 Organization of this Report

Section 2 presents the concepts and definitions of the flood risk analysis methodology. Section 3 describes the flood screening analysis procedures. System qualitative flood risk analysis and the NOAH computer program are discussed in Section 4. System failure and accident sequence quantification is the subject of Section 5. Section 6 discusses the limitations of the methodology. A review of the two example applications of the methodology is presented in Section 7. Appendices A through E contain detailed discussions of the two example applications.

2. CONCEPTS AND DEFINITIONS OF THE FLOOD RISK METHODOLOGY

This section presents the concepts and definitions of the flood risk analysis methodology. Several of the terms are event tree and fault tree terminology and are reproduced here to provide the reader a compact glossary for the flood risk methodology.

2.1 Flood Description

The flood risk analysis methodology is independent of the source of the flood being considered. Regardless of the source, the level of the resulting flood can be characterized as a function of time. A hypothetical flood level profile is shown in Figure 2.1. In the general case, the flood level profile will show an increase in flood level from the onset of the event until it attains a maximum value, followed by a period of decreasing level as the flood recedes. Components that are affected by a given flood event can be identified by their vulnerability elevation and the flood level profile.

Either a discretized or linear flood level profile is used as input to the flood analysis computer program. Examples of these profiles are shown in Figures 2.2 and 2.3. The discretized profile reflects the assumption that once the flood has reached a discrete level in the plant, that entire level is flooded.

2.2 Component Vulnerability Elevation

The "vulnerability elevation" for the component is defined as the lowest physical elevation that the flood level must surpass to affect the component. The vulnerability elevation allows proper treatment of the case where a component may be affected by the flood but not yet submerged itself. For example, a pump whose function is dependent on electrical connections at a lower elevation than the pump is assigned the lower vulnerability elevation. However, if the pump's vital electrical connections are physically higher than the pump, the pump's vulnerability elevation is the physical elevation of the pump. A component's vulnerability elevation is physically higher than the component if a barrier prevents the flood from affecting the component until the flood overflows the barrier. In this case, the vulnerability elevation corresponds to the physical elevation where the flood overflows the barrier.

2.3 Flooded Minimal Cut Sets

The flood analysis methodology uses a fault tree and other input to identify minimal cut sets that have all their associated components submerged by the flood. These flooded minimal cut sets are the failure modes of interest since the occurrence of a single minimal cut set guarantees the occurrence of the system failure.

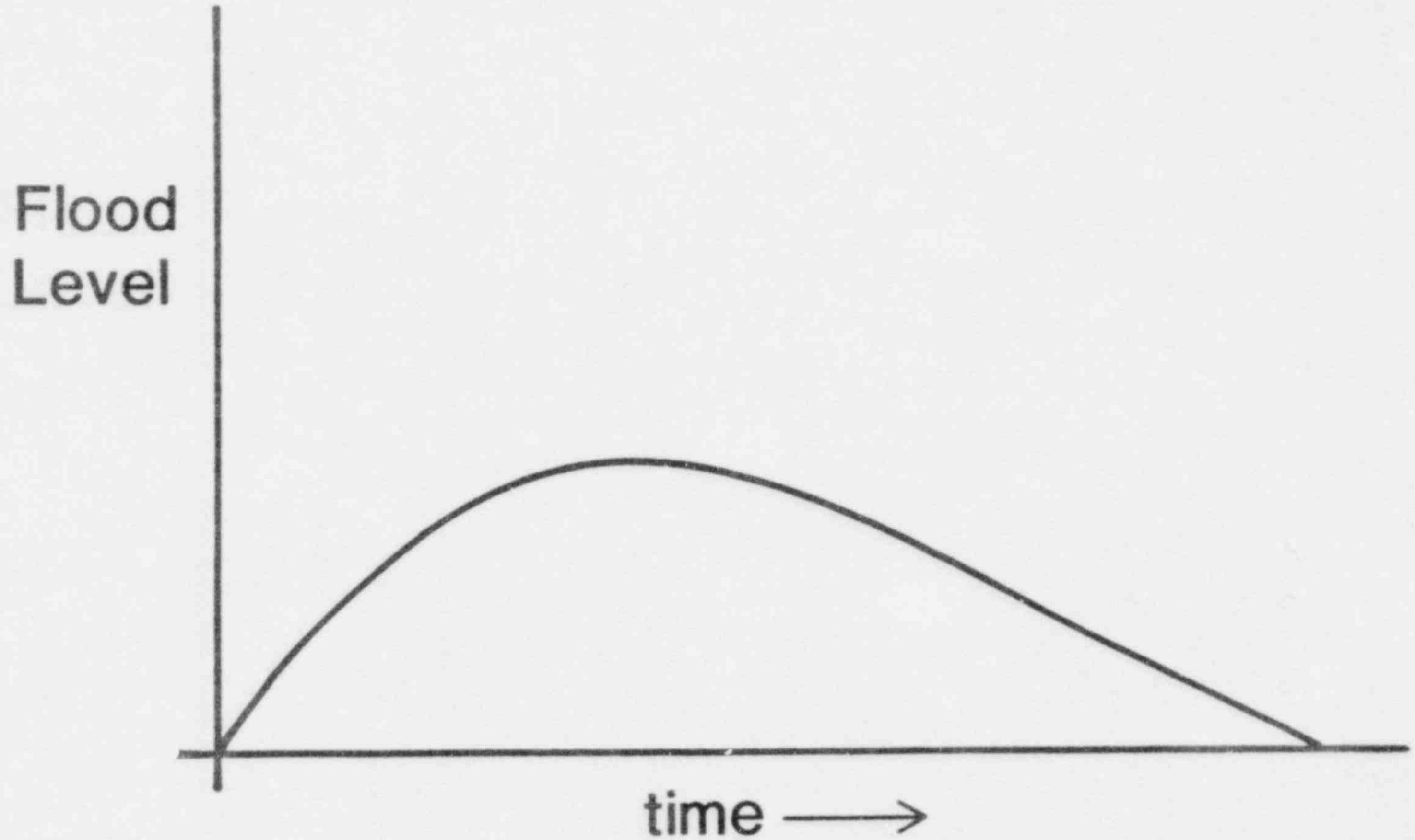

Figure 2.1 Hypothetical Flood Level Profile

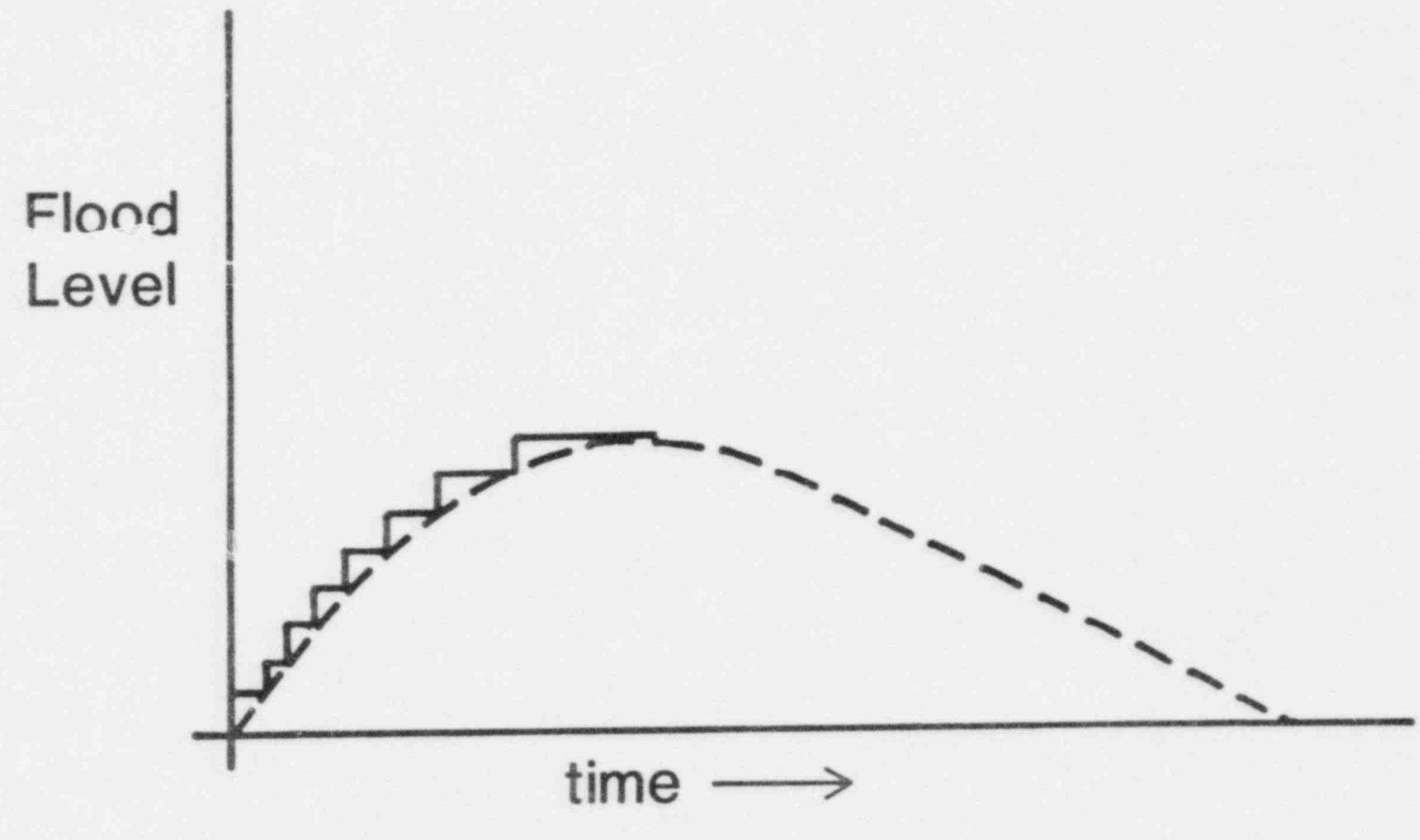

Figure 2.2 Discretized Flood Level Profile

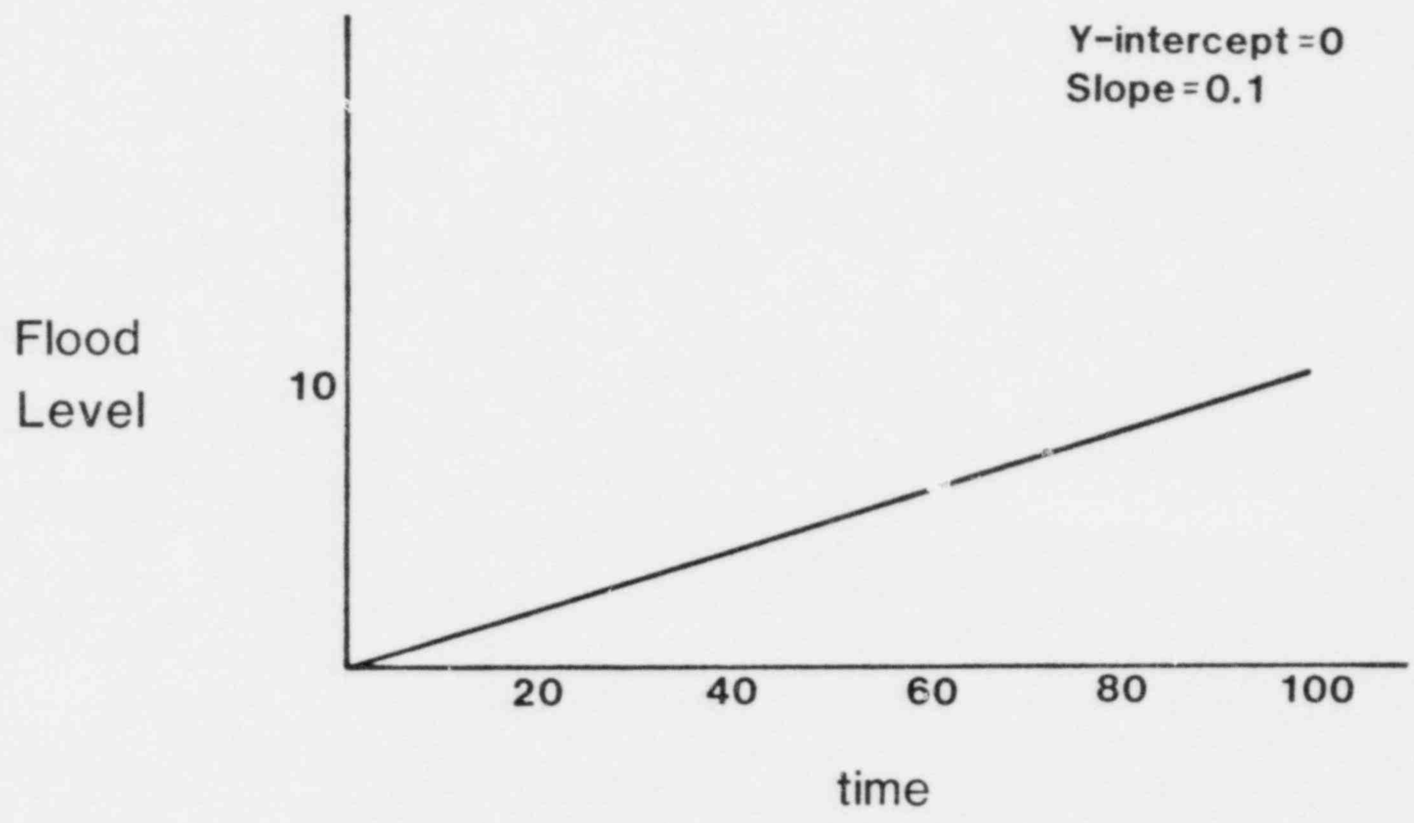

Figure 2.3 Linear Flood Level Profile

2.4 Partially Flooded Minimal Cut Sets

Partially flooded minimal cut sets are defined for the purpose of this project as those minimal cut sets in which at least one component is flooded and one or two components are not flooded. These minimal cut sets are potentially significant contributors to a system failure since they require only one or two components to fail, in addition to flood effects, to cause a system failure. Partially flooded minimal cut sets are particularly important in flood analysis when the flood of interest does not flood an entire minimal cut set.

2.5 Flood Protection Sets

A flood protection set is a group of components that, if they all are not flooded, guarantee the system is not failed as a result of the flood event. Flood protection sets can be synthesized from the flooded minimal cut sets (or partially flooded minimal cut sets) for each flood level of interest. The flood protection sets provide valuable qualitative information for determining where system flood protection efforts will be most effective.

2.6 Critical Flood Level

The "critical flood level" is defined as the minimum flood level where the first flooded minimal cut set is found. This is the minimum flood level where the system failure of interest can be directly caused by the flood.

2.7 Failure Flood Level

The "failure flood level" is defined as the minimum flood level where all the components in at least one minimal cut set are flooded and failed with probability one, thus resulting in a system failure probability of one. This is the minimum flood level where the system failure of interest is guaranteed to occur, given a flood to that level has occurred.

2.8 Event Sequence

Event trees are event sequence models that graphically display postulated accident scenarios (Figure 2.4). The elements of an event sequence, or accident sequence as they are often called, are an initiating event, branching operator failures and an identification of the consequence category to which the sequence leads. An initiating event is an undesirable event (component or system failure, transient, or external event) that starts an accident sequence. The branching operators generally represent actions taken by plant systems or

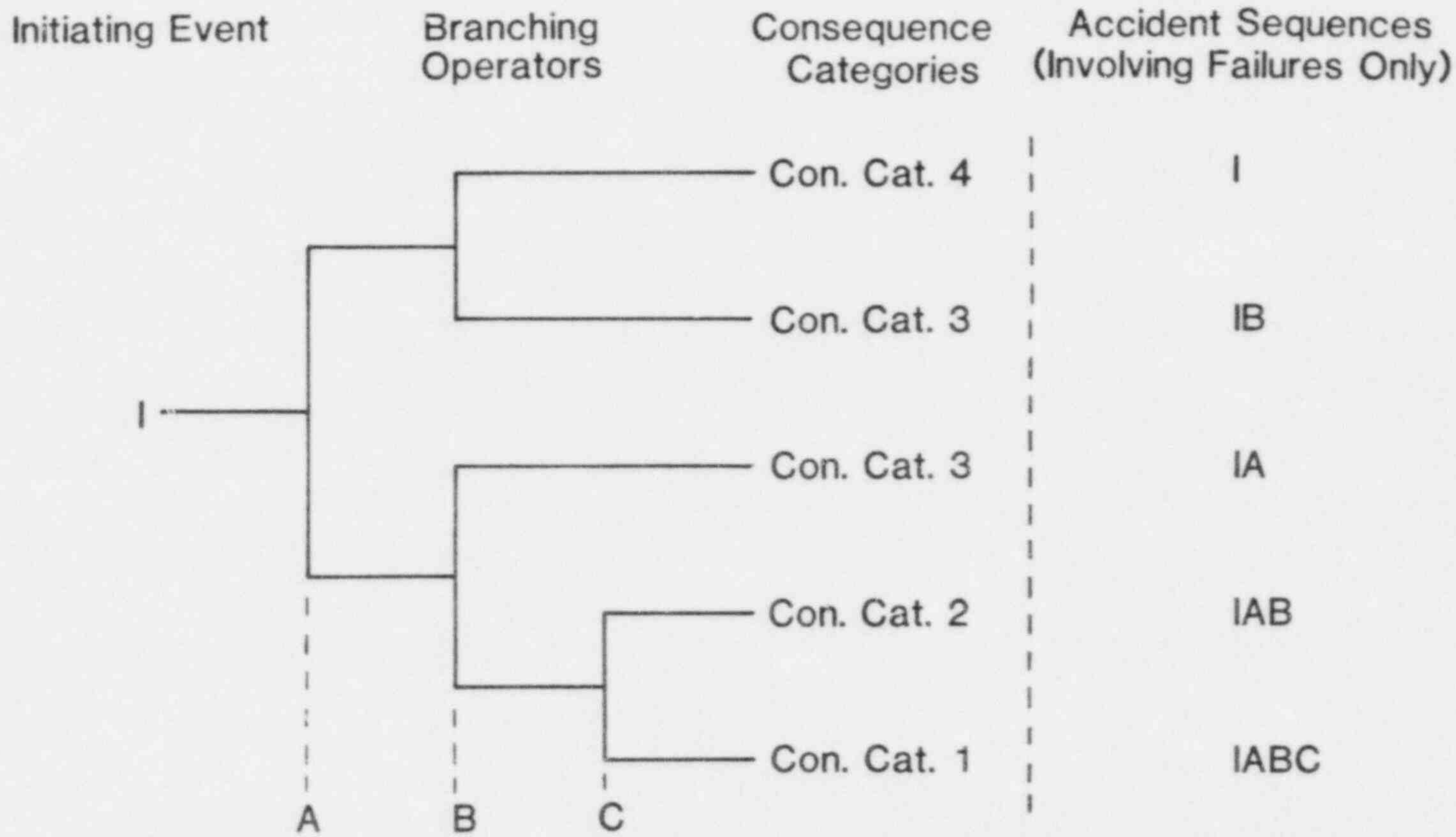

Figure 2.4 Example Event Tree

personnel which, if successful, act as barriers to the propagation of the event sequence or mitigate the effects of the initiating event. The success or failure of these branching operators determines the magnitude of the consequence of an accident. The consequence category identification defines the consequence to which the accident sequence leads.

2.9 Accident Sequence Occurrence Frequency

The occurrence frequency of a particular accident sequence is the product of the initiating event occurrence frequency and the conditional probabilities of failure on demand of the branching operators. The probabilities of failure on demand of the branching operators are usually very small; therefore, the probabilities of success on demand of the branching operators are very close to unity for systems normally encountered in nuclear power plants. In practice, the success on demand probabilities are conservatively assumed to be unity and the accident sequence occurrence frequency contains only failure events.

2.10 Flood Risk Analysis Procedure

The flood risk analysis procedure contains five steps that lead to quantification of flood effects in the accident sequence and consequence category occurrence frequencies. These five steps are:

- analyst prescreening,
- event sequence screening,
- system qualitative flood analysis,
- system quantitative evaluation, and
- accident sequence and consequence category quantitative evaluation.

Figure 2.5 is a flow diagram of the flood risk analysis procedure. Inputs and outputs of each step are indicated in the flow diagram. The following three sections discuss the methodology in detail.

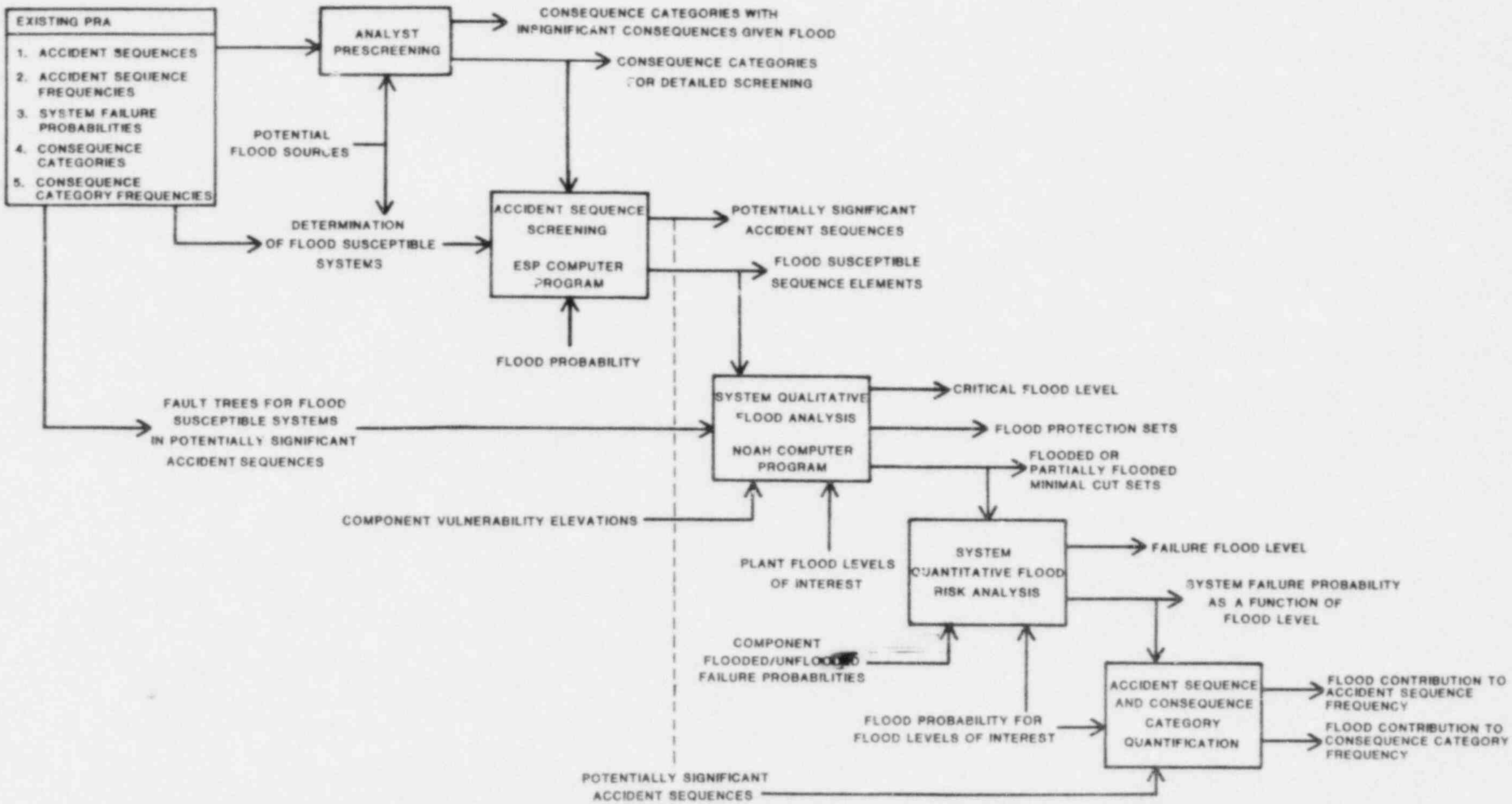

Figure 2.5 Flood Risk Analysis Procedure Flowchart

3. FLOOD SCREENING ANALYSES

Nuclear power plant probabilistic risk assessments (PRA's) usually postulate a large number (>100) of possible accident sequences. Each accident sequence contributes to one of several consequence categories. The accident sequence frequencies collectively determine the frequency at which consequences of various magnitudes occur; thereby providing a measure of risk. Usually, only a small number of sequences (dominant accident sequences) contribute significantly to the category frequency and these sequences are the ones analyzed in greatest detail.

The purpose of the flood screening analyses is to identify those accident sequences and systems that may be significant contributors to risk due to flood effects. The analyst cannot assume that the dominant accident sequences identified in the PRA are the most important sequences for flood analysis. Accident sequences which were previously considered less important, because of their relatively low expected frequencies, may contribute significantly to risk due to flood-induced failures. The screening process also provides a more manageable problem since accident sequences that are insignificant contributors to flood-induced risk can be removed from the analysis.

The flood screening analyses occupy the first two steps of the flood risk analysis procedure. The first screening analysis is a generic screening step based on plant characteristics and the result of the existing PRA. The second screening analysis employs a quantitative criterion for identifying individual accident sequences that are potentially significant contributors to flood-induced risk.

3.1 Analyst Prescreening

Analyst prescreening allows the analyst to eliminate from consideration entire categories of accident sequences or a class of flood sources prior to individual accident sequence screening. This can be done because the maximum contribution of a flood to the occurrence frequency of any consequence category is the occurrence frequency of the flood. On this basis, the analyst can perform prescreening to produce a more efficient event sequence screening in the second analysis step. The following discussion provides guidelines and examples for performing analyst prescreening.

3.1.1 Identifying Potential Flood Sources

Flood sources that may affect a nuclear power plant can be described by two classes of flood sources: (1) external flood sources, and (2) internal flood sources. External flood sources are the bodies of water such as rivers and lakes that are in the vicinity of a nuclear power plant. Large storage tanks on the plant site and outside the physical structure of the plant may also be considered as potential external flood sources. Internal flood sources are the large quantities of liquid inside the plant. Examples of internal sources include rupture of service water lines and inadvertent operation of a fire sprinkler system. The analyst must consider both of these sources of floods for a complete flood risk analysis.

3.1.2 Prescreening of Consequence Categories

Individual consequence categories are prescreened by comparing the occurrence frequency of a potential flood to the occurrence frequency of the consequence category. If the occurrence frequency of the flood is insignificant compared to the occurrence frequency of the consequence category, further analysis of the accident sequences within the category is not necessary.

An additional prescreening consideration is available when considering consequence categories that represent minor consequences in terms of risk. These minor consequences may be insignificant relative to the overall consequences of the flood (flooded cities, property damage, etc.) required to affect the plant. The analyst may elect not to consider a consequence category where the potential increase in the occurrence frequency of the consequences is completely overshadowed by the overall consequences of the flood itself.

3.1.3 Prescreening of Flood Sources

The analyst may eliminate one of the two types of flood sources from consideration on the same basis as the consequence category prescreening. Occurrence frequency comparisons for both types of flood sources are performed for each consequence category that passes the category prescreening. Prescreening the flood sources allows the analyst to focus on the more important flood sources for the accident sequence screening.

3.2 Accident Sequence Screening

3.2.1 Screening Procedure

To perform accident sequence screening, the analyst must identify accident sequence elements (initiating events or branching operators) that are considered susceptible to flood effects. An accident sequence element is considered flood-susceptible if it is expected to fail or be significantly degraded in the event a flood occurs. Determining which sequence elements are flood-susceptible requires qualitative considerations. Factors that indicate flood susceptibility include:

- the vulnerability elevation of equipment within a system,

- structural barriers to flooding,

- proximity of equipment to internal flood sources or flood pathways,

- the timing involved in demanding a system relative to the time the flood first affects the plant, and

- the capability of equipment to function in an extreme environment.

The analyst's assessment of a system's (branching operator) susceptibility to flooding is an important factor in the results of the accident sequence screening.

The analysis requires accident sequence screening for each consequence category that passes the analyst prescreening. The analyst screens all accident sequences within a consequence category in the following manner.

1. All flood-susceptible elements in the accident sequence are assumed to be failed with a probability of one. If the sequence contains no flood-susceptible elements, the sequence is eliminated from the analysis.

2. The analyst calculates the flooded occurrence frequency of the accident sequence. The flooded occurrence frequency is the product of the occurrence frequency of the flood and the occurrence probabilities of the sequence elements, assuming that the flood-susceptible elements have an occurrence probability of unity.

3. The accident sequence's flooded occurrence frequency is compared to a significance criterion; for example, a specified percentage of the consequence category's occurrence frequency.

4. Accident sequences considered significant, based on their flooded occurrence frequency, are retained for further analysis. Accident sequences deemed insignificant are discarded.

The analyst repeats this process for each accident sequence within a consequence category. The results for each category include:

- the significant accident sequences for each category, and

- the flood-susceptible sequence elements that require detailed analysis.

These significant accident sequences are the accident sequences that have the greatest potential for contributing to increased risk due to floods, based on the category's significance criterion (step 3 above). The flood-susceptible sequence elements identified for detailed analysis are those accident sequence elements that are flood-susceptible and are members of a significant accident sequence in the category.

The significant accident sequences of the category form the basis for quantifying the flood contribution to the consequence category in step five of the flood risk analysis procedure (Figure 2.5). The flood-susceptible sequence elements provide the basis for the detailed system qualitative flood analysis in step three.

3.2.2 Event Sequence Screening Program

The Event Sequence Screening Program (ESP)[4] performs the accident sequence screening described in the previous section. The basic input to ESP includes:

- a description of the initiating events and branching operators contained in the accident sequences, their respective unflooded occurrence frequencies or failure on demand probabilities, and an indication of their flood susceptibility,

- a flood occurrence frequency,

- the screening criterion used to identify significant accident sequences,

- a description of the consequence categories and their unflooded occurrence frequencies, and

- a description of the accident sequences.

The basic output of ESP consists of:

- the accident sequences that are potentially significant contributors to increased risk due to flood effects,

- the initiating events or branching operators that are considered flood-susceptible and appear in potentially significant accident sequences, and

- an estimate of the total consequence category occurrence frequency, which includes both unflooded and flooded effects.

In addition to the above information, ESP ranks the potentially significant accident sequences in order of contribution to the flooded occurrence frequency of a consequence category. Reference 4 is the user's manual for the ESP computer program.

4. SYSTEM QUALITATIVE FLOOD RISK ANALYSIS

The objective of the qualitative flood risk analysis is to identify the important failure modes for each flood-susceptible accident sequence element identified in the accident sequence screening. These important failure modes are the flooded minimal cut sets and partially flooded minimal cut sets for each flood-susceptible sequence element (flood-susceptible system failure). The qualitative flood analysis combines three basic inputs to perform a qualitative flood simulation. These inputs are:

1. The system fault tree - This fault tree defines the system failure of interest and the failure logic associated with the system failure.

2. Component vulnerability elevations - This elevation is the lowest level that the flood must surpass in order to affect the component.

3. Flood levels to be analyzed - These levels are the discrete flood levels used in the flood analysis. All basic events whose vulnerability elevations are below a particular flood level are considered flooded when minimal cut sets are determined.

The flood simulation determines the flooded minimal cut sets as a function of flood level. The methodology also identifies the critical flood level. The critical flood level is the flood level where the first flooded minimal cut set is found. For floods that do not surpass a system's critical flood level, the partially flooded minimal cut sets are the system's important failure modes.

The NOAH computer program(4) performs this qualitative flood simulation using a system fault tree. The inputs to NOAH include:

- control information specifying how the flood simulation is to be performed,

- a description of the flood levels to be analyzed,

- a description of the system fault tree,

- vulnerability elevations for the components in the system fault tree,

- basic event failure and repair data (optional), and

- a description of the flood level profile versus time (optional).

The fault tree description input to NOAH is identical to the fault tree description input to the MOCUS[5] and PREP[6] computer programs.

The output of the NOAH program depends on whether the analysis reaches the critical flood level. If the critical flood level is found, the basic output consists of:

1. The critical flood level - This is the flood level where the first flooded minimal cut set is found. The critical flood level can be determined without determining flooded minimal cut sets.

2. The flooded minimal cut sets for each flood level - This list identifies the minimal cut sets that have all their components flooded at each flood level increment.

3. The flood protection sets for each level - This list identifies groups of components that, if they are all made invulnerable to floods, would prevent the system as modeled from failing as a result of a flood.

4. Flooded components for each flood level - This list identifies the components that are flooded within each flood level increment, that is, the order of component submersion.

If the analysis does not reach the critical flood level, the basic output consists of:

1. Partially flooded minimal cut sets - This list identifies minimal cut sets that have all but one or two of their components flooded when the highest flood level for the analysis is reached. Partially flooded minimal cut sets are not determined if flooded minimal cut sets are found during the flood analysis.

2. Flood protection sets for the maximum level analyzed - This list identifies groups of components that, if they are all made invulnerable to floods, would prevent the system as modeled from failing as a result of a flood and single or double random failures.

3. The components that are flooded at the maximum level analyzed.

In addition to the flood simulation, the NOAH computer program has the capability to identify a specified component's role in the flood analysis results. For example, if the analyst requests the role of pump A in the flood analysis results, NOAH will identify and list the following information for pump A:

1. The flooded or partially flooded minimal cut sets which contain pump A. These minimal cut sets are grouped according to the flood level where the minimal cut set is flooded.

2. The vulnerability elevation of each component in the minimal cut sets.

Reference 4 is the user's manual for the NOAH computer program.

5. QUANTITATIVE FLOOD RISK ANALYSIS

Steps four and five of the flood risk analysis procedure consist of quantifying the flood effects on system failure probability and accident sequence occurrence frequency. Both point estimates and time-dependent analyses are possible. The required inputs for the quantitative flood analysis are:

1. the order of component submersion,

2. the time point corresponding to each component's submersion (for time-dependent analysis only),

3. each component's initial failure probability and normal (unflooded) failure rate,

4. the flooded and/or partially flooded minimal cut sets from the system fault tree, and

5. the component's flood response.

The NOAH computer program provides Inputs 1, 2, and 4 in the results of the qualitative flood risk analysis. Input 3 is standard input to existing quantitative reliability analysis techniques and can be obtained from the plant's PRA. The component's flood response, Input 5, is characterized in one of three ways:

1. No effect - Some components in the system fault trees remain unaffected upon submersion by the flood. For example, the submersion of a structural member has no effect on that member. This response requires no additional input for the quantitative evaluation.

2. Degraded - In this case, the system component is subjected to a non-normal operating environment which the component might be able to tolerate for some period of time. A degraded component has a discontinuous increase in unavailability at the time of submersion or a subsequent increase in failure rate, or both. For this response, the component's increase in unavailability upon submersion, if any, and the component's flooded failure rate are required as input to the quantitative evaluation.

3. Failed - The system component is subjected to a non-normal operating environment which the component cannot tolerate, and therefore

fails with probability one upon submersion by the flood. For the quantitative evaluation, the component's unavailability is set to one at the time of submersion.

These three component flood responses are shown graphically in Figure 5.1.

The results of the quantitative flood analysis are:

- time-dependent or point estimates of the probabilistic failure characteristics for the system failure of interest and flooded or partially flooded minimal cut sets,
- the expected occurrence frequency of accident sequences and consequence categories that include the effects of the flood, and
- the failure flood level, defined as the minimum flood level where all the components in at least one minimal cut set are flooded and failed with probability one, thus, resulting in a system failure probability of one.

Quantitative importance rankings for the flooded minimal cut sets and accident sequences are additional results from the quantitative flood analysis.

The KITT-2 computer program[6] is applicable for the time-dependent analysis of flood effects. The program accepts component initial failure probabilities and allows changes in a component's failure rate and unavailability at specified time points, allowing a complete description of the component's flood response. Preparing the time-dependent input for KITT-2 to describe the component flood responses can be tedious. The NOAH computer program contains output options that prepare portions of the KITT-2 input for the analysis. KITT-2 calculates and prints time-dependent reliability characteristics for the components, the minimal cut sets, and the system failure of interest.

The KITT-2 program is also applicable for point estimate evaluations of the flood effects. As in the time-dependent case, only the degraded and failed component flood responses require changes in the component's characteristics upon submersion. The estimated failure probabilities for the components, the components' times of submersion, and the system minimal cut sets are input to KITT-2 to estimate the system failure probability. For this application, the individual components are described as inhibit conditions in the KITT-2 input.

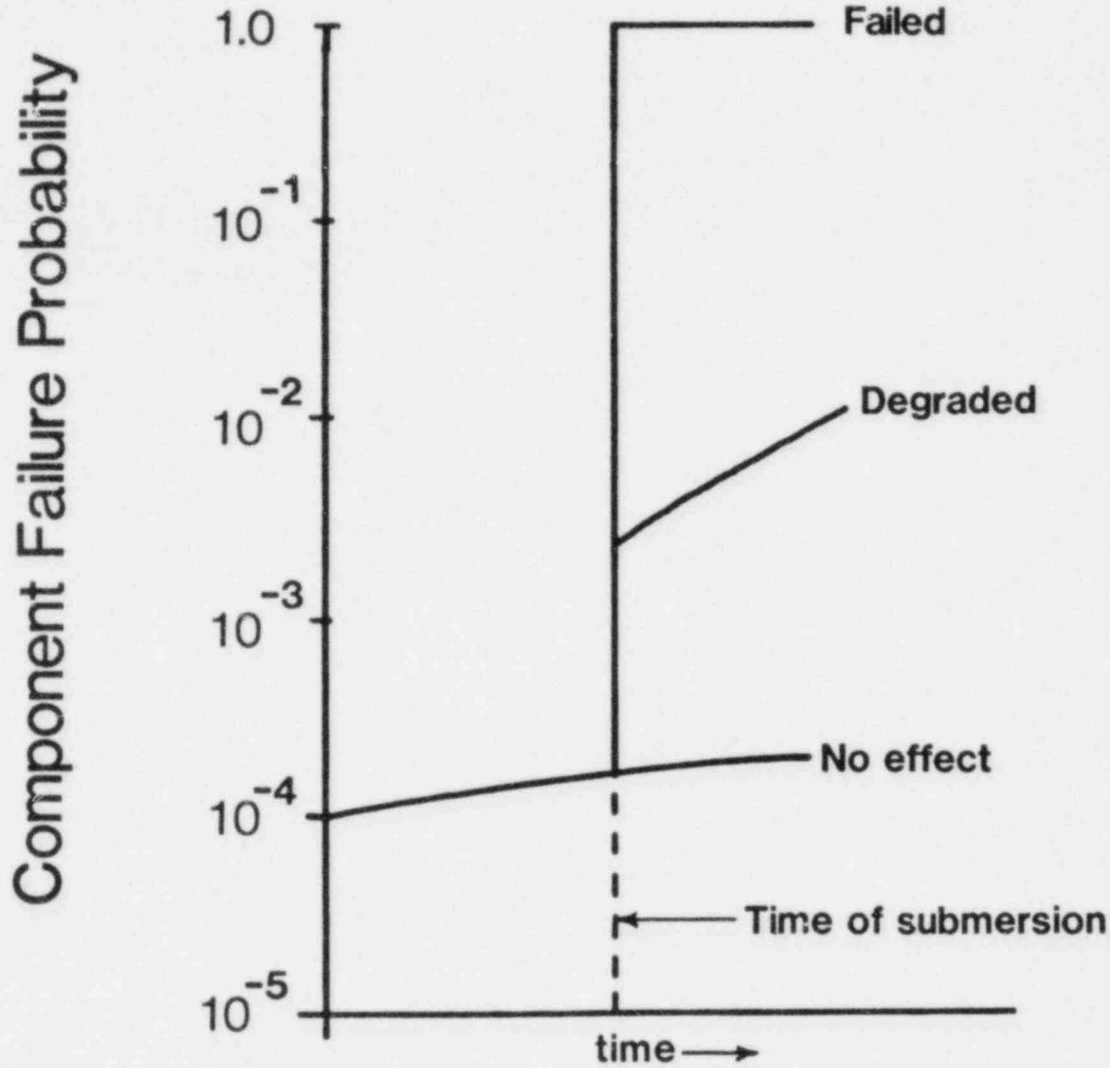

Figure 5.1 Allowed Component Flood Responses for Three Components That Have Identical Reliability Characteristics Before Submersion

5.1 Quantitative Methodology

This section develops the basis for the equations necessary to calculate the flood effects for all events of interest in the quantitative flood risk analysis. These events of interest are:

- basic event occurrence probability,
- minimal cut set occurrence probability,
- system failure occurrence probability,
- accident sequence occurrence frequency, and
- consequence category occurrence frequency.

Sections 5.3 through 5.7 present appropriate equations for each of these quantities. These equations employ the following definitions:

$f \equiv$ the event the flood exists, and

$\overline{f} \equiv$ the event the flood does not exist.

The events f and $\overline{f}$ are mutually exclusive. Therefore, any event X can be expressed as:[7]

$$X = (\overline{f} \cap X) \cup (f \cap X), \tag{1}$$

and its probability represented by:

$$P(X) = P(\overline{f})P(X \mid \overline{f}) + P(f)P(X \mid f) \tag{2}$$

where the conditional probabilities reflect the probability of X given no flood occurrence and the probability of X given flood occurrence, respectively. Substituting $P(\overline{f}) = 1 - P(f)$ in equation 2 and rearranging terms yields:

$$P(X) = P(X \mid \overline{f}) + P(f)[P(X \mid f) - P(X \mid \overline{f})] \ . \tag{3}$$

The first term on the right hand side of equation 3 is the unflooded contribution to the event's probability and the second term is the flooded contribution to the event's probability. The flooded contribution term consists of the flood occurrence probability and the increase in the event's probability, given the flood has occurred. This increase in the event's occurrence probability describes the "flood damage state" of the event.

The flooded contribution is the quantity of interest in the quantitative flood analysis. Calculating the flooded contribution allows the analyst to "add on" the flood effects to the results of an existing risk assessment.

5.2 Determining Flood Occurrence Probabilities

Proper evaluation of the flood occurrence probability is essential to determining the contribution of floods to the occurrence frequency of accident consequences. The desired probability is an exceedance probability; that is, the probability that a flood exceeds the flood level where damage to plant equipment occurs. For example, assume that flood level L is the flood level where plant damage first occurs. Figure 5.2 shows a hypothetical flood level frequency density with flood level L identified on the x-axis. The desired flood occurrence probability is the integral of the density for flood levels greater than or equal to flood level L; that is,

$$P(f_L) = \int_L^\infty f(\ell)d\ell, \qquad (4)$$

where

$P(f_L)$ = the occurrence probability of a flood equal to or greater than flood level L, and

$f(\ell)$ = the flood level frequency density function.

The flood occurrence probability given by equation 4 is applicable for analyses considering a single flood damage state in the quantitative evaluation. Flood level L corresponds to the minimum flood level that results in this flood damage state.

For application in analyses where multiple flood levels result in multiple flood damage states, the analyst must evaluate the flood occurrence probability for each flood damage state. For example, Figure 5.3 shows the flood level frequency density with four flood levels identified on the x-axis. Each flood level corresponds to a change in the event's flood damage state. The applicable flood probabilities are:

$$\int_1^2 f(\ell)d\ell = P(f_1) - P(f_2) \text{ for damage state A,} \qquad (5)$$

$$\int_2^3 f(\ell)d\ell = P(f_2) - P(f_3) \text{ for damage state B,} \qquad (6)$$

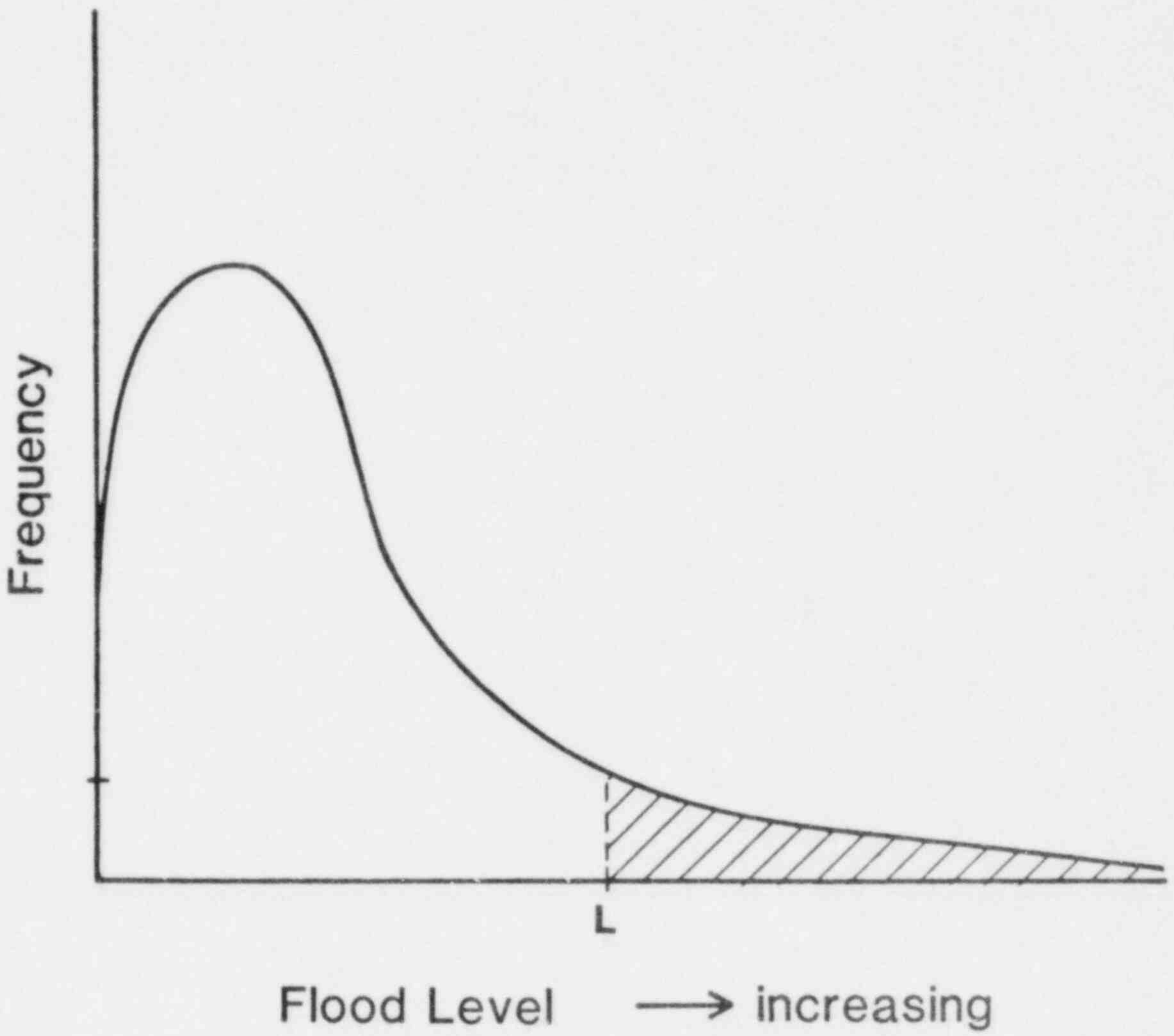

Figure 5.2 Hypothetical Flood Level Frequency Density Example

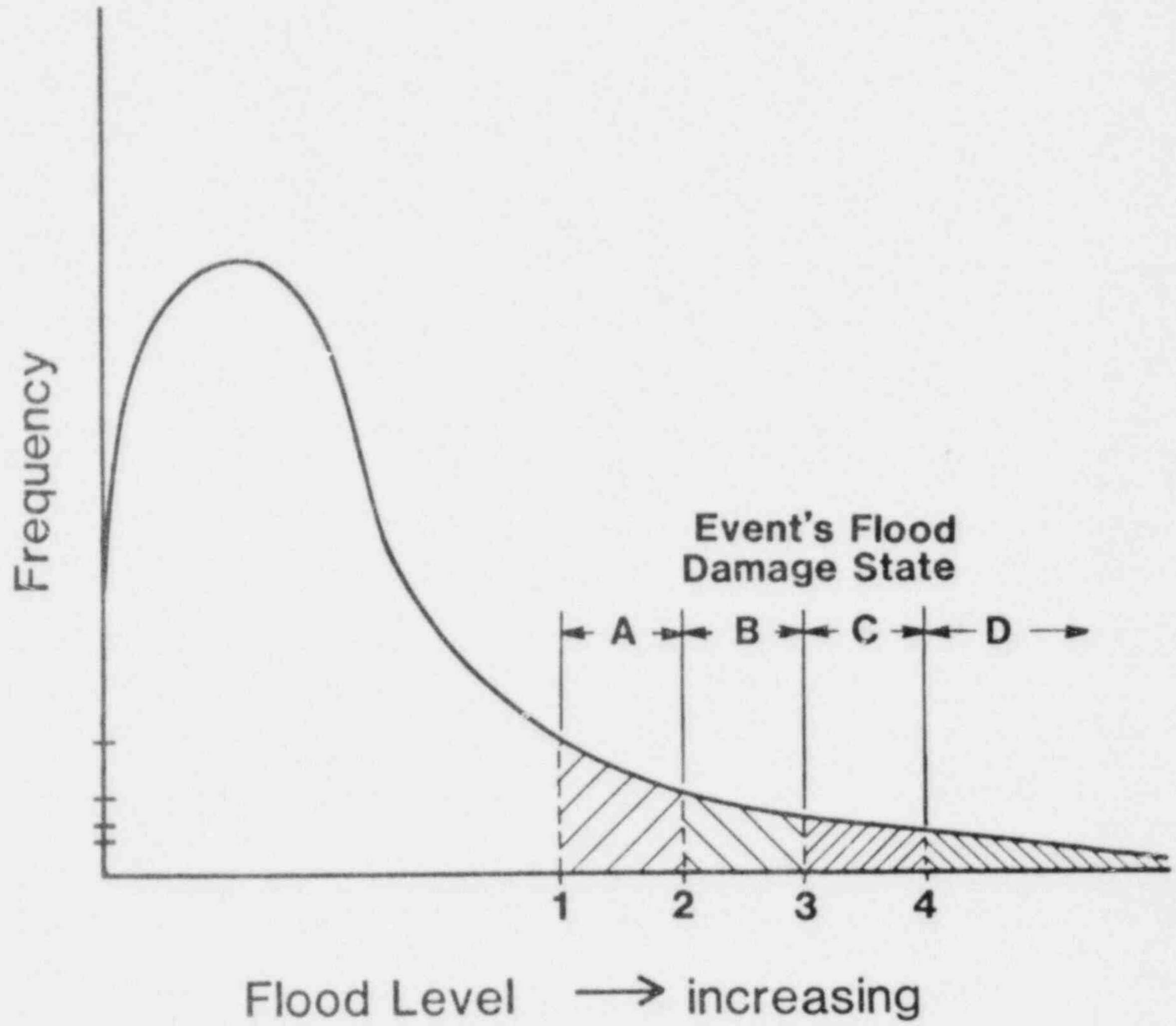

Figure 5.3 Hypothetical Flood Level Frequency Density Example for Multiple Flood Damage States

$$\int_3^4 f(\ell)d\ell = P(f_3) - P(f_4) \text{ for damage state C, and} \tag{7}$$

$$\int_4^\infty f(\ell)d\ell = P(f_4) \text{ for damage state D.} \tag{8}$$

Rewriting equation 3 (Section 5.1) to include this multi-level flooded contribution results in:

$$\begin{aligned} P(X) = P(X|\overline{f}) &+ [P(f_1) - P(f_2)]\cdot[P(X|f_1) - P(X|\overline{f})] \\ &+ [P(f_2) - P(f_3)]\cdot[P(X|f_2) - P(X|\overline{f})] \\ &+ [P(f_3) - P(f_4)]\cdot[P(X|f_3) - P(X|\overline{f})] \\ &+ P(f_4)[P(X|f_4) - P(X|\overline{f})]. \end{aligned} \tag{9}$$

Equation 9 includes a flooded contribution for each specific flood damage state and corresponding flood occurrence probability. Equation 9 can be written in general form as:

$$\begin{aligned} P(X) = P(X|\overline{f}) &+ \sum_{j=1}^{L-1} \{[P(f_j) - P(f_{j+1})]\cdot[P(X|f_j) - P(X|\overline{f})]\} \\ &+ P(f_L)[P(X|f_L) - P(X|\overline{f})], \end{aligned} \tag{10}$$

where

f_j = the event a flood equal to or exceeding level j exists, and

L = the number of flood damage states.

A comprehensive flood risk analysis will include assessment of multiple flood damage states as the flood progressively affects more and more components or systems in the plant. The following sections present both single- (flood damage) state and multi- (flood damage) state equations for quantitative flood risk analysis.

5.3 Basic Event Occurrence Probability

The flood response of a basic event, shown graphically in Figure 5.1, is described by equation 3 in Section 5.1. Redefining the event variables, the appropriate single-state equation for the basic event's occurrence probability is:

$$P(B) = P(B|\overline{f}) + P(f)[P(B|f) - P(B|\overline{f})], \tag{11}$$

where

B = the event the basic event B exists, and

P(B) = the occurrence probability of basic event B.

Equation 11 is also the multi-state equation for basic event occurrence probability. Since the basic event is allowed only one flood response (Section 5), it experiences only one flood damage state.

5.4 Minimal Cut Set Occurrence Probability

A minimal cut set is a group of basic events that are collectively sufficient to result in the system failure of interest. The minimal cut set therefore represents the logical intersection of a group of basic events. The probability of a logical intersection is the product of the individual events; therefore, the appropriate single-state equation for a minimal cut set is:

$$P(M) = \prod_{i=1}^{m} P(B_i \mid \overline{f}) + P(f)\left[\prod_{i=1}^{m} P(B_i \mid f) - \prod_{i=1}^{m} P(B_i \mid \overline{f})\right], \quad (12)$$

where

M = the event the minimal cut set M exists,

P(M) = the occurrence probability of minimal cut set M,

B_i = the event basic event B_i of minimal cut set M exists, and

m = the number of basic events comprising minimal cut set M.

The appropriate multi-state equation for a minimal cut set is:

$$P(M) = \prod_{i=1}^{m} P(B_i \mid \overline{f}) + \sum_{j=1}^{L-1} \left\{[P(f_j) - P(f_{j+1})]\cdot\left[\prod_{i=1}^{m} P(B_i \mid f_j) - \prod_{i=1}^{m} P(B_i \mid \overline{f})\right]\right\}$$

$$+ P(f_L)\left[\prod_{i=1}^{m} P(B_i \mid f_L) - \prod_{i=1}^{m} P(B_i \mid \overline{f})\right]. \quad (13)$$

The maximum flood damage state for a minimal cut set is the flood level where the minimal cut set is totally flooded. A minimal cut set can experience as many flood damage states as there are basic events in the minimal cut set.

5.5 System Failure Occurrence Probability

The system failure (fault tree TOP event) is the logical union of the minimal cut sets for the system fault tree. The probability of a logical union is the sum of the individual event probabilities, less all intersections of two events, plus all intersections of three events, and so on, until all intersection terms have been accounted for[8]. Ignoring these intersection terms, a first-order approximation for the single-state occurrence probability of the system failure is:

$$P(T) = \sum_{i=1}^{\ell} P(M_i \mid \overline{f}) + P(f) \left[\sum_{i=1}^{\ell} P(M_i \mid f) - \sum_{i=1}^{\ell} P(M_i \mid \overline{f}) \right], \qquad (14)$$

where

T	=	the event the system failure exists,
$P(T)$	=	the occurrence probability of system failure T,
M_i	=	the event minimal cut set M_i exists, and
ℓ	=	the number of minimal cut sets resulting in the system failure.

In systems that are highly susceptible to floods, this first-order approximation will greatly overestimate the system failure occurrence probability. In these cases, including the correction terms is necessary.

The multi-state equation for the system failure occurrence probability (first-order approximation) is:

$$P(T) = \sum_{i=1}^{\ell} P(M_i \mid \overline{f}) + \sum_{j=1}^{L-1} \left\{ [P(f_j) - P(f_{j+1})] \cdot \left[\sum_{i=1}^{\ell} P(M_i \mid f_j) - \sum_{i=1}^{\ell} P(M_i \mid \overline{f}) \right] \right\}$$

$$+ P(f_L) \left[\sum_{i=1}^{\ell} P(M_i \mid f_L) - \sum_{i=1}^{\ell} P(M_i \mid \overline{f}) \right]. \qquad (15)$$

The maximum flood damage state for a system failure is the failure flood level of the system. The system can experience as many flood damage states as there are basic events in the system.

5.6 Accident Sequence Occurrence Frequency

An accident sequence is the logical intersection of an initiating event and branching operator (system) failures. The appropriate single-state equation for the accident sequence occurrence frequency is:

$$P(S) = \prod_{i=1}^{n} P(T_i \mid \overline{f}) + P(f)\left[\prod_{i=1}^{n} P(T_i \mid f) - \prod_{i=1}^{n} P(T_i \mid \overline{f})\right], \tag{16}$$

where

S = the event accident sequence S exists,

P(S) = the probability per unit time (occurrence frequency) of accident sequence S,

T_i = the event the sequence element T_i of accident sequence S exists, and

n = the number of elements in accident sequence S.

The multi-state equation for the accident sequence occurrence frequency is:

$$P(S) = \prod_{i=1}^{n} P(T_i \mid \overline{f}) + \sum_{j=1}^{L-1} \left\{[P(f_j) - P(f_{j+1})]\cdot\left[\prod_{i=1}^{n} P(T_i \mid f_j) - \prod_{i=1}^{n} P(T_i \mid \overline{f})\right]\right\}$$

$$+ P(f_L)\left[\prod_{i=1}^{n} P(T_i \mid f_L) - \prod_{i=1}^{n} P(T_i \mid \overline{f})\right]. \tag{17}$$

The maximum flood damage state for an accident sequence is the highest failure flood level among the failure flood levels of the sequence's elements (initiating event or system failures). The highest failure flood level among the sequence elements defines the failure flood level of the accident sequence.

5.7 Consequence Category Occurrence Frequency

A consequence category is the logical union of a group of accident sequences. A first-order approximation for the single-state consequence category occurrence frequency is:

$$P(C) = \sum_{i=1}^{k} P(S_i \mid \overline{f}) + P(f)\left[\sum_{i=1}^{k} P(S_i \mid f) - \sum_{i=1}^{k} P(S_i \mid \overline{f})\right], \tag{18}$$

where

C = the event an accident sequence resulting in consequence category C exists,

$P(C)$	=	the probability per unit time (occurrence frequency) of a category C occurrence,
S_i	=	the event accident sequence S_i exists and results in a category C occurrence, and
k	=	the number of accident sequences contributing to consequence category C.

For consequence categories that are highly susceptible to flooding, this approximation will greatly overestimate the consequence category occurrence frequency. In these cases, including correction terms (discussed in Section 5.5) is necessary.

The multi-state equation for the consequence category occurrence frequency (first-order approximation) is:

$$P(C) = \sum_{i=1}^{k} P(S_i \mid \overline{f}) + \sum_{j=1}^{L-1} \{[P(f_j) - P(f_{j+1})] \cdot [\sum_{i=1}^{k} P(S_i \mid f_j) - \sum_{i=1}^{k} P(S_i \mid \overline{f})]\}$$

$$+ P(f_L)[\sum_{i=1}^{k} P(S_i \mid f_L) - \sum_{i=1}^{k} P(S_i \mid \overline{f})]. \quad (19)$$

The maximum flood damage state for a consequence category is the lowest failure flood level of any accident sequence that contributes to that consequence category.

6. LIMITATIONS OF THE METHODOLOGY

Determining all the minimal cut sets for the large complex fault trees found in practice is a generic problem of fault tree analysis. Quite often the number of minimal cut sets makes the task of determining those minimal cut sets impractical or impossible. The procedures implemented in the flood risk analysis methodology make this task less difficult by determining flooded minimal cut sets as they are submerged by a flood. However, as the flood depth increases and the number of flooded minimal cut sets approaches the total number of minimal cut sets, the methodology can be overwhelmed in the same manner as other conventional fault tree methods. In this case, extensions to the methodology are required if all these cut sets are required.

The methodology considers only one flood variable, flood level. Other flood variables such as flooding rate could be important.

The flood models presented in this report do not address potential changes in the risk assessment consequence model due to the effects of the flood. For example, an extensive river flood that affects the plant will possibly result in evacuation of the nearby population due to the flood itself prior to the plant damage. This would alter the population density that is available for exposure to a radioactive release from the plant, possibly reducing the potential consequences from the flood-induced accident. In existing risk assessments, each accident sequence contributes to a category that represents a broad range of consequences. The flood risk analysis methodology assumes that both the flooded and unflooded accident sequence contributes to the same broad category of consequences; that is, the change in the consequence model due to the flood does not place the accident sequence in a different consequence category.

The data required to properly evaluate the flooded failure probabilities and the flood occurrence probabilities are not readily available. Their evaluation requires qualitative considerations.

7. EXAMPLE APPLICATIONS OF THE FLOOD RISK ANALYSIS METHODOLOGY

Two example applications of the flood risk analysis methodology serve to demonstrate the use of the methodology and the results that can be achieved. Both applications relate to the Surry Power Station, the pressurized water reactor (PWR) used in the Reactor Safety Study.(1) The Reactor Safety Study provided the desired inputs from an existing risk assessment, that is, accident sequences and their occurrence frequencies, a consequence category structure, system failure probabilities and system fault tree models. A plant visit in February 1980 and design information from the Nuclear Regulatory Commission provided additional information for developing component vulnerability elevations. The project applied the flood risk analysis methodology to two flood scenarios using this information.

The first application considers the effects of a flood from an external source on the Auxiliary Feedwater System at the Surry Power Station. The analysis results show the flood effects on the probability of the dominant accident sequences* of the WASH-1400 transient event tree that involve failure of the Auxiliary Feedwater System. Figure 7.1 shows a typical result from the study - the core melt probability due to the dominant transient event accident sequences as a function of flood probability for a 10-foot flood (measured inside the plant). The flood contribution to the total probability for the case shown here considers only the dominant transient event accident sequences which involve failure of the Auxiliary Feedwater System. Appendix A describes this application and presents the results.

The second application considers the effects of a flood from an internal source at the Surry Power Station. The source selected is the rupture of a main steam or feedwater line in the main steam valve housing (MSVH) area. The Reactor Safety Study discusses this event's effect on the Auxiliary Feedwater System. This study also considers effects on the Containment Spray Injection System due to its proximity to the Auxiliary Feedwater System. Figure 7.2 shows a typical result from the study; the flood contribution to the consequence category occurrence frequencies for all transient event accident sequences for a flood probability of 7.5×10^{-5} per year. Appendix E describes this application and presents the results.

The results presented in Appendices A through E are demonstration examples for the flood risk analysis methodology. They should not be interpreted as a statement of the risk from the Surry Power Station since no effort has been expended to evaluate the applicable flood probabilities. For this reason, all results are presented as a function of flood probability.

*A complete flood analysis could require consideration of otherwise non-dominant accident sequences since the flood can increase the occurrence frequency of a sequence.

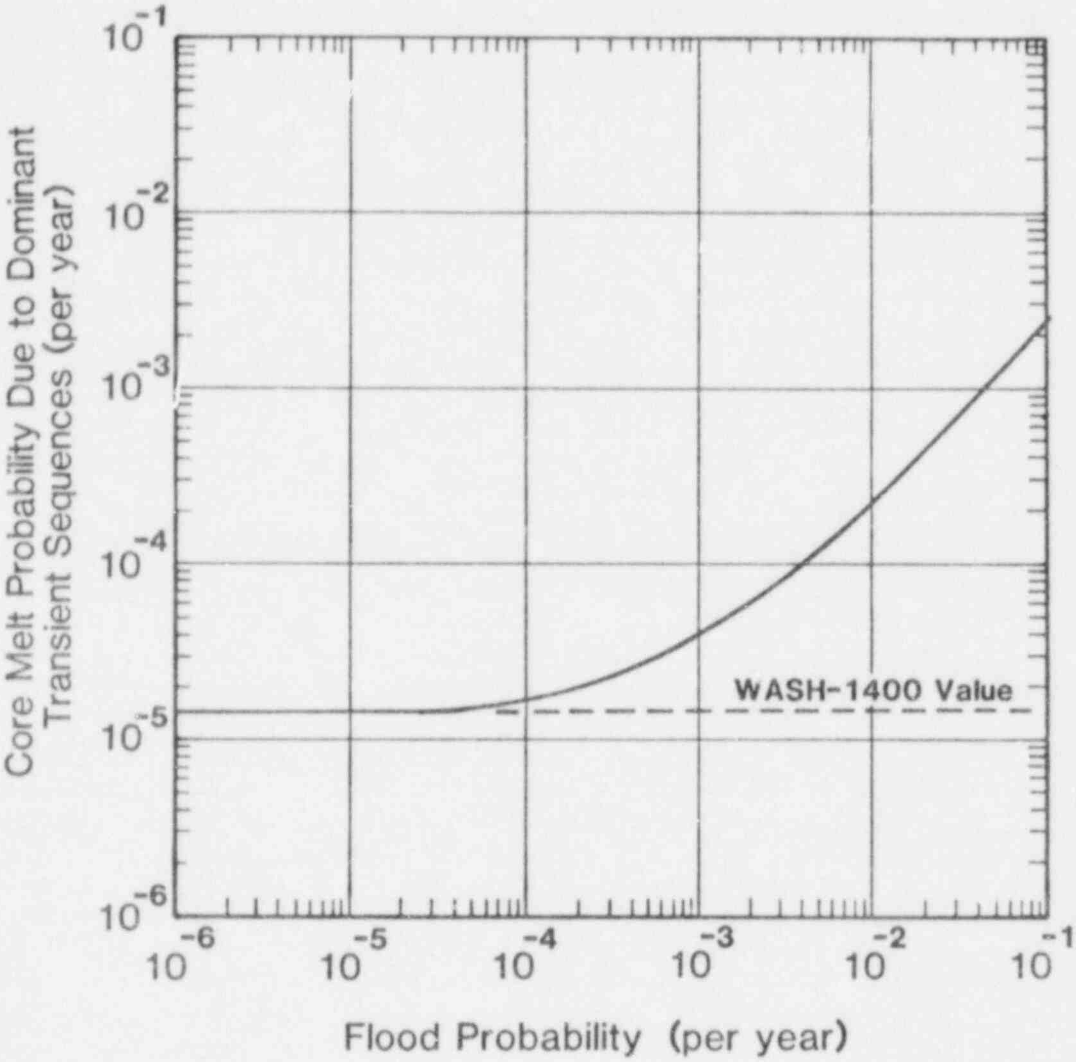

Figure 7.1 Core Melt Probability (per year) Due to the Dominant Transient Event Accident Sequences as a Function of Flood Probability for a 10-Foot Flood (measured internally) at the Surry Power Station

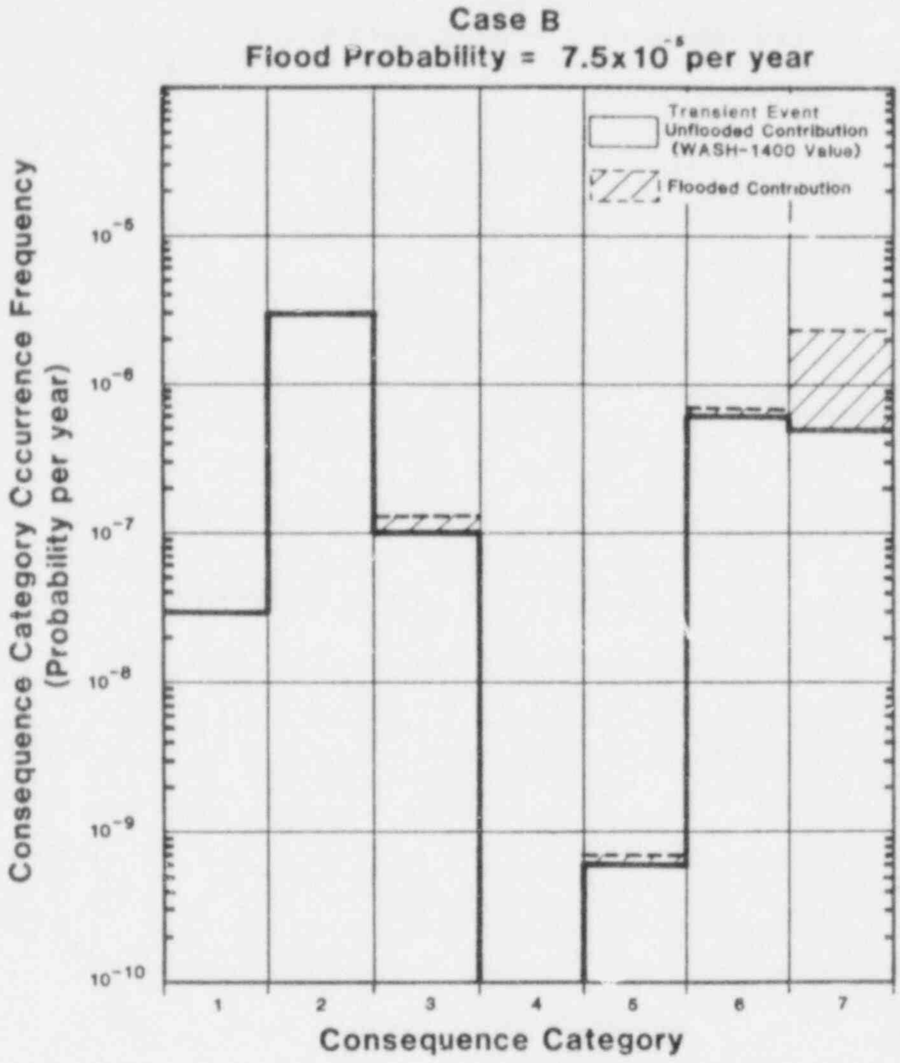

Figure 7.2 Flooded Contribution to Individual Consequence Category Occurrence Frequencies for All Transient Event Accident Sequences and the MSVH Flood, Case B, Flood Probability = 7.5 x 10^{-5} per year

8. SUMMARY

The flood risk analysis methodology presented in this report offers several advantages for assessing the impact of floods on nuclear power plant risk. These advantages are:

1. The flood risk analysis procedure is applicable at any stage of the probabilistic risk assessment (PRA) effort. The analyst can perform the flood risk analysis in parallel with the unflooded risk analysis or as an "add on" analysis after completion of the unflooded PRA.

2. Flooded contributions to risk can be determined for any quantity of interest in the PRA, for example, system failure probability, accident sequence occurrence frequency, or consequence category occurrence frequency.

3. The qualitative flood simulation provides valuable information for specifying flood protection measures, i.e., flood protection sets.

4. The analysis effort is reduced by analyst prescreening and accident sequence screening that eliminates insignificant contributors prior to detailed analysis efforts.

These advantages and the available computer aids provide the analyst with a viable tool for performing flood risk analysis and allow a more comprehensive assessment of the risks resulting from nuclear power plants.

The results of the flood risk analysis are useful in both the licensing and regulatory process. The analysis results can be compared with risk criteria to determine the suitability of a nuclear power plant site or the adequacy of flood protection barriers. The analysis also provides information that is valuable in specifying flood protection measures (barriers or procedures) for individual safety systems or the power plant as a whole. Owners of nuclear power plants can also use the analysis results for identifying flood protection measures for increased plant availability or for demonstrating compliance with regulatory requirements.

Additional applications of the flood risk analysis methodology are needed to refine the analysis procedure. An extensive, full-scale application will uncover problems associated with the procedure that are not apparent in the example applications discussed in this report.

Such an analysis should consider multiple flood damage states. The methodology presently available provides the tools for the analysis and this full-scale application will enhance the techniques for fully utilizing these tools.

REFERENCES

1. Reactor Safety Study, WASH-1400 (NUREG-75/014), U. S. Nuclear Regulatory Commission, October 1975.

2. Lewis, H. W., et al., Risk Assessment Review Group Report to the U. S. Nuclear Regulatory Commission, NUREG/CR-0400, September 1978.

3. Burdick, G. R., et al., A Collection of Methods for Reliability and Safety Engineering, ANCR-1273, Aerojet Nuclear Co., April 1976.

4. Wagner, D. P., et al., ESP and NOAH - Computer Programs for Flood Risk Analysis, JBFA-107-81, JBF Associates, Inc., Knoxville, Tennessee, December 1981.

5. Fussell, J. B., et al., MOCUS - A Computer Program to Obtain Minimal Sets from Fault Trees, ANCR-1156, Aerojet Nuclear Co., August 1974.

6. Vesely, W. E., and Narum, R. E., PREP and KITT: Computer Codes for the Automatic Evaluation of a Fault Tree, IN-1349, Idaho Nuclear Corporation, August 1970.

7. Walpole, R. E., and Myers, R. H., Probability and Statistics for Engineers and Scientists, The Macmillan Company, New York, 1972.

8. Vesely, W. E., Analysis of Fault Trees by Kinetic Tree Theory, IN-1330, Idaho Nuclear Corporation, October 1969.

9. McBride, A. F., Investigation of the Effects of Major Floods on the Safety of the Surry Nuclear Power Station, SAI-OR-147-046, Science Applications, Inc., Oak Ridge, Tennessee, September 1980.

APPENDIX A

A FLOOD ANALYSIS OF THE SURRY POWER STATION AUXILIARY FEEDWATER SYSTEM

A.1 INTRODUCTION

This appendix describes a flood analysis of the Auxiliary Feedwater System (AFWS) of the Surry Power Station. The analysis demonstrates the methodology developed for the Flood Risk Analysis Methodology Development Project. This analysis is a part of the FY80 tasks of the project.

No attempt is made to quantify the probability of the flood considered or identify the source of the flood. The flood analysis methodology determines the flood effects on the system using existing system models obtained from the Reactor Safety Study as input. Results of the Reactor Safety Study analysis of the Surry AFWS are reviewed here to provide a reference for assessing the flood effects. Estimated changes in the probabilities of the Reactor Safety Study dominant accident sequences from the transient event tree are also presented. No effort was made to determine if accident sequences that were negligible contributors to the Reactor Safety Study results become significant contributors in the event of a flood. The analysis considers only accident sequences that were determined to be dominant in the Reactor Safety Study.

A.2 PROBLEM DESCRIPTION

A.2.1 Auxiliary Feedwater System Description

The function of the Auxiliary Feedwater System (AFWS) is to provide feedwater to the secondary side of the steam generators upon loss of main feedwater. This function is necessary to (1) maintain an adequate coolant inventory in the steam generators and (2) transfer heat to the environment following a transient event that results in loss of the Main Feedwater System. A loss of both the Main and Auxiliary Feedwater Systems for more than one and one-half hours after the transient event could result in core melting[1].

Figure A.1 is a simplified flow diagram of the AFWS. The system has three pumps, two electric motor-driven with a capacity of 350 gallons per minute each, and one turbine-driven with a capacity of 700 gallons per minute. The pumps can be started either automatically or manually. The electric pumps start automatically when:

1. a Safety Injection Control System (SICS) signal is present,
2. loss of offsite power is detected,
3. the main feedwater pumps are shut off, or
4. low water level is detected in a steam generator.

The turbine pump starts automatically when:

1. low water level is detected in a steam generator, or
2. loss of offsite power is detected.

All the pumps are aligned to the 110,000 gallon condensate storage tank via separate suction lines at all times, except when maintenance is being performed on a pump. The three pumps deliver water to two headers which penetrate containment. Inside containment, each steam generator can receive condensate from either header.

All the decay heat produced can be removed by any one of the three pumps delivering feedwater to any one of the three steam generators. The amount of feedwater needed decreases with time. The operator can throttle flow to the steam generators by shutting off redundant pumps and then, utilizing the motor-operated valves inside containment, decrease the flow as necessary to match the steam produced and released.

The 110,000 gallon condensate storage tank contains enough water to allow cooldown for approximately eight hours. If the AFWS is

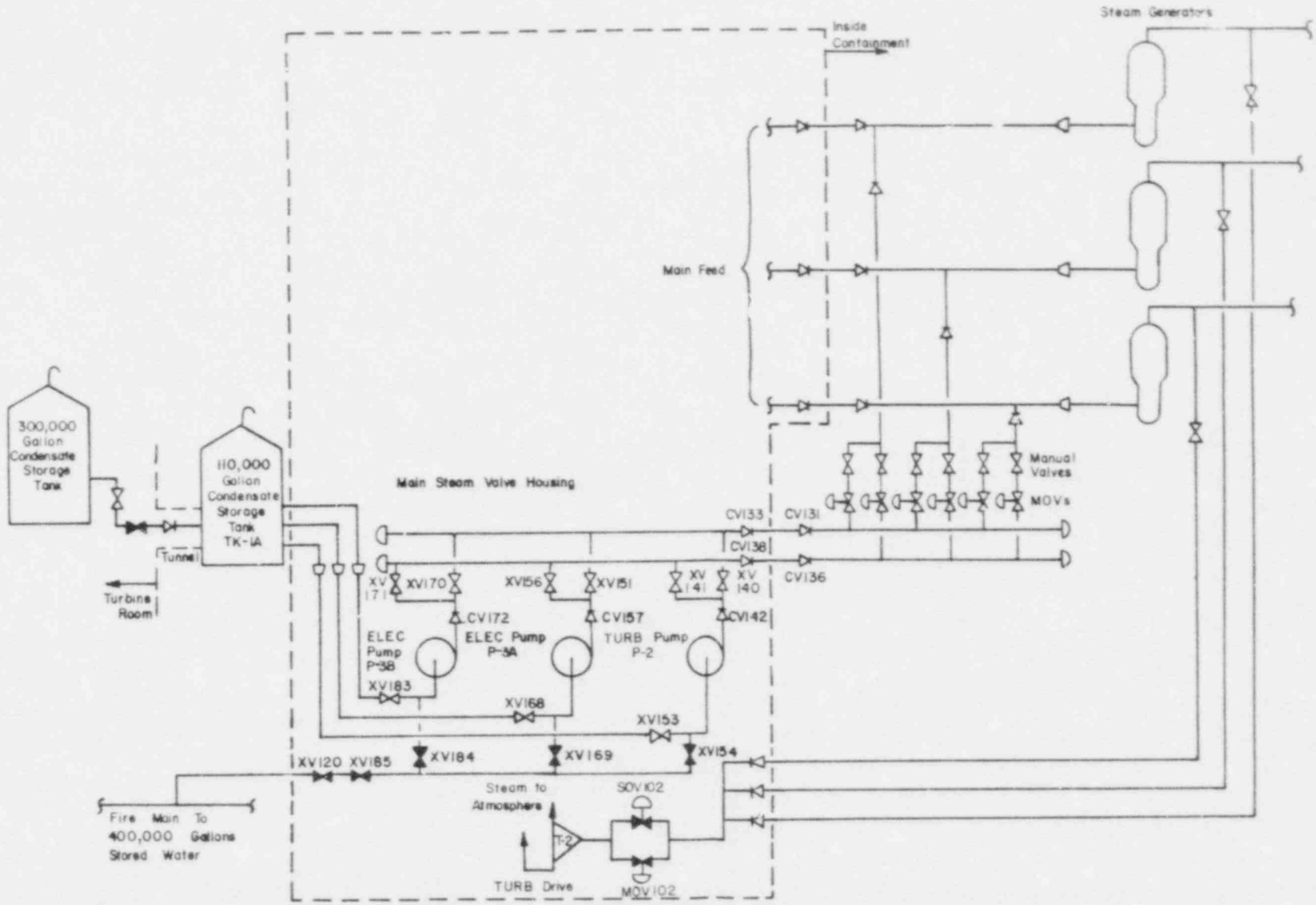

Figure A.1 Surry AFWS Simplified Flow Diagram required for a longer period, the operator must take action to valve in additional water sources. There are two sources available; a 300,000 gallon storage tank and the fire main which makes available at least 400,000 gallons with up to 400 gallons per minute replacement from wells.

A.2.2 Flood Scenario at the Surry Power Station

The Surry Nuclear Power Station is located in eastern Virginia on the James River. The James River provides cooling water for the station's condensers via an inlet canal upstream of the station. After removing heat from the condensers, the water is discharged to the James River via an outlet canal downstream of the station. Simplified elevation and plan views of the Surry Station are shown in Figures A.2 and A.3.

As shown, the station consists of two nuclear reactor plant units. The two containment buildings each contain a nuclear steam supply system consisting of a pressurized water reactor (PWR) and three steam generators. The steam generators of each unit supply steam to separate turbine generators located in the turbine building. The annulus and auxiliary buildings contain process and safety systems. The control rooms and relay rooms are located in the service building between the auxiliary building and turbine building.

The local grade elevation at the site is 27 feet above the mean water level in the outlet canal and 6 feet above the mean level in the inlet canal. The site is afforded some protection by levees between the inlet canal and the plant buildings. A flood at the plant site would occur if the James River water level increased greatly. The effects of floods at the plant site are discussed below.*

A.2.2.1 Flood Depths Less than Local Grade Elevation

Flood depths less than the local grade elevation are assumed in this study to have no effect on plant equipment. Floods of this magnitude may result in failures of the VEPCO grid supplied by the Surry Plant. This would result in a plant trip unless an anticipatory reduction in plant power to house load was accomplished. Access to and from the site could also be restricted.

---

* Site effects and flood pathways into the plant buildings were obtained from a visit to the Surry Plant on February 21, 1980.[9]

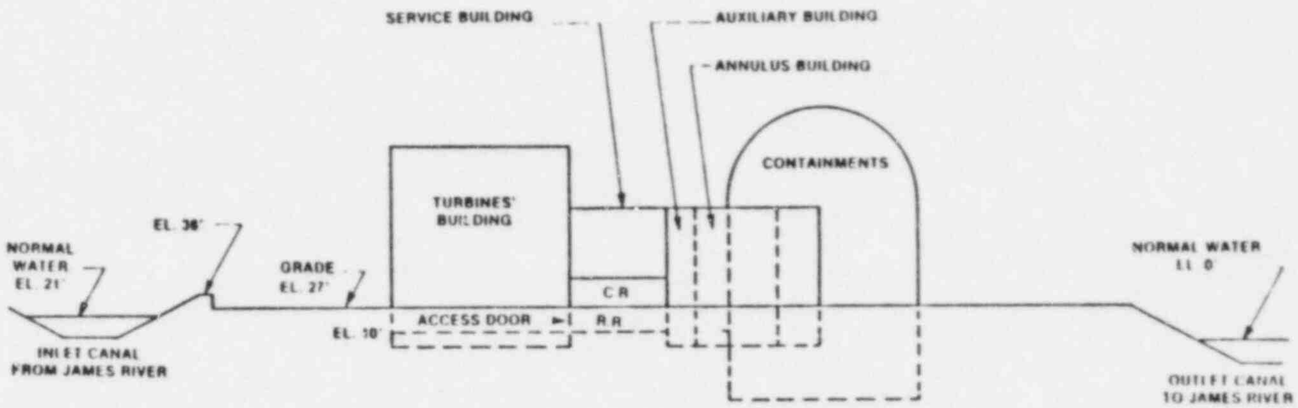

Figure A.2 Elevation of the Surry Nuclear Power Plants

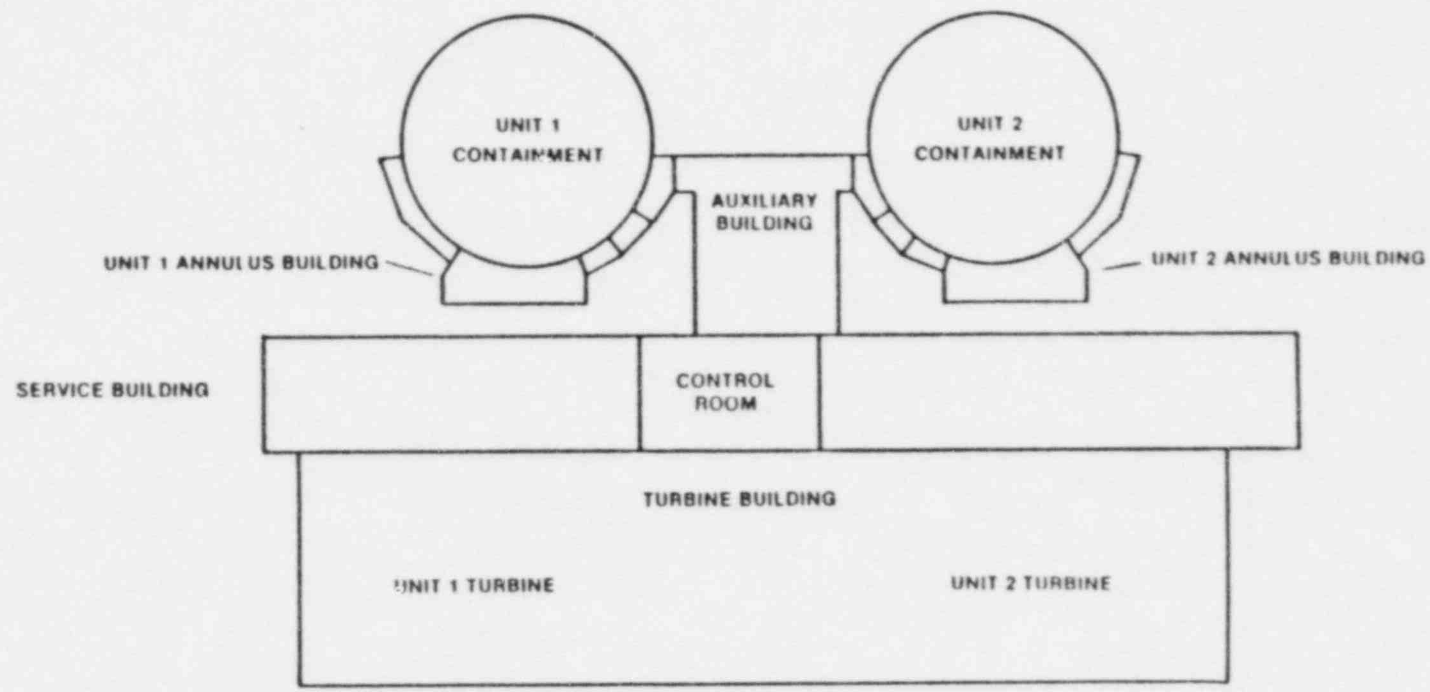

Figure A.3 Plan of the Surry Nuclear Power Plants

A.2.2.2 Flood Depths Above Local Grade Elevation

In contrast to flood depths less than local grade elevation, floods with a depth only slightly above local grade elevation (less than 2 feet above) are expected to fail a majority of the plant's equipment. Flood depths above local grade elevation will result in water flow into the buildings through grade level doors and eventually submerge the portions of the buildings that are below local grade elevation. The extent to which a building fills will depend on the duration of the flood and the flow rate into the buildings. For purposes of this study, non-sealed buildings are assumed to fill to the exterior flood elevation. The assumptions concerning the postulated flood on the site buildings are:

- Containment - The containment building is sealed and no flood pathways exist into the building.

- Turbine - If a flood above local grade elevation occurs, the turbine building would begin to flood through many grade level doors (including large corrugated "roll-up" doors). Flooding in the lower levels of the turbine building (elevation less than 10 feet) results in loss of main feedwater to both plants due to failure of the condensate pum s.

  As the water level in the turbine building rises above the 10-foot elevation floor, water spills over the 2-foot high barrier separating the turbine building from the relay room located in the service building. The relay room then floods from leakage around the doors or through the doors if the hydrostatic pressure opens the doors. This flood flow path is schematically shown in Figure A.4. Flooding the relay room results in shorting all electric power, control and sensor circuits of the Surry unit.

- Auxiliary - The equipment located in the auxiliary building requires electric power for its operation. Since electric power is assumed lost due to flooding of the relay room, no additional failures are postulated. The additional effects of auxiliary building flooding are restricted access to the building and possible additional post-flood recovery problems.

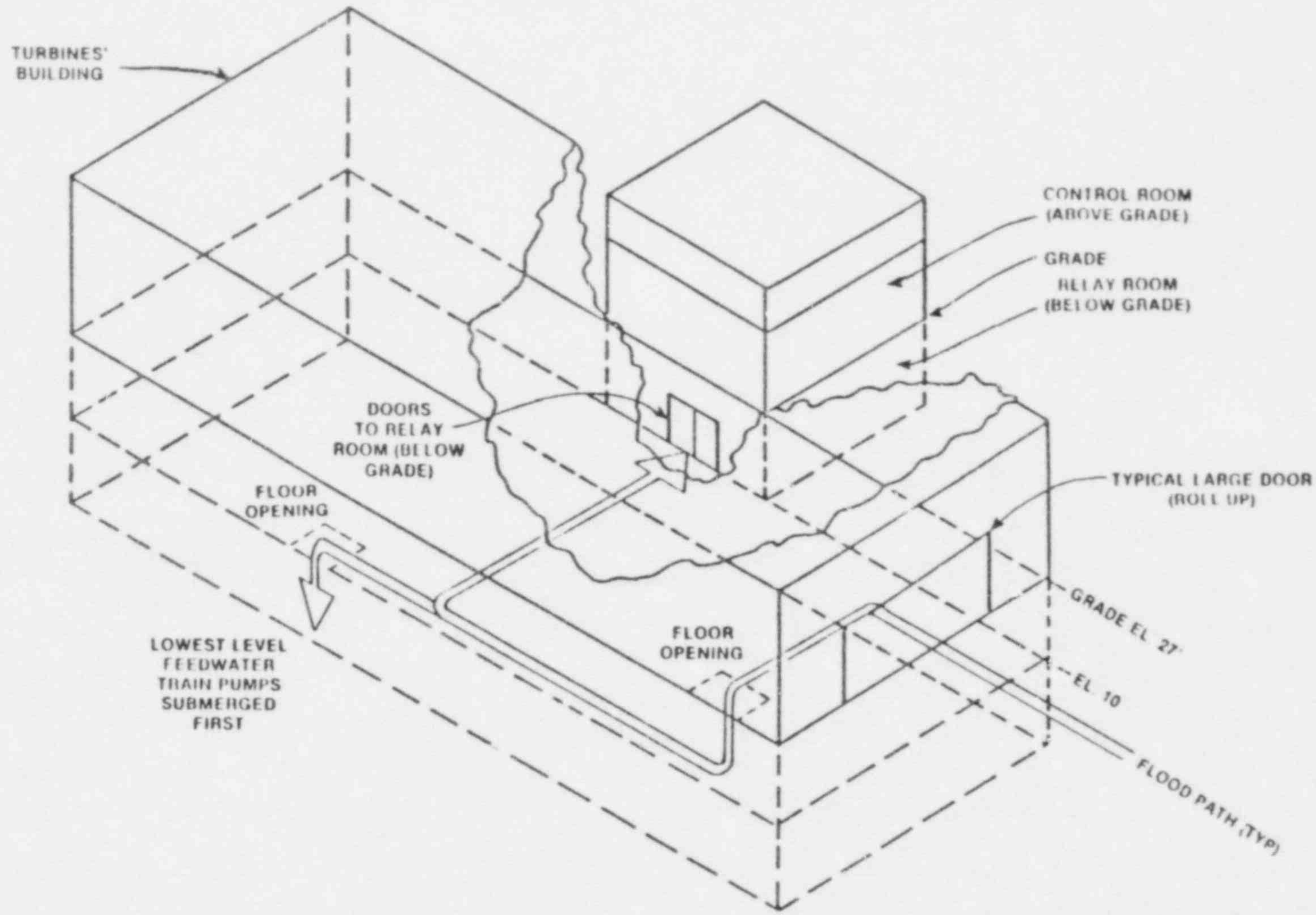

Figure A.4 Typical Flood Path Through the Turbine Building to the Relay Room

The effects of a flood greater than two feet above local grade elevation are expected to be similar to those of up to two feet above local grade elevation floods. The major differences are reduced access to plant areas other than the containment buildings, and that the steam turbine-driven pump must operate while submerged. Although this pump/driver is not guaranteed to fail when submerged, the pump's reliability in this operating mode is significantly reduced.

A.2.2.3 Flood Profile for the Surry AFWS Analysis

Figure A.5 shows a flood level profile for the Surry AFWS based on the flood scenario discussed above. The profile indicates that the analysis considers two flood levels, 10 feet and greater than 29 feet, and these are related to external flood levels in Table A.1. The zero flood level corresponds to the system's unflooded state. The time scale details are not important in this analysis since time-dependent system failure characteristics are not used once the flood begins. When the external flood level rises above 27 feet (local grade elevation), portions of the buldings below local grade elevation begin to fill. The flood level of 10 feet is considered since that is the elevation of the plant's relay room. At a flood level above 29 feet, the AFWS pumps are submerged. A more finely resolved discretized flood level profile would not affect the results of the analysis presented here because of the location of the AFWS equipment in the Surry Plant.

A.2.3 AFWS Fault Trees

The Nuclear Regulatory Commission provided fault trees for the Surry AFWS for use in the Surry AFWS flood analysis. The fault trees are based on the assumptions that:

1. Removal of decay heat from the primary system via the steam generators requires a minimum flow rate of 350 gallons per minute.

2. The 110,000 gallon condensate storage tank contains sufficient water to supply auxiliary feedwater for eight hours.

3. If the AFWS is required beyond 8 hours, the fire main supply must be valved in and sufficient steam to operate the turbine-driven pump is not available. Also, the electric pumps are assumed to be running and do not require restarting.

4. The requirement for the AFWS includes either:

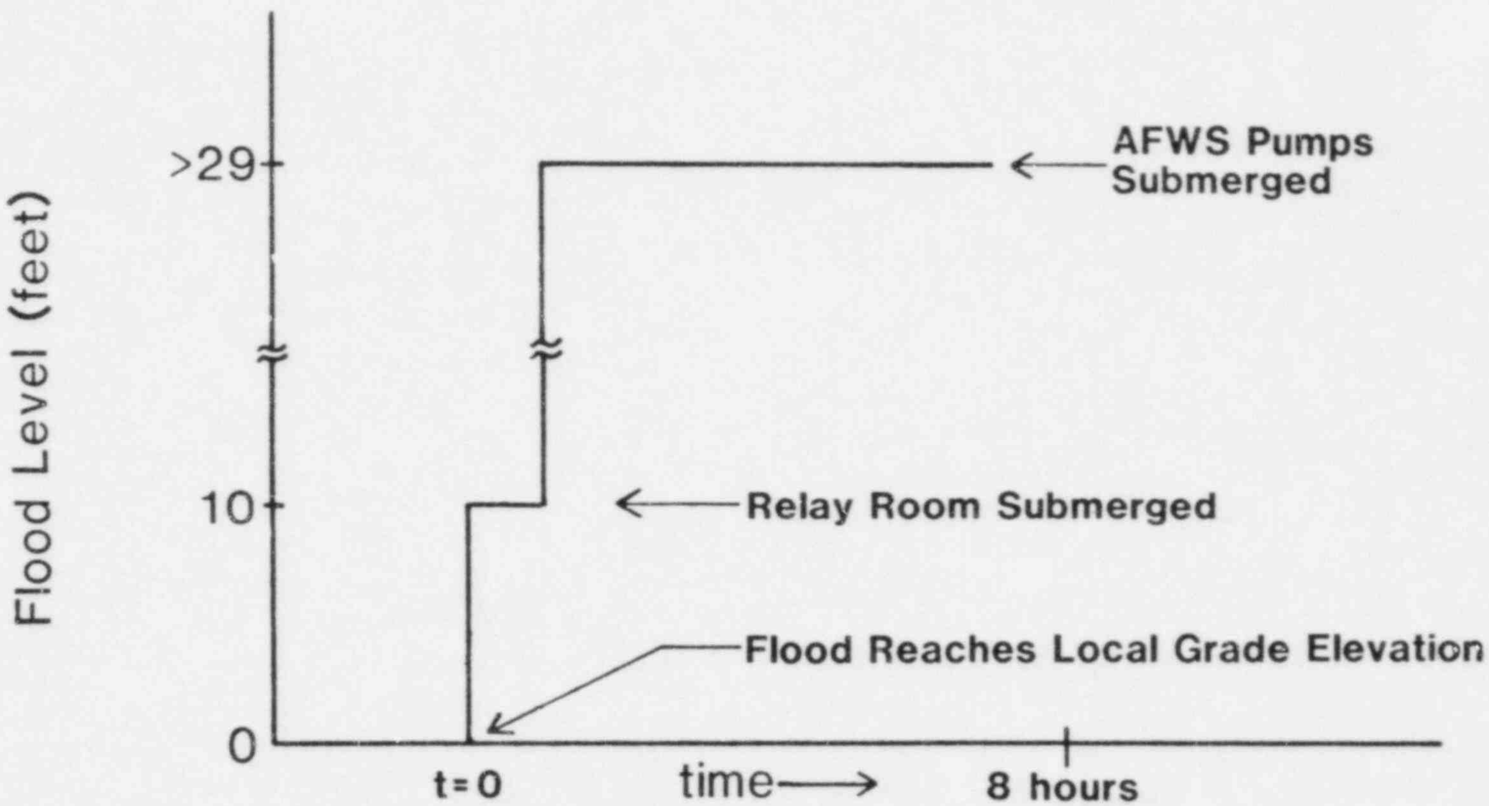

Figure A.5 Discretized Flood Level Profile for the Surry AFWS Flood Analysis

Table A.1 Relation of External Flood Levels to AFWS Flood Levels

AFWS Flood Level (feet)	Relation to External Flood Level
0	A flood level less than 27 feet above mean water level; therefore, below local grade elevation. The AFWS is not affected.
10	A flood level slightly above 27 feet begins to flood the AFWS. The 10 foot AFWS flood level is important because it submerges the relay room.
>29	A flood level greater than 29 feet above mean water level; therefore, greater than 2 feet above local grade elevation. The AFWS pumps are submerged at this flood level.

a. a small LOCA,
b. loss of offsite power, or
c. any other transient which causes loss of main feedwater.

5. Loss of offsite power affects both Units 1 and 2 of the Surry Power Station; however, only Unit 1 AFWS is considered in this study.

As a result of assumptions 2 and 3, two fault trees are required to describe the AFWS, one for the time period from start through eight hours, and one for the time period exceeding eight hours. The system failure of interest for both time periods is "Auxiliary Feedwater System Failure", which is defined as insufficient flow to all three steam generators.

The analysis evaluated these fault trees based on the postulated flood scenario at the Surry Plant, and modified the fault trees to reflect the following assumptions:

1. The probability of AFWS starting on demand is assumed to be unaffected by the flood. This assumption is justified by the observation that the minimum internal elevation for equipment important to the AFWS is 10 feet, i.e., the relay room. As flood water enters the buildings, elevations below 10 feet will fill first, failing the main feedwater system via the condensate pumps. Therefore, the demand for auxiliary feedwater will occur prior to flooding the equipment necessary to start the AFWS. Due to this assumption, the probability of failure to start of the AFWS is assumed to be equal to the probability used in the Reactor Safety Study.

2. Many of the failure events represented in the AFWS fault tree are assumed to be unaffected by submersion. These events include pipe ruptures, check valve failures and normally open manual valve failures. Also, components located inside the containment building are assumed to be isolated from the flood effects.

Applying these two assumptions resulted in the modified AFWS fault trees shown in Figures A.6 and A.7. Figure A.8 shows test and maintenance contributions to AFWS failures in the start to eight-hour time period. Appendix B contains the event code definitions. Appendix II of the Reactor Safety Study[1] contains a detailed discussion of the fault tree events represented in the fault trees.

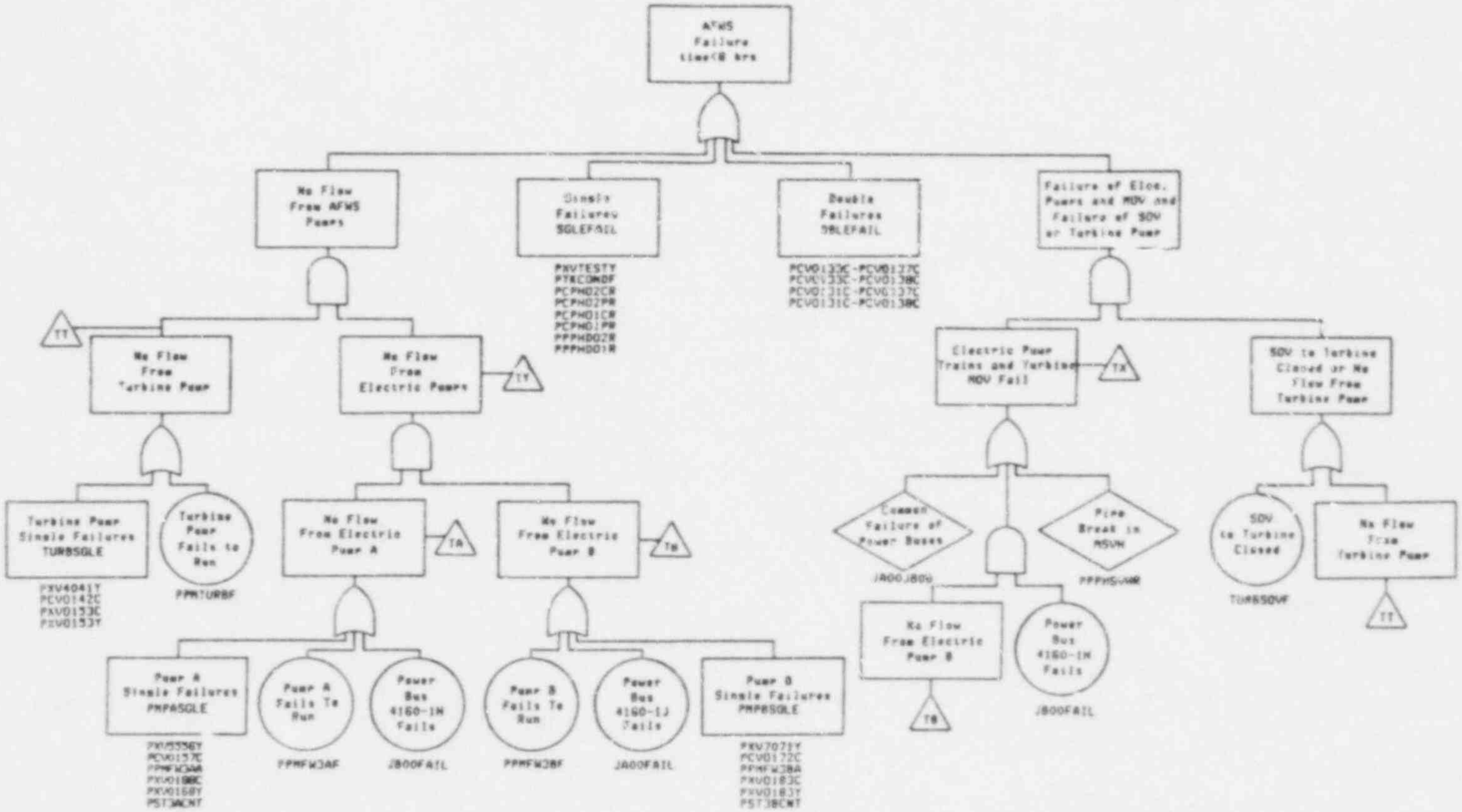

Figure A.6 Modified AFWS Fault Tree for the Time Period Start to 8 Hours

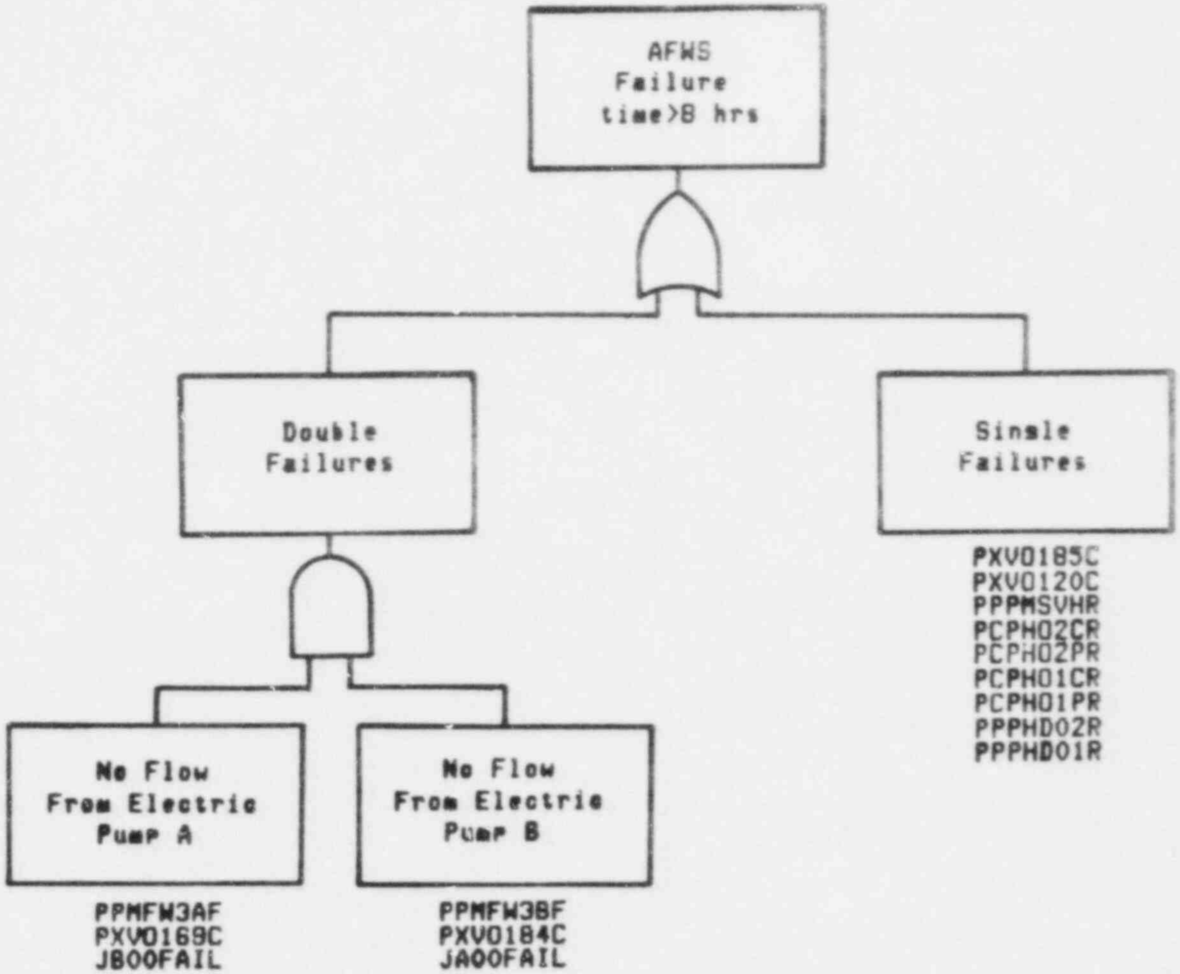

Figure A.7 Modified AFWS Fault Tree for the Time Period 8 to 24 Hours

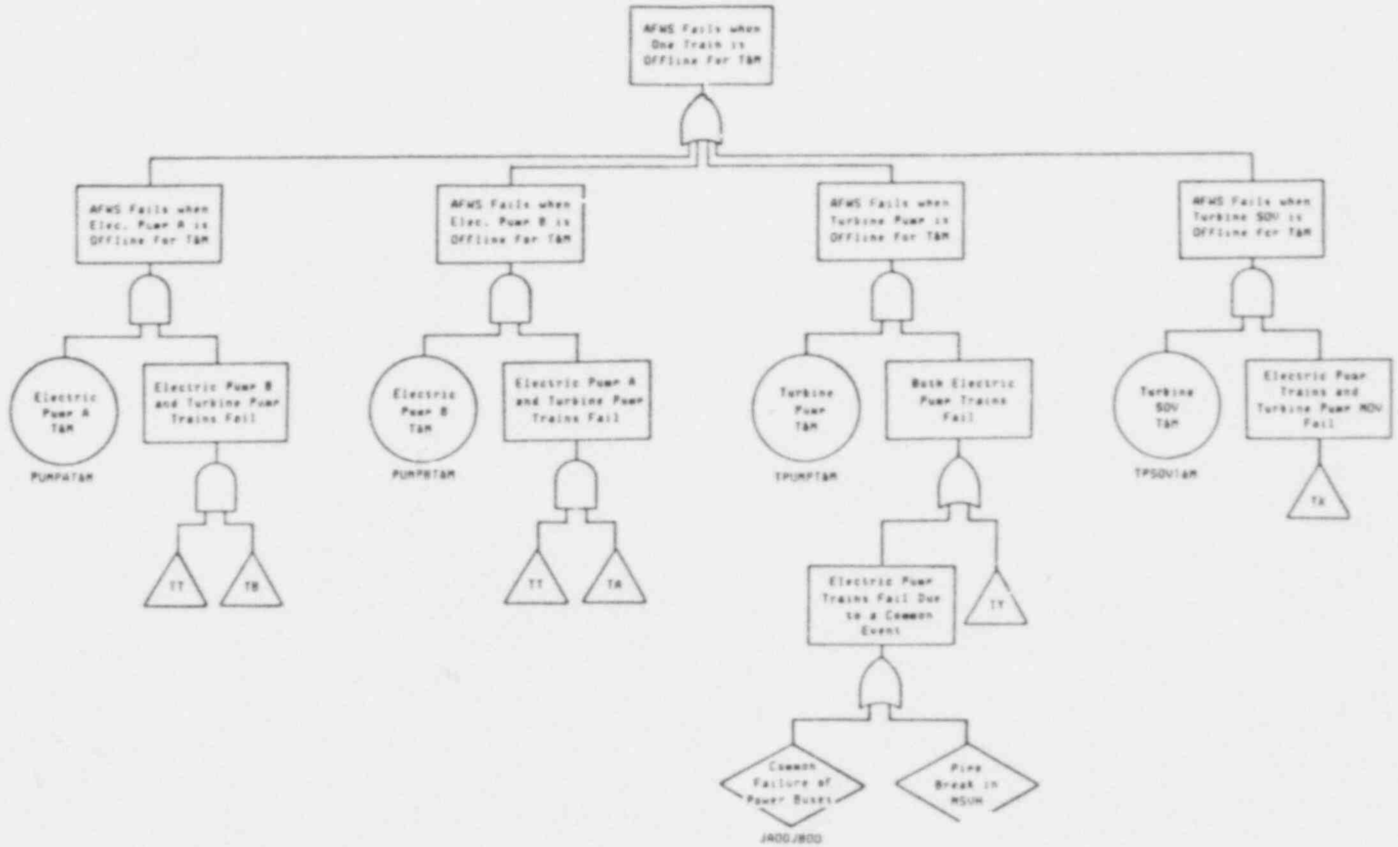

Figure A.8 Modified Fault Tree for AFWS Failure When One AFWS Train is Offline for Test and Maintenance

A.2.4 Electric Power System Fault Trees

The Nuclear Regulatory Commission also provided fault trees for the Surry Electric Power System for use in the Surry AFWS flood analysis. The AFWS interfaces with the electric power system. Failure of either 4160 volt AC bus (1H or 1J) will disable an electric pump. Failure of the 480 volt AC bus (1H) will fail the motor-operated valve which admits steam to the turbine. Failure of the 125 volt DC buses (1A or 1B) will each fail an electric pump control circuit.

The analysis evaluated the Electric Power System fault trees based on the postulated flood scenario at the Surry Plant and the assumptions made in modifying the AFWS fault trees. The results of the evaluation were:

1. Electric power is assumed to be unaffected by the flood at the time of demand for the AFWS. Therefore, electric power failures are adequately described by the failure probabilities presented in the Reactor Safety Study.

2. After AFWS has started, only 4160 volt AC buses (1H and 1J) are essential to operation of the AFWS. Since all electric power fails upon submersion of the relay room (internal elevation = 10 feet), detailed development of the faults that contribute to the failure of the 4160 volt AC buses is unnecessary. Therefore, the 4160 volt AC bus failures are incorporated directly into the AFWS fault trees as single events.

A.2.5 Vulnerability Elevations of AFWS Components

The "component vulnerability elevation" is defined as the lowest physical elevation that the flood level must surpass in order to affect the component. Most of the events contained in the AFWS fault trees experience no effects from submersion or are isolated from the flood (Section A.2.3). Those events that are expected to experience significant effects due to submersion are listed with their vulnerability elevation in Table A.2.

Table A.2 Vulnerability Flevations for AFWS Basic Events That Are Expected to Fa.l upon Submersion

Basic Event Code	Description	Vulnerability Elevation (Feet)
JAOOFAIL	Power Bus 4160-1J Fails	10
JBOOFAIL	Power Bus 4160-1H Fails	10
PPMTURBF	Turbine Pump Fails to Run	29
PPMFW3AF	Electric Pump A Fails to Run	29
PPMFW3BF	Electric Pump B Fails to Run	29

A.3 QUALITATIVE EVALUATION

The NOAH computer program(4) analyzed the modified AFWS fault trees using the flood level profile and component vulnerability elevations as input. The following sections discuss the results of this analysis.

A.3.1 Critical Flood Level

The critical flood level is defined as the flood level where the first flooded minimal cut set is found. This is the minimum flood level where the system failure of interest can be directly caused by the flood.

The critical flood level for the Surry AFWS in the time period from start to eight hours is 29 feet. The critical flood level in the time period exceeding eight hours is 10 feet. The reduction in the critical flood level results from the turbine-driven pump being unavailable for time periods exceeding eight hours because the steam supply to the turbine pump is exhausted.

A.3.2 Flooded Minimal Cut Sets

The analysis determined flooded minimal cut sets for the 10-foot flood and the 29-foot flood for both AFWS fault trees. The remaining minimal cut sets, that is, the minimal cut sets that contain at least one component that is unaffected by the flood, were also determined.

Table A.3 lists the flooded minimal cut sets for each fault tree. Appendix C contains a complete list of the minimal cut sets for the modified AFWS fault trees.

Table A.3 Flooded Minimal Cut Sets for the AFWS Analysis

AFWS Flood Level (feet)	Flooded Minimal Cut Sets
Start to 8 Hours	
>29	1. Turbine Pump, Electric Pump A and Electric Pump B Fail to Run.
	2. Turbine Pump and Electric Pump A Fail to Run and Power Bus 4160-1J Fails.
	3. Turbine Pump and Electric Pump B Fail to Run and Power Bus 4160-1H Fails.
	4. Turbine Pump Fails to Run and Power Buses 4160-1J and 4160-1H Fail.
8 to 24 Hours	
10	1. Power Buses 4160-1J and 4160-1H Fail.
>29	1. Electric Pump A and Electric Pump B Fail to Run.
	2. Power Bus 4160-1H Fails and Electric Pump B Fails to Run.
	3. Power Bus 4160-1J Fails and Electric Pump A Fails to Run.

A.4 QUANTITATIVE EVALUATION

The quantitative flood analysis involves estimating the AFWS failure probability for each flood level and incorporating the flooded AFWS failure probability into selected accident sequences that involved failure of the AFWS. This allows calculation of the flooded contribution to the total probability of each accident sequence.

This analysis considers only the dominant accident sequences that contain AFWS failure from the transient event tree in the Reactor Safety Study. Table A.4 lists these sequences with their failure probability as reported in the Reactor Safety Study. All these accident sequences result in core melt.

A.4.1 Assumptions

Assumptions made for the quantitative analysis include:

1. The emergency power buses (4160 volt AC, 1H and 1J), electric motor-driven AFWS pumps and the turbine-driven AFWS pump are failed with probability one upon submersion by the flood. While, in reality, the turbine-driven AFWS pump may continue to operate after submersion, the submersion of the pump represents an extreme environmental condition which would seriously degrade the pump's performance. Therefore, the turbine-driven pump is assumed failed upon submersion.

2. Components are assumed to be submerged at the minimum flood level that can affect the component.

3. The demand for AFWS is assumed to result from the failure of the condensate pumps as the flood water fills the lowest elevation in the turbine building. Therefore, no flood effects are considered in the AFWS probability of failure to start.

4. The flood is assumed to result in the initiating transient loss of main feedwater via failure of the condensate pumps. That is, the probability of the transient is one, given a flood greater than 27 feet above mean water level has occurred.

Table A.4 Transient Event Dominant Accident Sequences Considered in the Surry AFWS Flood Analysis

Accident Sequence*	Reactor Safety Study Probability Per Year Without Floods
TML-α	6×10^{-8}
TML-β	3×10^{-10}
TML-ϵ	6×10^{-6}
TMLB´-α	3×10^{-8}
TMLB´-γ	7×10^{-7}
TMLB´-δ	2×10^{-6}
TMLB´-ϵ	6×10^{-7}

* T - Transient Event

M - Failure of the Secondary System Steam Relief Valves and the Power Conversion System (Main Feedwater System)

L - Failure of the Secondary System Steam Relief Valves and the Auxiliary Feedwater System

B´ - Failure to Recover Either Onsite or Offsite Electric Power Within About 1 to 3 Hours Following an Initiating Transient Which is a Loss of Off-site AC Power

α - Containment Rupture Due to a Reactor Vessel Steam Explosion

β - Containment Failure Resulting from Inadequate Isolation of Containment Openings and Penetrations

γ - Containment Failure Due to Hydrogen Burning

δ - Containment Failure Due to Overpressure

ϵ - Containment Vessel Melt-Through

A.4.2 Failure Date

Appendix II of the Reactor Safety Study provided the failure probability estimates used in this study for the Auxiliary Feedwater System analysis. Appendix V provided the probabilities for quantifying the accident sequences. Therefore, all assumptions in the Reactor Safety Study that apply to the failure data are also applicable to this study. Appendix B lists these failure probabilities for the AFWS components.

A.4.3 Quantitative Results

A.4.3.1 Failure Flood Level

The failure flood level is defined as the minimum flood level where all the components in at least one minimal cut set are flooded and failed with probability one, resulting in a system failure probability of one. For the start to eight hours case, the failure flood level is 29 feet. For time periods exceeding eight hours, the failure flood level is 10 feet. The reduction in the failure flood level is due to the turbine-driven AFWS pump's being unavailable after eight hours.

A.4.3.2 AFWS Failure Probability

The analysis determined AFWS failure probabilities for two types of initiating transients. These transients are:

1. small pipe break and transients excluding loss of off-site power, and

2. loss of off-site power.

Table A.5 gives the AFWS failure probability from the Reactor Safety Study, which represents the system's unflooded state, and the values for the 10-foot and 29-foot floods calculated as part of the flood analysis for each initiating event. Once the flood has reached a level of 10 feet, the AFWS failure probabilities for the two types of initiating transients are equivalent. This is because loss of power occurs (both off-site and on-site) upon flooding the plant's relay room at a flood level of 10 feet.

A.4.4 Flood Effects on Accident Sequence Probability

The analysis determined individual accident sequence probabilities as a function of flood probability. Two cases are analyzed for each of the flood levels considered.

Table A.5 AFWS Failure Probabilities

		Failure Probability (Per Year)		
Initiating Event	Time Period	Unflooded (Reactor Safety Study)	10-Foot Flood	>29-Foot Flood
Small Pipe Break and Transients excluding Loss of Off-site Power	Start to 8 Hours	3.7×10^{-5}	2.2×10^{-2}	1.0
	8 to 24 Hours	1.2×10^{-3}	1.0	1.0
Loss of Off-site Power	Start to 8 Hours	1.5×10^{-4}	2.2×10^{-2}	1.0
	8 to 24 Hours	3.8×10^{-3}	1.0	1.0

1. Best case - Only flood effects on the AFWS were incorporated into the accident sequence probability. All other contributors, except the transient event probability, were held constant at their Reactor Safety Study values.

2. Worst case - In addition to the flood effects on the AFWS, events M and B' were assumed failed with probability one by the flood. The M event is non-recovery of the main feedwater system, and the B' event is nonrecovery of offsite electric power.

For both cases, the transient initiating event was assumed to occur with probability one given the flood had occurred. Also, the analysis considers no flood effects on the containment failure mode probabilities; therefore, these probabilities are held constant at their Reactor Safety Study values.

Figures A.9 and A.10 show results of these evaluations. These figures show the core melt probability per year due to floods (the sum of the individual sequence probabilities due to floods) as a function of flood probability for the 10-foot and greater than 29-foot floods. Appendix D gives the results for the individual accident sequences. Each graph is marked to indicate the flood doubling probability. The flood doubling probability is the flood probability that results in an accident sequence probability, due to floods, that is equal to the accident sequence probability reported in the Reactor Safety Study; thereby, doubling the total accident sequence probability. For example, consider the best case curve shown in Figure A.9. The flood doubling probability for the 10-foot flood is 1.36×10^{-3} per year. At this flood probability, the total core melt probability is 1.88×10^{-5} per year, 50% (9.4×10^{-6}) of which is due to the flood effects.

Figures A.11 and A.12 show the flood effects on the total core melt probability due to the dominant transient event accident sequences for the 10-foot and greater than 29-foot floods, respectively. These curves give the total core melt probability due to transients as a function of flood probability. The total core melt probability includes only the dominant transient event accident sequences identified in the Reactor Safety Study. The flood effects contribution is the result of the dominant transient accident sequences that involved failure of the AFWS (7 of 12 dominant transient sequences involve the AFWS).

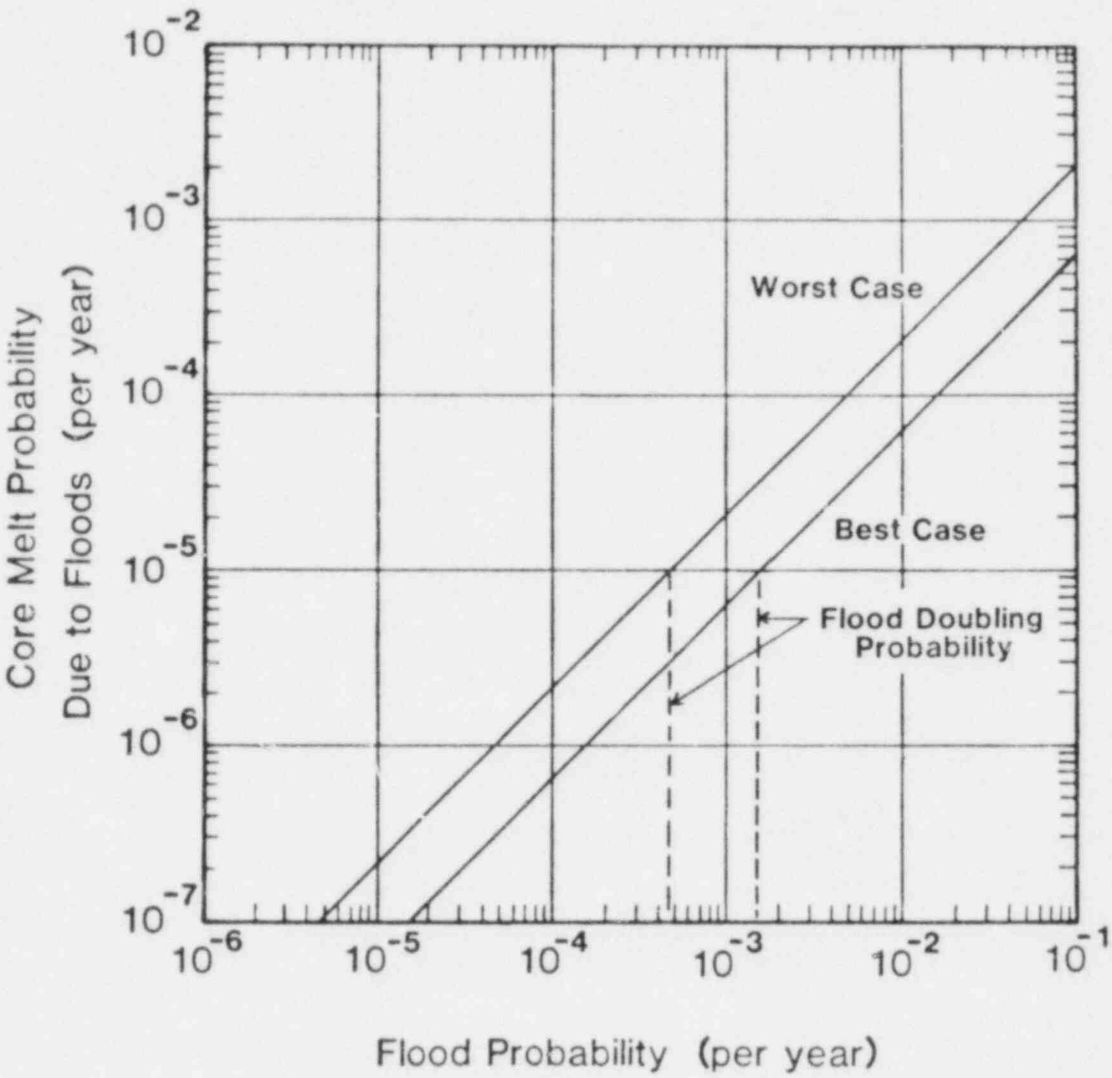

Figure A.9 Core Melt Probability (per year) Due to Flood Effects on the Dominant Transient Accident Sequences Involving the AFWS as a Function of Flood Probability for the 10-Foot Flood at the Surry Power Station

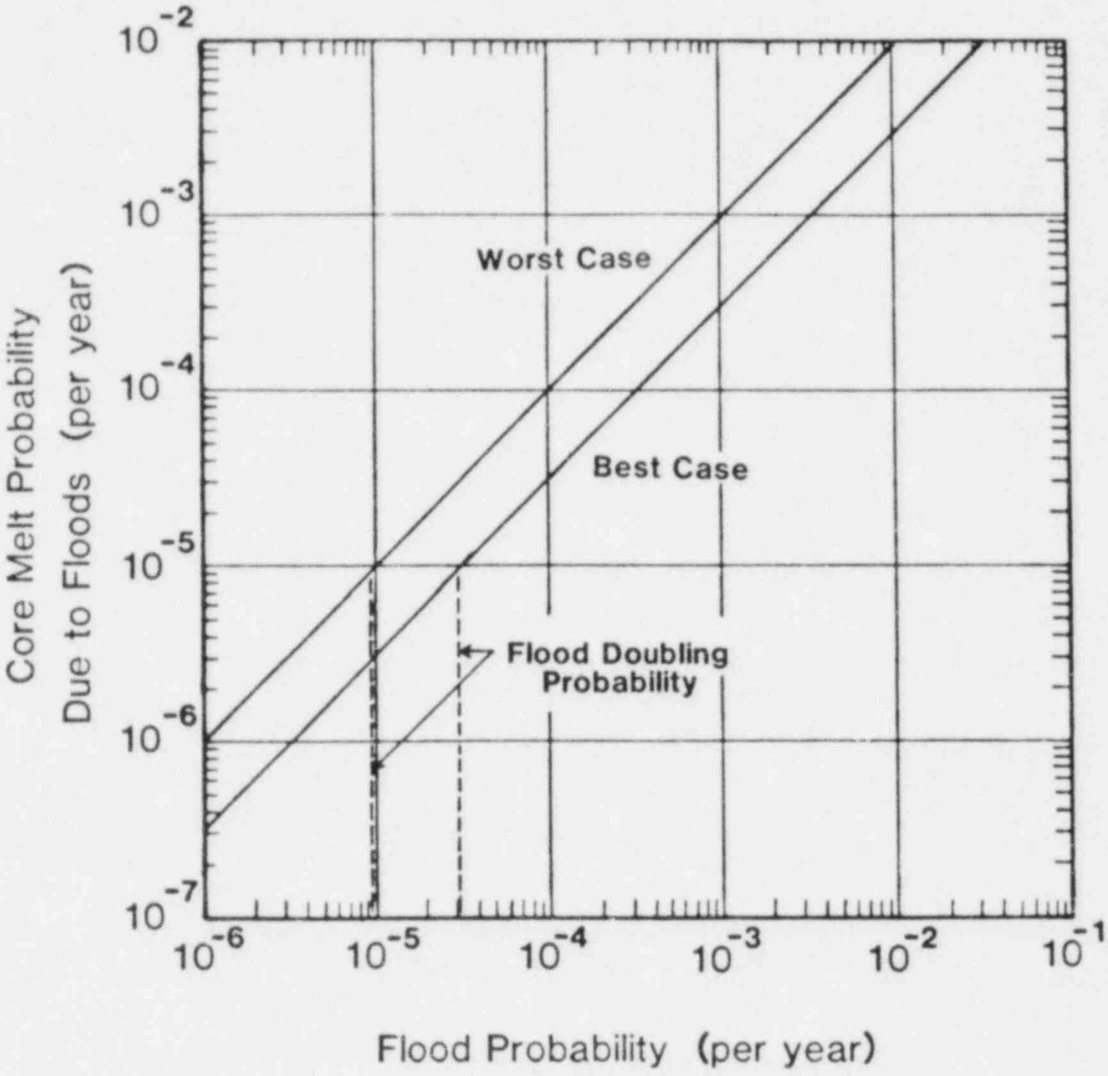

Figure A.10 Core Melt Probability (per year) Due to Flood Effects on the Dominant Transient Accident Sequences Involving the AFWS as a Function of Flood Probability for the Greater Than 29-Foot Flood at the Surry Power Station

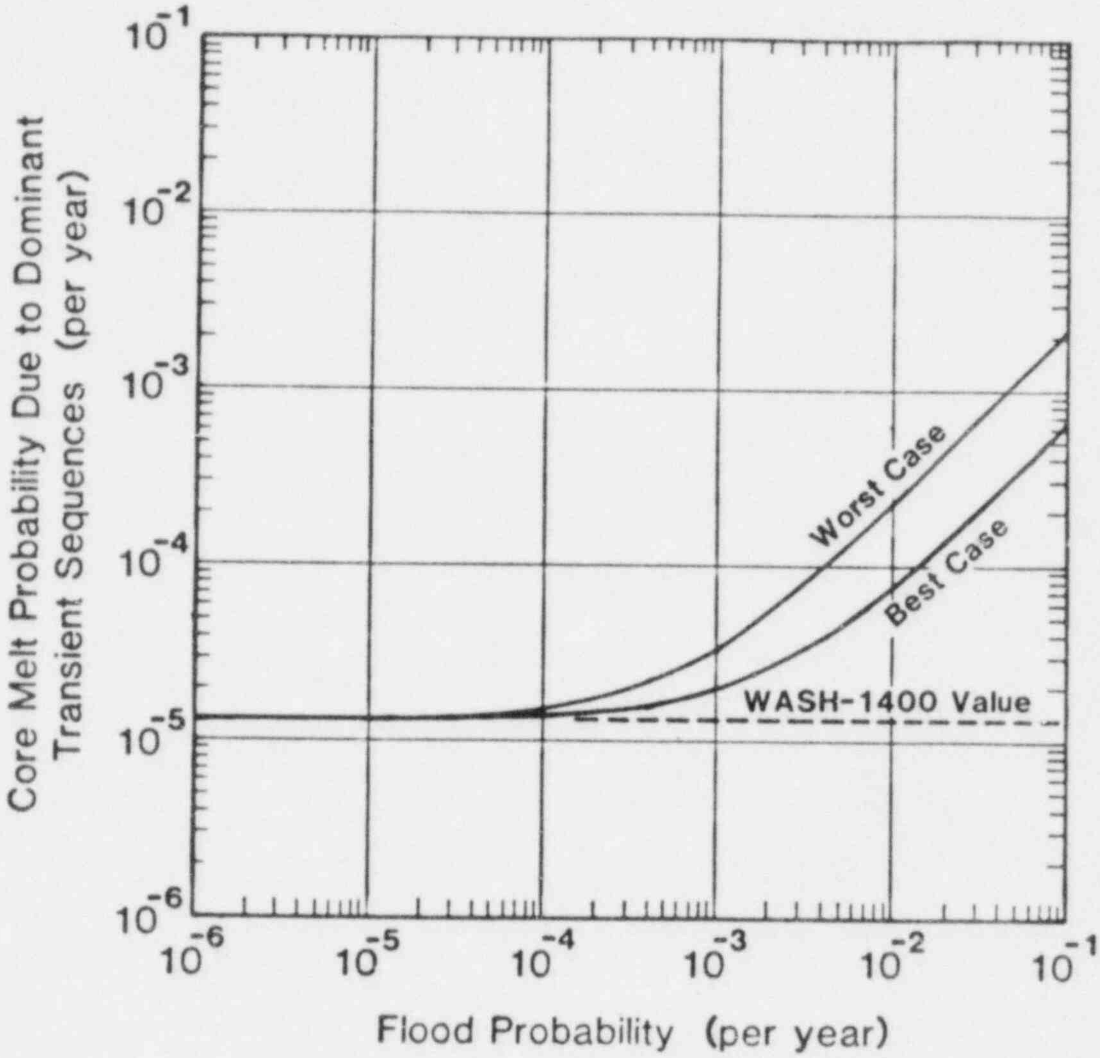

Figure A.11 Core Melt Probability (per year) Due to the Dominant Transient Event Accident Sequences, Including the Effects of the 10-Foot Flood on the AFWS, as a Function of Flood Probability

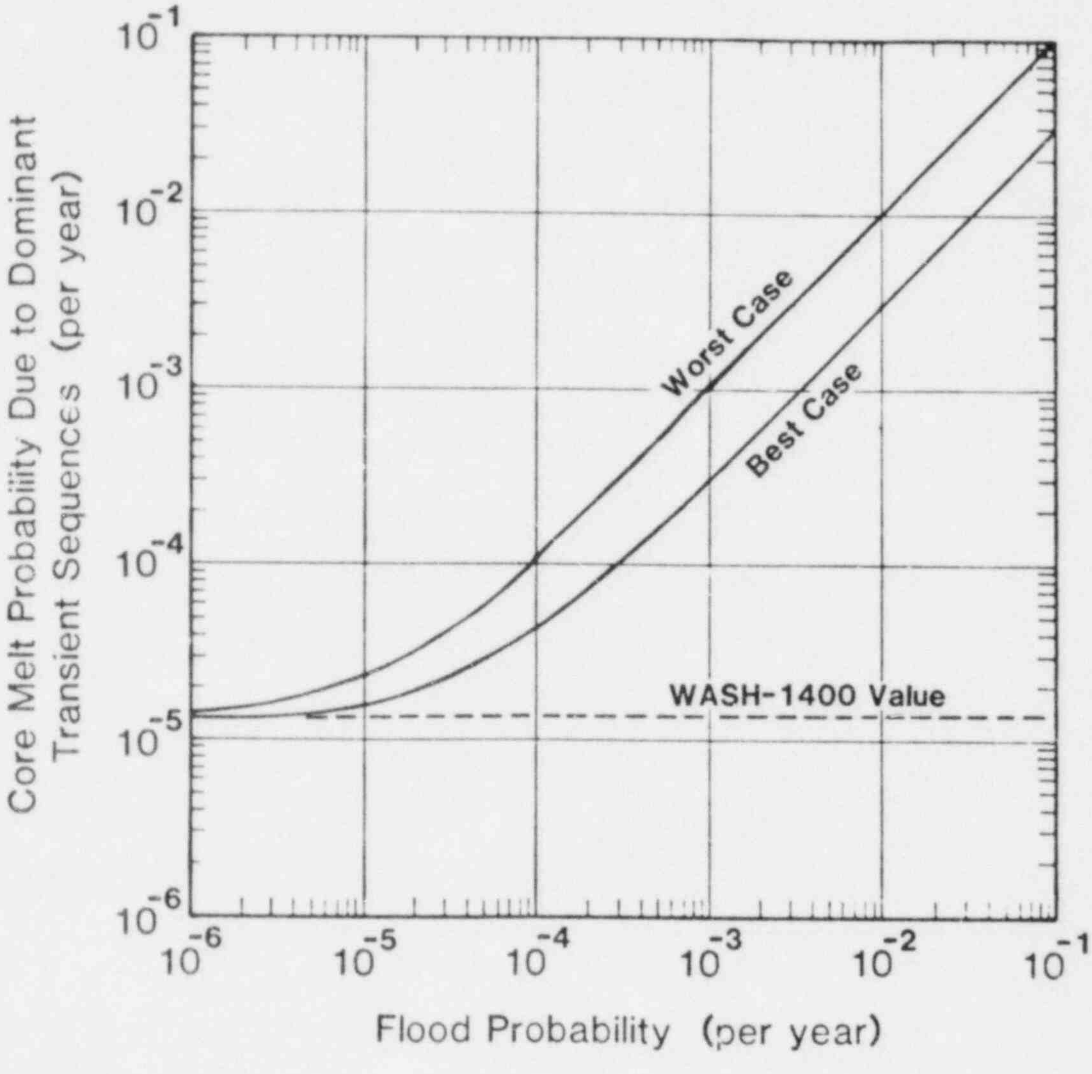

Figure A.12 Core Melt Probability (per year) Due to the Dominant Transient Event Accident Sequences, Including the Effects of the Greater Than 29-Foot Flood on the AFWS, as a Function of Flood Probability

APPENDIX B

BASIC EVENT DESCRIPTIONS

AND DATA FOR

THE SURRY AFWS FLOOD ANALYSIS

Table B.1 AFWS Basic Event Descriptions and Data for the Time Period Start to 8 Hours

Basic Event Code	Basic Event Description	Vulnerability Elevation	Unflooded Failure Probability	Flooded Failure Probability
JA00JB00	Common Failure of Power Buses	10	$1x10^{-2}$*	1.0
JB00FAIL	Power Bus 4160-1H Fails	10	$3.7x10^{-2}$*	1.0
JA00FAIL	Power Bus 4160-1J Fails	10	$3.7x10^{-2}$*	1.0
PPMTURBF	Turbine Pump Fails to Run	29	$1x10^{-3}$	1.0
PPMFW3AF	Electric Pump A Fails to Run	29	$2.4x10^{-4}$	1.0
PPMFW3BF	Electric Pump B Fails to Run	29	$2.4x10^{-4}$	1.0
TURBSOVF	Solenoid Operated Valve to Turbine Closed	NA**	$1x10^{-3}$	NA**
SGLEFAIL ***	Single Failures	NA	$3.05x10^{-5}$	NA
PXVTESTY	All Normally Open Manual Valves Closed for Pump Test are Inadvertently Left Closed	NA	$3x10^{-5}$	NA
PTKCONDF	COND TK (1-CN-TK-1) Does Not Supply Water	NA	$3.6x10^{-8}$	NA
PCPH02CR	Weld Cap on End of No. 2 Header (Cont. Side) Comes Off	NA	$1x10^{-7}$	NA
PCPH02PR	Weld Cap on End of No. 2 Header (MSVH Side) Comes Off	NA	$1x10^{-7}$	NA

Table B.1 Continued

Basic Event Code	Basic Event Description	Vulnerability Elevation	Unflooded Failure Probability	Flooded Failure Probability
PCPH01CR	Weld Cap on End of No. 1 Header (Cont. Side) Comes Off	NA	$1x10^{-7}$	NA
PCPH01PR	Weld Cap on End of No. 1 Header (MSVH Side) Comes Off	NA	$1x10^{-7}$	NA
PPPHD02R	No. 2 6" Header Ruptures	NA	$3.6x10^{-8}$	NA
PPPHD01R	No. 1 6" Header Ruptures	NA	$3.6x10^{-8}$	NA
DBLEFAIL	Double Failures	NA	$4x10^{-8}$	NA
PCV0133C	Check Valve 133 in Header No. 1 Fails Closed on Demand	NA	$1x10^{-4}$	NA
PCV0131C	Check Valve 131 in Header No. 1 Fails Closed on Demand	NA	$1x10^{-4}$	NA
PCV0137C	Check Valve 137 in Header No. 2 Fails Closed on Demand	NA	$1x10^{-4}$	NA
PCV0138C	Check Valve 138 in Header No. 2 Fails Closed on Demand	NA	$1x10^{-4}$	NA

Table B.1 Continued

Basic Event Code	Basic Event Description	Vulnerability Elevation	Unflooded Failure Probability	Flooded Failure Probability
TURBSGLE	Turbine Pump Single Failures	NA	$6.2x10^{-3}$	NA
PXV4041Y	Turbine Pump Manual Valve 4041 Does Not Open	NA	$3x10^{-3}$	NA
PCV0142C	Turbine Pump Check Valve 142 Closed	NA	$1x10^{-4}$	NA
PXV0153C	Turbine Pump Manual Valve 153 Closes	NA	$1x10^{-4}$	NA
PXV0153Y	Turbine Pump Manual Valve 153 Not Open	NA	$3x10^{-3}$	NA
PPPMSVHR	Pipe Break in MSVH	NA	$7.5x10^{-5}$	NA
PMPASGLE	Electric Pump A Single Failures	NA	$1.09x10^{-2}$	NA
PXV5556Y	Electric Pump A Manual Valve 5556 Not Open	NA	$3x10^{-3}$	NA
PCV0157C	Electric Pump A Check Valve 157 Closed	NA	$1x10^{-4}$	NA
PPMFW3AA	Electric Pump A Fails to Start	NA	$1x10^{-3}$	NA
PXV0168C	Electric Pump A Manual Valve 168 Closes	NA	$1x10^{-4}$	NA
PXV0168Y	Electric Pump A Manual Valve 168 Not Open	NA	$3x10^{-3}$	NA

Table B.1 Continued

Basic Event Code	Basic Event Description	Vulnerability Elevation	Unflooded Failure Probability	Flooded Failure Probability
PST3ACNT	Electric Pump A Control Circuit Fails	NA	3.7×10^{-3}	NA
PMPBSGLE	Electric Pump B Single Failures	NA	1.09×10^{-2}	NA
PXV7071Y	Electric Pump B Manual Valve 7071 Not Open	NA	3×10^{-3}	NA
PCV0172C	Electric Pump B Check Valve 172 Closed	NA	1×10^{-4}	NA
PPMFW3BA	Electric Pump B Fails to Start	NA	1×10^{-3}	NA
PXV0183C	Electric Pump B Manual Valve 183 Closes	NA	1×10^{-4}	NA
PXV0183Y	Electric Pump B Manual Valve 183 Not Open	NA	3×10^{-3}	NA
PST3BCNT	Electric Pump B Control Circuit Fails	NA	3.7×10^{-3}	NA
PUMPAT&M	Electric Pump A Test and Maintenance	NA	7.9×10^{-3}	NA
PUMPBT&M	Electric Pump B Test and Maintenance	NA	7.9×10^{-3}	NA

Table B.1 Continued

Basic Event Code	Basic Event Description	Vulnerability Elevation	Unflooded Failure Probability	Flooded Failure Probability
TPSOVT&M	Solenoid Operated Valve to Turbine Test and Maintenance	NA	5.8×10^{-3}	NA
TPUMPT&M	Turbine Pump Test and Maintenance	NA	7.9×10^{-3}	NA

* This basic event is considered only for the initiating transient Loss of Offsite Power. Its contribution is negligible for the Small Pipe Break transients.

** NA signifies that the basic event is either unaffected by submersion or isolated from the flood. Therefore, no vulnerability elevation or flooded failure probability is required.

*** The basic events contained within the bracket were represented throughout the analysis by the event name immediately preceding the bracket.

Table B.2 AFWS Basic Event Descriptions and Data for the Time Period 8 to 24 Hours

Basic Event Code	Basic Event Description	Vulnerability Elevation	Unflooded Failure Probability	Flooded Failure Probability
JBOOFAIL	Power Bus 4160-1H Fails	10	4.8×10^{-2}*	1.0
JAOOFAIL	Power Bus 4160-1J Fails	10	4.8×10^{-2}*	1.0
PPMFW3AF	Electric Pump A Fails to Run	29	2.4×10^{-4}	1.0
PPMFW3BF	Electric Pump B Fails to Run	29	2.4×10^{-4}	1.0
PXV0169C	Manual Valve 169 Closed	NA**	5.4×10^{-4}	NA**
PXV0184C	Manual Valve 184 Closed	NA	5.4×10^{-4}	NA
PXV0185C	Manual Valve 185 Closed	NA	5.4×10^{-4}	NA
PXV0120C	Manual Valve 120 Closed	NA	5.4×10^{-4}	NA
PPPMSVHR	Pipe break in MSVH	NA	7.5×10^{-5}	NA
PCPH02CR	Weld Cap on End of No. 2 Header (Cont. Side) Comes Off	NA	1×10^{-7}	NA
PCPH02PR	Weld Cap on End of No. 2 Header (MSVH Side) Comes Off	NA	1×10^{-7}	NA
PCPH01CR	Weld Cap on End of No. 1 Header (Cont. Side) Comes Off	NA	1×10^{-7}	NA

Table B.2 Continued

Basic Event Code	Basic Event Description	Vulnerability Elevation	Unflooded Failure Probability	Flooded Failure Probability
PCPH01PR	Weld Cap on End of No. 1 Header (MSVH Side) Comes Off	NA	1×10^{-7}	NA
PPPHD02R	No. 2 6" Header Ruptures	NA	3.6×10^{-8}	NA
PPPHD01R	No. 1 6" Header Ruptures	NA	3.6×10^{-8}	NA

* See footnote to Table B.1.
** See footnote to Table B.1.

APPENDIX C

MINIMAL CUT SETS

FOR THE

AFWS MODIFIED FAULT TREES

Table C.1 Minimal Cut Sets for the AFWS for the Time Period Start to 8 Hours

AFWS Flood Level (Feet)	Minimal Cut Sets		
>29	PPMTURBF	PPMFW3AF	PPMFW3BF
	PPMFW3BF	PPMTURBF	JBOOFAIL
	PPMTURBF	PPMFW3AF	JAOOFAIL
	PPMTURBF	JBOOFAIL	JAOOFAIL
NA*	SGLEFAIL		
	DBLEFAIL		
	PPPMSVHR	TURBSGLE	
	PPPMSVHR	TURBSOVF	
	PPPMSVHR	PPMTURBF	
	TURBSGLE	PMPASGLE	PPMFW3BF
	PPMFW3BF	TURBSGLE	JBOOFAIL
	PPMTURBF	PMPASGLE	PPMFW3BF
	TURBSGLE	PPMFW3AF	PPMFW3BF
	TURBSGLE	PMPASGLE	JAOOFAIL
	TURBSGLE	PMPASGLE	PMPBSGLE
	PMPBSGLE	TURBSOVF	JBOOFAIL
	PPMTURBF	PMPASGLE	JAOOFAIL
	PPMTURBF	PMPASGLE	PMPBSGLE
	TURBSGLE	PPMFW3AF	JAOOFAIL
	TURBSGLE	PPMFW3AF	PMPBSGLE
	TURBSGLE	JBOOFAIL	JAOOFAIL
	TURBSGLE	JBOOFAIL	PMPBSGLE
	PPMTURBF	PPMFW3AF	PPMBSGLE
	PPMTURBF	JBOOFAIL	PMPBSGLE
	PPMFW3BF	TURBSOVF	JBOOFAIL
	JAOOFAIL	TURBSOVF	JBOOFAIL

* NA - At least one basic event in the minimal cut set is not affected by submersion or is not submerged by the flood.

Table C.2 Minimal Cut Sets for the AFWS for the Time Period 8 to 24 Hours

AFWS Flood Level (Feet)	Minimal Cut Sets	
10	JBOOFAIL	JAOOFAIL
>29	PPMFW3AF	PPMFW3BF
	JBOOFAIL	PPMFW3BF
	PPMFW3AF	JAOOFAIL
NA*	PXV0185C	
	PPPMSVHR	
	PCPH02CR	
	PCPH02PR	
	PCPH01CR	
	PCPH01PR	
	PPPHD02R	
	PPPHD01R	
	PXV0120C	
	PXV0169C	PPMFW3BF
	PPMFW3AF	PXV0184C
	PXV0169C	PXV0184C
	PXV0169C	JAOOFAIL
	JBOOFAIL	PXV0184C

* NA - At least one basic event in the minimal cut set is not affected by submersion or is not submerged by the flood.

Table C.3 Minimal Cut Sets for the AFWS Test and Maintenance Fault Tree

1.	PPPMSVHR	TPSOVT&M	
2.	PPPMSVHR	TPUMPT&M	
3.	PPMTURBF	PUMPBT&M	PPMFW3AF
4.	PPMTURBF	PUMPBT&M	JBOOFAIL
5.	JAOOFAIL	TPSOVT&M	JBOOFAIL
6.	PMPBSGLE	TPSOVT&M	JBOOFAIL
7.	PPMFW3AF	TPUMPT&M	PPMFW3BF
8.	JBOOFAIL	TPUMPT&M	PPMFW3BF
9.	PMPASGLE	TPUMPT&M	JAOOFAIL
10.	PMPASGLE	TPUMPT&M	PMPBSGLE
11.	PPMFW3AF	TPUMPT&M	JAOOFAIL
12.	PPMFW3AF	TPUMPT&M	PMPBSGLE
13.	JBOOFAIL	TPUMPT&M	JAOOFAIL
14.	JBOOFAIL	TPUMPT&M	PMPBSGLE
15.	PPMTURBF	PUMPAT&M	PPMFW3BF
16.	TURBSGLE	PUMPAT&M	JAOOFAIL
17.	TURBSGLE	PUMPAT&M	PMPBSGLE
18.	PPMTURBF	PUMPBT&M	PMPASGLE
19.	TURBSGLE	PUMPBT&M	PPMFW3AF
20.	TURBSGLE	PUMPBT&M	JBOOFAIL
21.	PPMFW3BF	TPSOVT&M	JBOOFAIL
22.	PMPASGLE	TPUMPT&M	PPMFW3BF
23.	PPMTURBF	PUMPAT&M	JAOOFAIL
24.	PPMTURBF	PUMPAT&M	PMPBSGLE
25.	TURBSGLE	PUMPBT&M	PMPASGLE
26.	TURBSGLE	PUMPAT&M	PPMFW3BF

APPENDIX D

GRAPHS OF THE INDIVIDUAL ACCIDENT SEQUENCE RESULTS AS A FUNCTION OF FLOOD PROBABILITY FOR THE SURRY AFWS FLOOD ANALYSIS

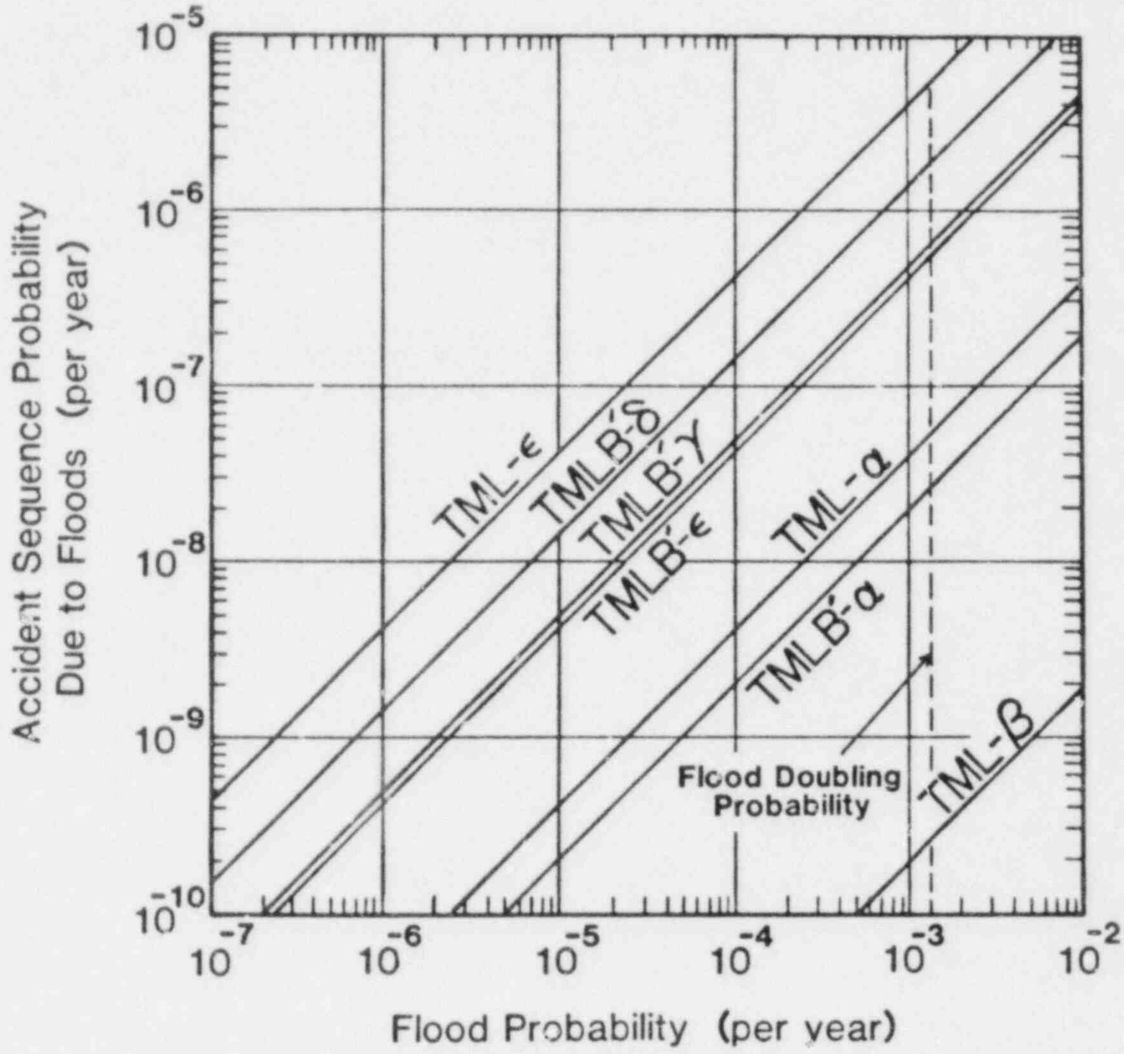

Figure D.1 Accident Sequence Probability Due to the Effects of the 10-Foot AFWS Flood as a Function of Flood Probability, Best Case

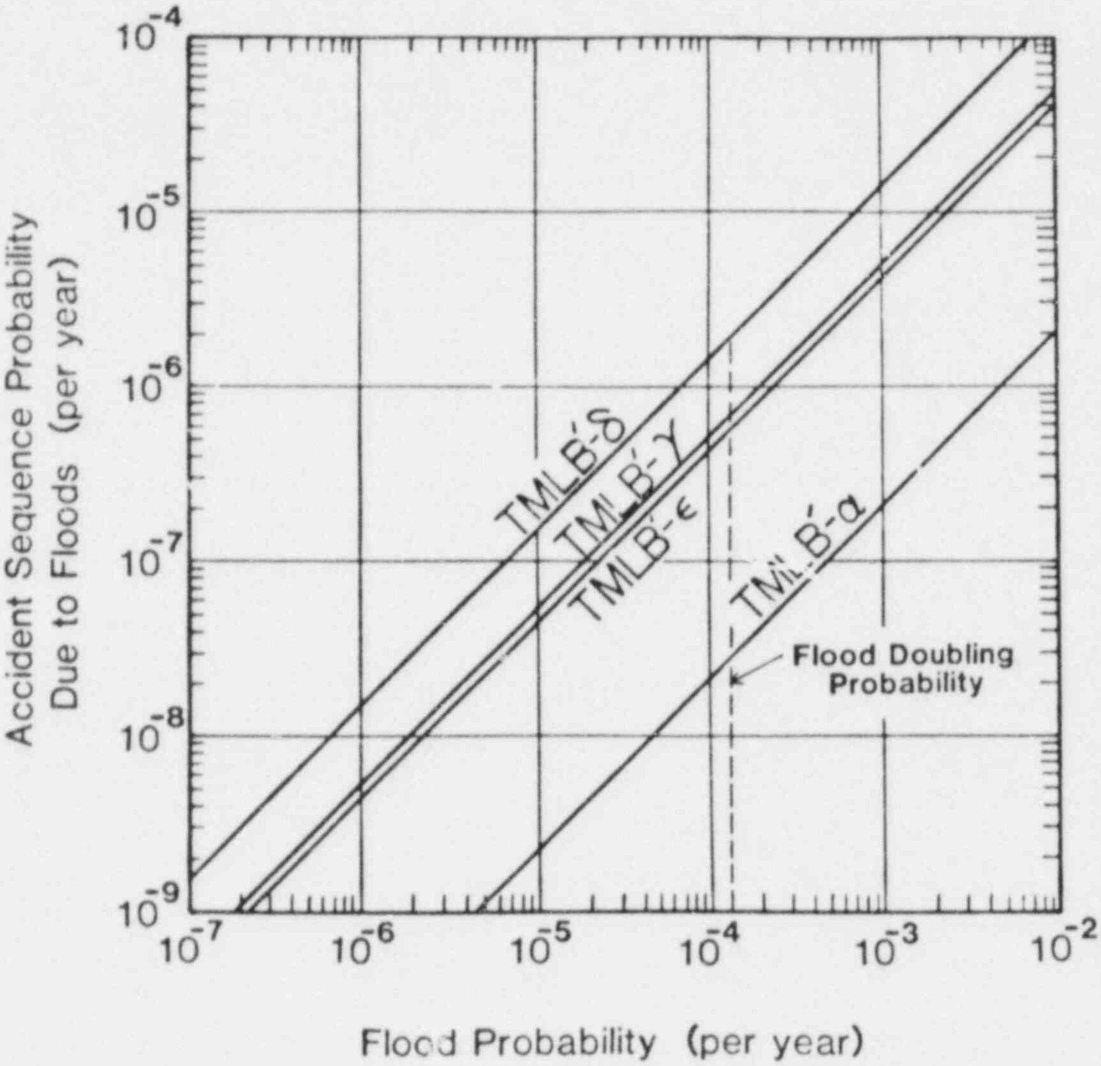

Figure D.2 Accident Sequence Probability Due to the Effects of the 10-Foot AFWS Flood as a Function of Flood Probability, Worst Case

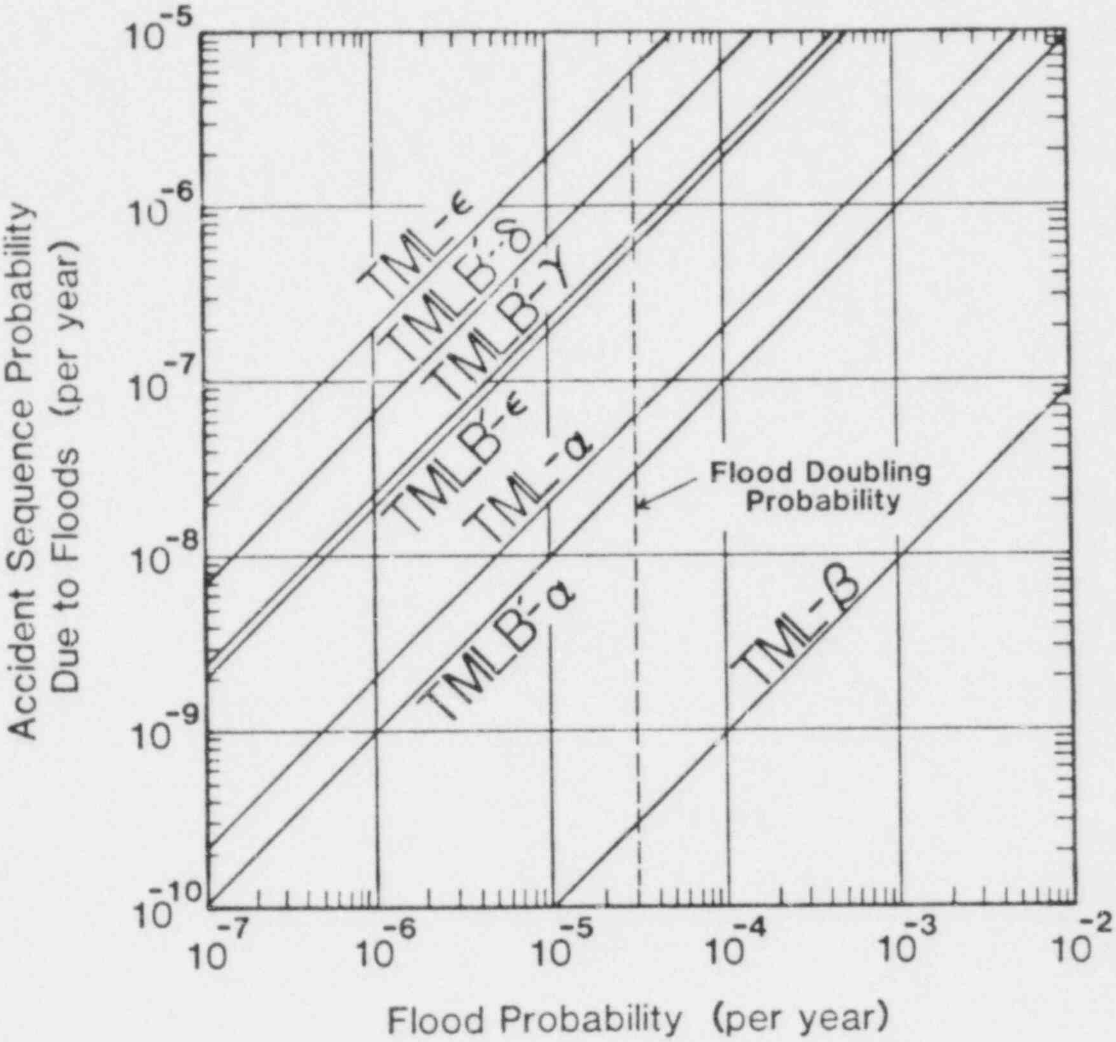

Figure D.3 Accident Sequence Probability Due to the Effects of the Greater Than 29-Foot AFWS Flood as a Function of Flood Probability, Best Case

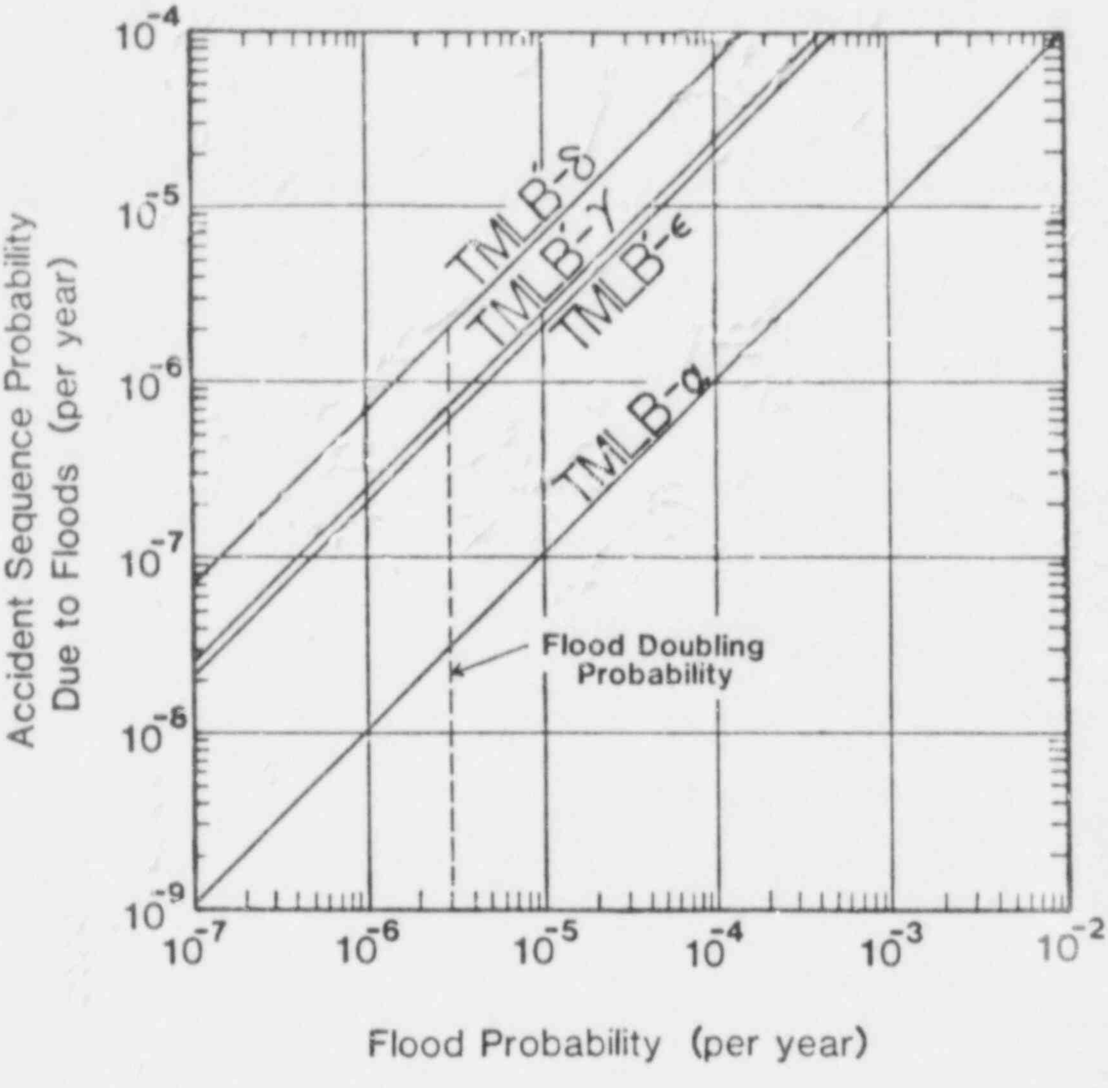

Figure D.4 Accident Sequence Probability Due to the Effects of the Greater Than 29-Foot AFWS Flood as a Function of Flood Probability, Worst Case

APPENDIX E

ANALYSIS OF AN INTERNAL

FLOOD SOURCE AT THE

SURRY POWER STATION

E.1 INTRODUCTION

This appendix describes the second example application of the flood risk analysis methodology. This example differs from the first analysis (Appendix A) in that the flood considered is the result of an internal source rather than an external source. Also, the flood risk analysis methodology is more fully developed as a result of FY81 tasks.

The analysis centers on the Surry Power Station so that information from the results of the pressurized water reactor (PWR) evaluation presented in the Reactor Safety Study[1] can be used. The Surry Power Station is the PWR plant in the Reactor Safety Study. The Nuclear Regulatory Commission provided additional plant design information and layout diagrams for the Surry Power Station.

The analysis makes no attempt to quantify the probability of the flood considered although the analysis identifies a specific flood source. Instead, a range of flood probab'lities are considered, and the results are presented as a function of the flood probability.

E.2 PROBLEM DESCRIPTION

This section describes the internal flood scenario at the Surry Plant and the systems affected by the flood. Appendix A (Section A.2.2) gives a general description of the Surry Plant site and the plant layout.

E.2.1 Flood Source

This analysis considers the effects of an internal flood source on the results of the Reactor Safety Study's PWR risk assessment. The internal flood source considered here is a main steam or feedwater pipe rupture in the main steam valve housing (MSVH) area of the Surry Power Station. The Reactor Safety Study identifies this event as a potential source of component failure due to flooding or extreme environment.

E.2.2 Systems Affected

The analysis considers three separate systems susceptible to potential flood damage from the postulated pipe rupture in the MSVH. These systems are:

- the Main Feedwater System,
- the Auxiliary Feedwater System, and
- the Containment Spray Injection System.

E.2.2.1 Main Feedwater System

The analysis considers the Main Feedwater System susceptible to the postulated internal flood source. This susceptibility is due to the assumption that the pipe rupture involves a main steam or feedwater line, rather than flooding of Main Feedwater System components. For this reason, the analysis assumes that the Main Feedwater System is failed for the duration of the event.

E.2.2.2 Auxiliary Feedwater System

All three Auxiliary Feedwater System (AFWS) pumps reside in the MSVH area and are exposed to the effects of the postulated flood event. The analysis assumes that all electrical components in the MSVH fail due to the flood. This results in the AFWS's being totally dependent on the turbine-driven pump train of the system. Appendix A (Section A.2.1) contains a description of the AFWS.

E.2.2.3 Containment Spray Injection System

The analysis considers the Containment Spray Injection System (CSIS) susceptible to the postulated flood because the two containment spray pumps are located in a room adjoining the AFWS pump room (Figure E.1). A doorway joins the two pump rooms and provides a degree of protection to the CSIS pumps if the door is secured. The analysis considers a range of effects on the CSIS pumps.

The principal function of the Containment Spray Injection System is to reduce the pressure of the containment by delivering cold water through spray heads to the containment volume. The CSIS consists of two essentially identical subsystems, each fully capable of delivering sufficient spray to the containment. Both subsystems draw suction from the refueling water storage tank (RWST) and are required to operate only until the water supply in the RWST is exhausted. Figure E.2 is a simplified flow diagram of the CSIS.

E.2.2.4 Internal Flood Scenario

This analysis considers a variety of flood effects arising from the flood effects of the postulated pipe rupture in the MSVH area. Three specific cases are defined for analysis. These cases are:

- Case A - Only Main and Auxiliary Feedwater Systems equipment receive damage due to the flood event. Case A assumes that the Containment Spray Injection System is fully protected from the flood.

- Case B - In addition to the flood effects to the Main and Auxiliary Feedwater Systems, Case B assumes flood damage to one of the two CSIS pumps.

- Case C - Case C assumes flood damage to both CSIS pumps, in addition to Main and Auxiliary Feedwater System failure.

The following sections describe the analysis of these three internal flood scenarios.

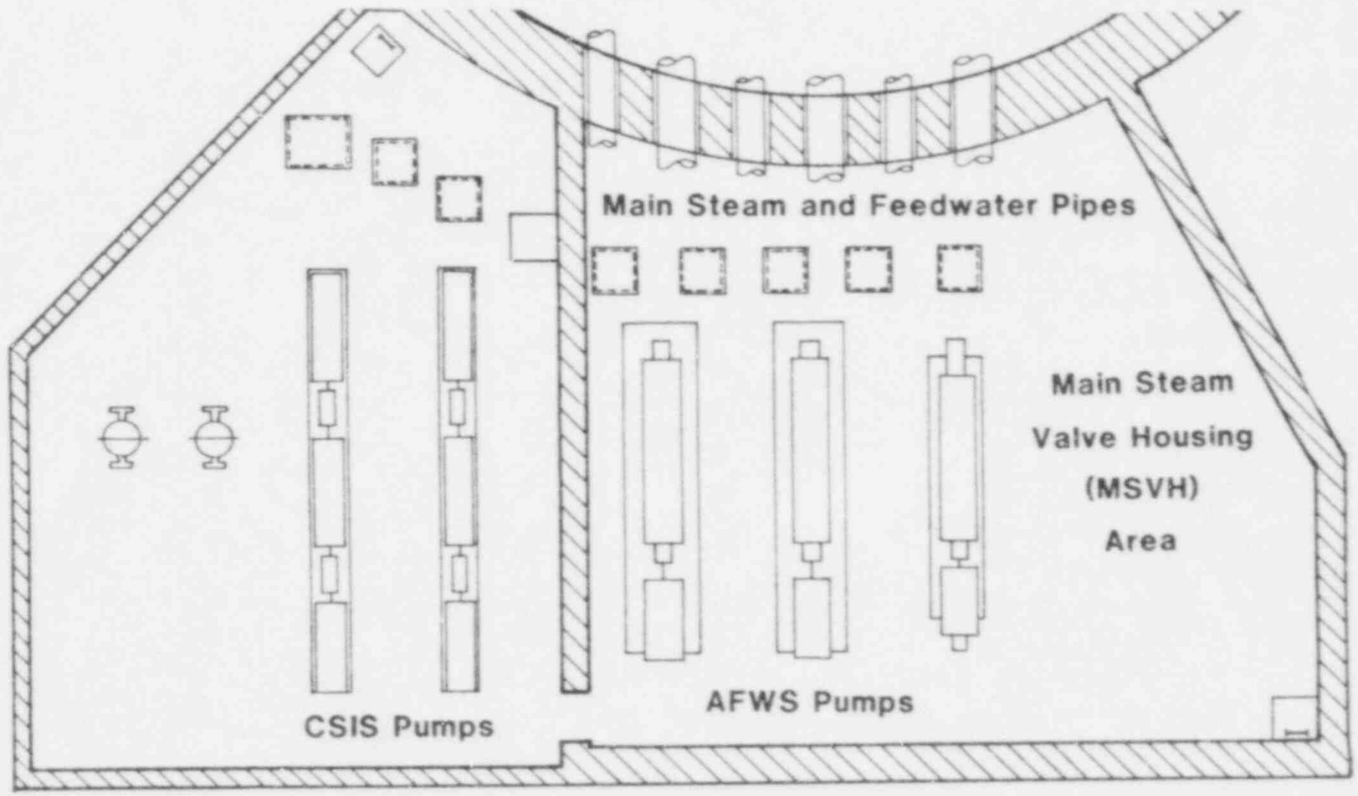

Figure E.1 Main Steam Valve Housing (MSVH) Area Showing CSIS and AFWS Pump Locations

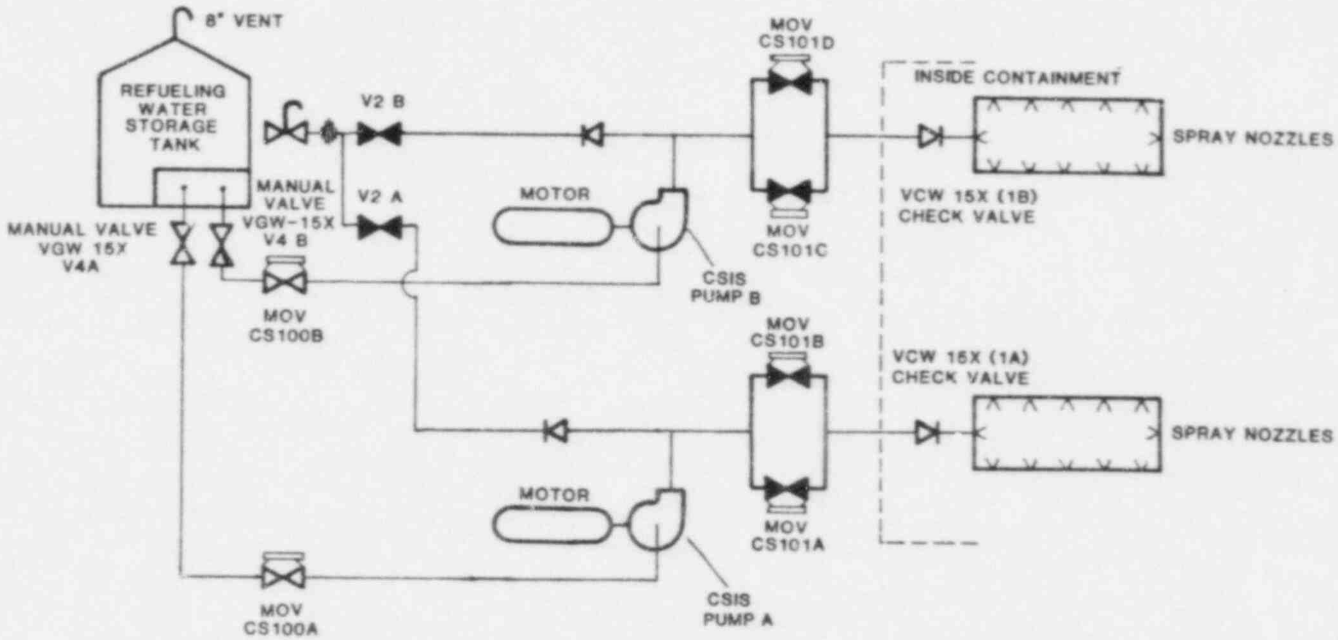

Figure E.2 Surry CSIS Simplified Flow Diagram

E.3 ACCIDENT SEQUENCE SCREENING

The analysis used the ESP computer program[4] to screen all accident sequences from the Reactor Safety Study event trees for significance in the event of the postulated flood. The ESP computer program screens accident sequences within a consequence category to determine potentially significant accident sequences for further analysis. The analysis screening criterion is five percent of the consequence category's occurrence frequency for each type of initiating event (transient, small LOCA, etc.). That is, any accident sequence that has a potential flooded occurrence frequency greater than five percent of its consequence category occurrence frequency is identified as a potentially significant accident sequence. The flood probability chosen for the screening criterion (7.5×10^{-5} per year) is the Reactor Safety Study's probability estimate for a pipe rupture in the MSVH area.

Table E.1 lists the 14 potentially significant accident sequences identified in the screening analysis. All 14 sequences are from the Reactor Safety Study transient event tree. This is because the postulated flood event introduces a transient event (loss of main feedwater) with a probability of one. The flood event has little or no effect on loss of coolant accident (LOCA) initiating event frequencies, and therefore, the LOCA accident sequence flooded occurrence frequencies are insignificant contributors for the flood under consideration.

None of the transient event accident sequences identified in Table E.1 are dominant accident sequences as identified in the Reactor Safety Study. The dominant transient event accident sequences in the Reactor Safety Study result from the initiating transient "loss of off-site power". As with the LOCA sequences, the negligible effect of the flood event on the initiating transient "loss of off-site power" prevented the identification of the dominant transient event accident sequences as potentially significant accident sequences. Loss of main feedwater initiates all the accident sequences listed in Table E.1.

The screening analysis did not eliminate any of the flood susceptible systems (Section E.2.2) at this stage of the analysis. Section E.4 describes the qualitative flood analysis of these systems.

Table E.1 Potentially Significant Accident Sequences Identified in the Accident Sequence Screening Analysis

Consequence Category*	Accident Sequence**	Unflooded Occurrence Frequency (WASH-1400)	ESP Estimated Flooded Occurrence Frequency
1	TMLC-α	8.9×10^{-11}	7.5×10^{-7}
1	TMLQC-α	8.9×10^{-13}	7.5×10^{-9}
2	TMLC-γ	2.1×10^{-9}	1.8×10^{-5}
2	TMLC-δ	5×10^{-9}	4.2×10^{-5}
2	TMLQC-γ	2.1×10^{-11}	1.8×10^{-7}
2	TMLQC-δ	5×10^{-11}	4.2×10^{-7}
3	TML-α	3.7×10^{-8}	7.5×10^{-7}
3	TMLQ-α	3.7×10^{-10}	7.5×10^{-9}
5	TML-β	1.9×10^{-10}	3.8×10^{-9}
5	TMLQ-β	1.9×10^{-12}	3.8×10^{-11}
6	TMLC-ε	1.7×10^{-9}	1.4×10^{-5}
6	TMLQC-ε	1.7×10^{-11}	1.4×10^{-7}
7	TML-ε	3.7×10^{-6}	7.4×10^{-5}
7	TMLQ-ε	3.7×10^{-8}	7.4×10^{-7}

*There are no category 4 accident sequences resulting from transient initiating events.

**T = Transient Event, Loss of Main Feedwater
M = Failure of the Main Feedwater System
L = Failure of the Auxiliary Feedwater System
Q = Failure of the primary system safety relief valves to reclose after opening
C = Failure of the Containment Spray Injection System
α = Containment rupture due to reactor vessel steam explosion
β = Containment failure resulting from inadequate isolation of containment openings and penetrations
γ = Containment failure due to hydrogen burning
δ = Containment failure due to overpressure
ε = Containment vessel melt-through

E.4 QUALITATIVE FLOOD ANALYSIS

The NOAH computer program[4] performed the qualitative flood simulation for both the Auxiliary Feedwater System (AFWS) and the Containment Spray Injection System (CSIS). Appendix A contains the fault trees used in the AFWS analysis. Figure E.3 shows the fault tree used in the CSIS analysis.

The Auxiliary Feedwater System contains only partially flooded minimal cut sets for the postulated flood event. This is true for all three cases defined in Section E.2.2.4. The flood-damaged components are the two electric motor-driven AFWS pumps. These two events combine with the failure of the turbine-driven AFWS pump and the failure of the solenoid operated valve that admits steam to the turbine to form the important partially flooded minimal cut sets.

For Case A, the Containment Spray Injection System has no flood-damaged components and remains unaffected by the flood event. The analysis considers one CSIS pump flood-damaged in Case B. This results in partially flooded minimal cut sets when combined with failures in the second train of the CSIS. In Case C, the analysis assumes both CSIS pumps are flood-damaged, resulting in a single flooded minimal cut set for the system.

No qualitative flood analysis is required for the Main Feedwater System since the analysis assumes that the postulated flood event disables the Main Feedwater System.

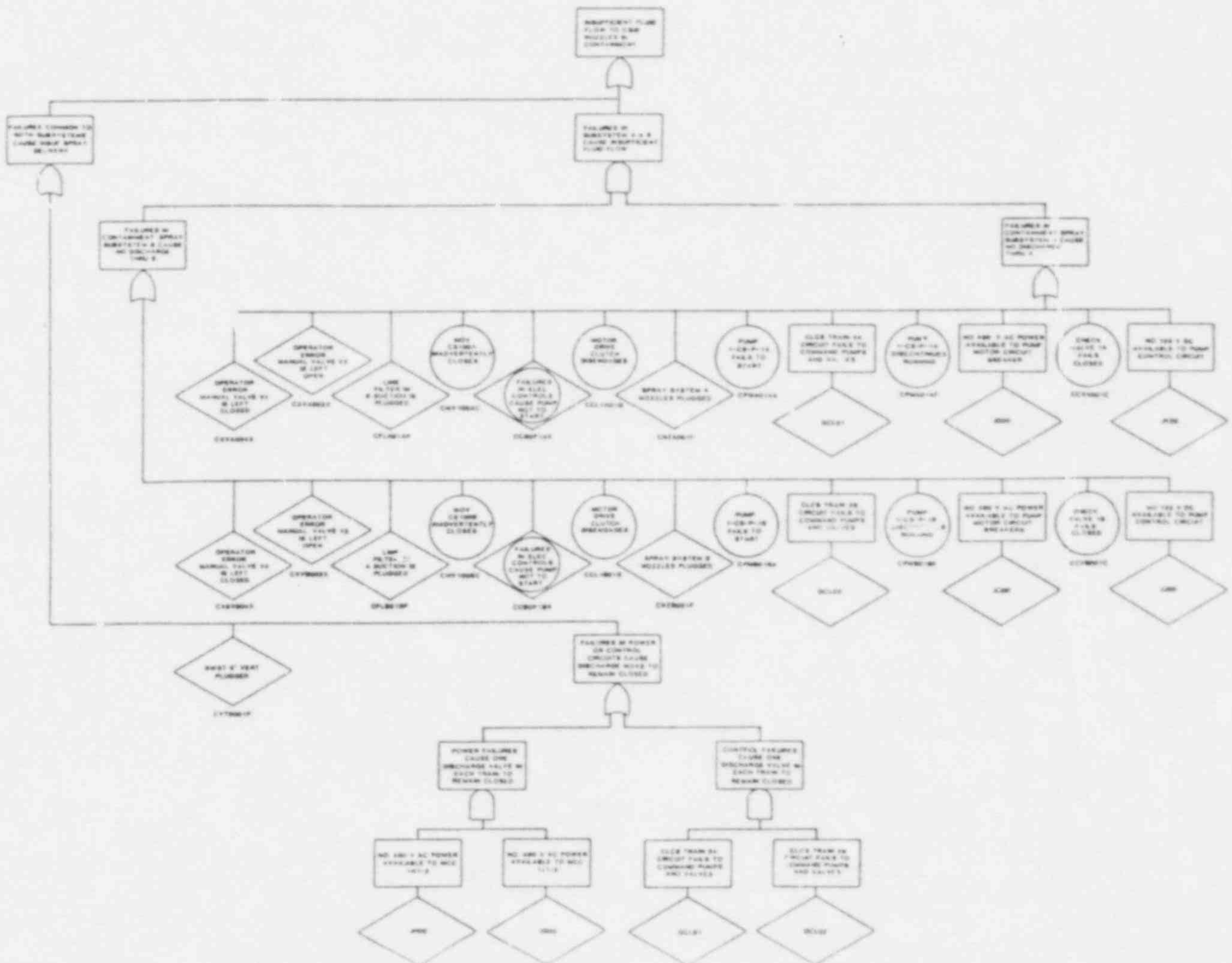

Figure E.3 CSIS Fault Tree

E.5 QUANTITATIVE EVALUATION

The quantitative evaluation determined the AFWS and CSIS failure probabilities for each of the three cases defined in Section E.2.2.4. Appendix II of the Reactor Safety Study provided the component failure probability estimates used in the quantitative evaluation of the AFWS and CSIS. Therefore, all assumptions in the Reactor Safety Study that apply to the failure data are also applicable to this analysis.

This evaluation assumes a failure probability of one for the flood-damaged components in each case. The analysis also assumes a failure probability of one for the Main Feedwater System and the occurrence of the transient event, given the postulated flood event has occurred.

E.5.1 System Failure Probabilities

Table E.2 gives the AFWS and CSIS failure probabilities for the unflooded case and for each of the three flood-damaged cases. In each of the three cases, the AFWS relies totally on the turbine-driven AFWS pump to deliver feedwater to the steam generators. The CSIS is undamaged in Case A and relies on a single CSIS pump in Case B. For Case C, both CSIS pumps are flood-damaged and the system is failed with a probability of one.

E.5.2 Accident Sequence Quantification

The accident sequence quantification step evaluated the potentially significant accident sequences identified in the accident sequence screening analysis (Section E.3) using the system flood-damaged failure probabilities for each of the three cases. The analysis used the single-state flood equations of Section 5 to determine the flood contribution to each consequence category as a function of flood probability. In each case, the unflooded contribution is the value for the consequence category occurrence frequency due to transient initiating events, prior to application of the category smoothing technique used in the Reactor Safety Study. Figures E.4 through E.6 show the flood contribution to each consequence category for each of the three cases, respectively, assuming a flood probability of 7.5×10^{-5} per year, the Reactor Safety Study estimate for the pipe rupture in the main steam valve housing area. Figures E.7 through E.9 display the same information for a flood probability of 7.5×10^{-4} per year. Figure E.10 is a graph of the total flooded contribution (sum of the consequence categories' flooded contributions) to the probability of core melt as a function of flood probability. Figure E.11 shows the total core melt probability resulting from all transient event accident sequences as a function of flood probability, including both flooded and unflooded contributions, for all three cases. Figure E.12 shows the total core melt probability resulting from all accident sequences considered in the Reactor Safety Study as a function of flood probability, including both flooded and unflooded contributions.

Table E.2 Failure Probabilities for the AFWS and the CSIS for Each of the Three Cases

Case	Failure Probability (Per Year) AFWS	CSIS
Unflooded (WASH-1400 value)	3.7×10^{-5}	2.4×10^{-3}
Case A	2.2×10^{-2}	2.4×10^{-3}
Case B	2.2×10^{-2}	2.4×10^{-2}
Case C	2.2×10^{-2}	1.0

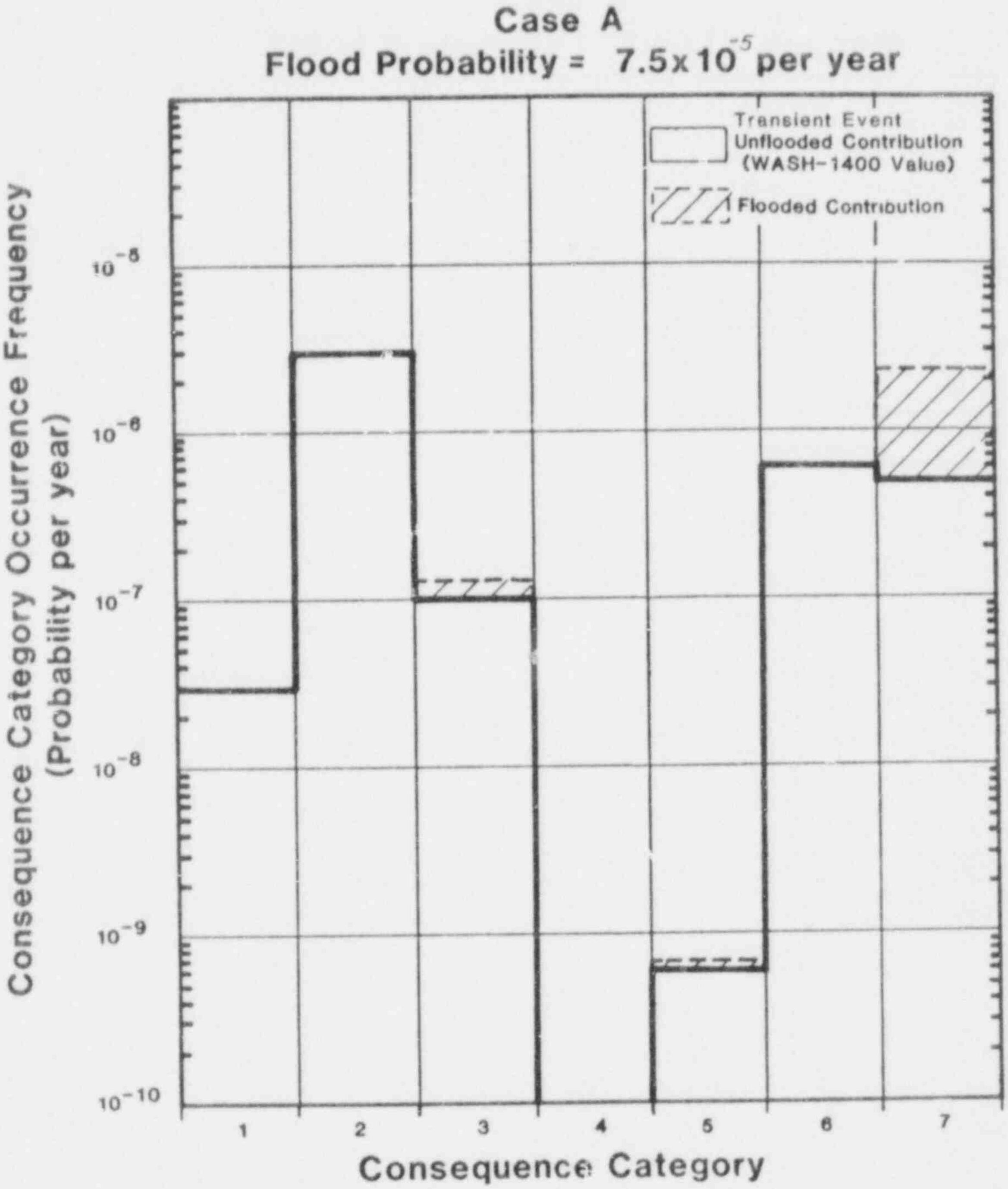

Figure E.4 Flooded Contribution to Individual Consequence Category Occurrence Frequencies for All Transient Event Accident Sequences and the MSVH Flood, Case A, Flood Probability = 7.5 x 10^{-5} per year

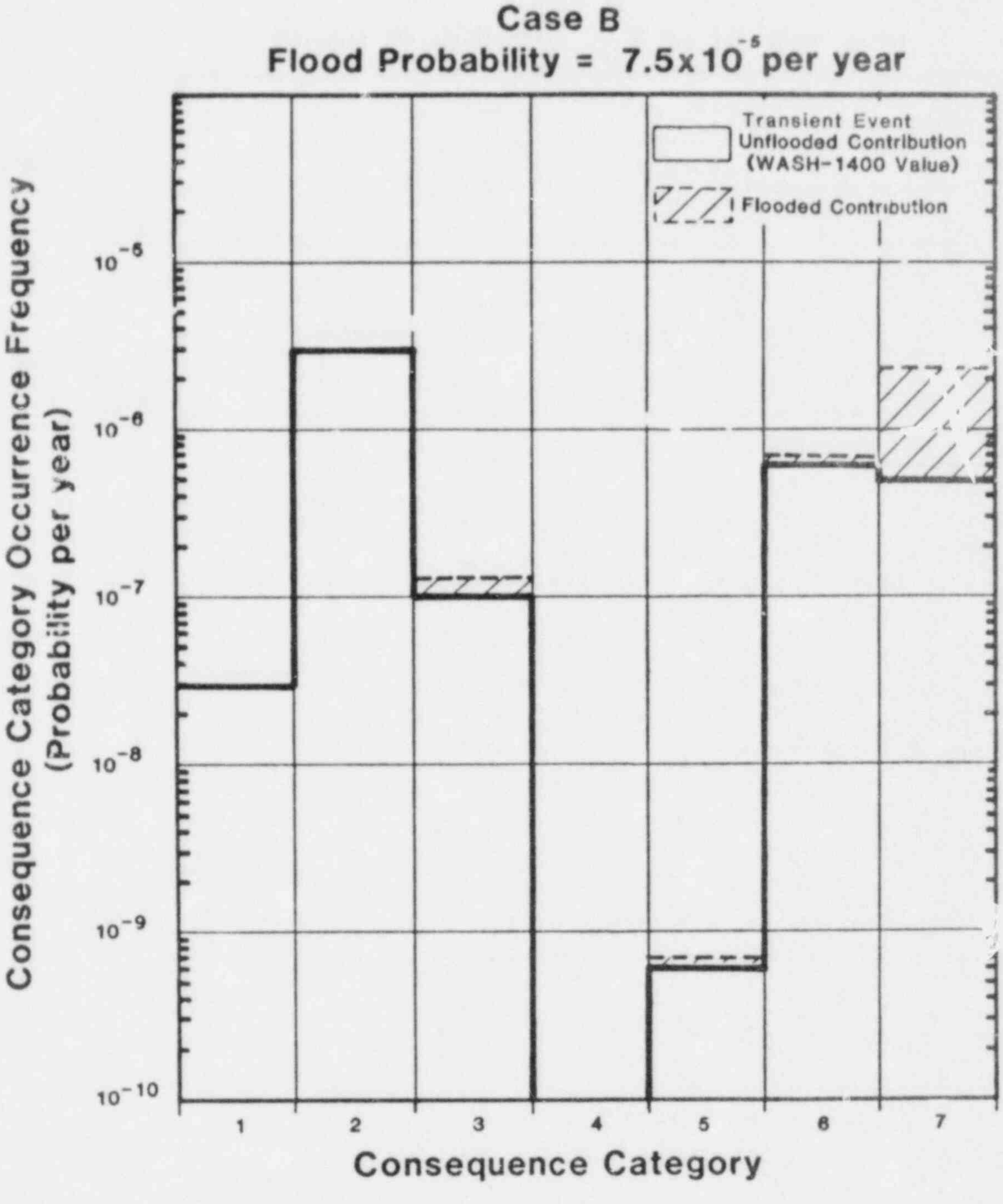

Figure E.5 Flooded Contribution to Individual Consequence Category Occurrence Frequencies for All Transient Event Accident Sequences and the MSVH Flood, Case B, Flood Probability = 7.5 x 10^{-5} per year

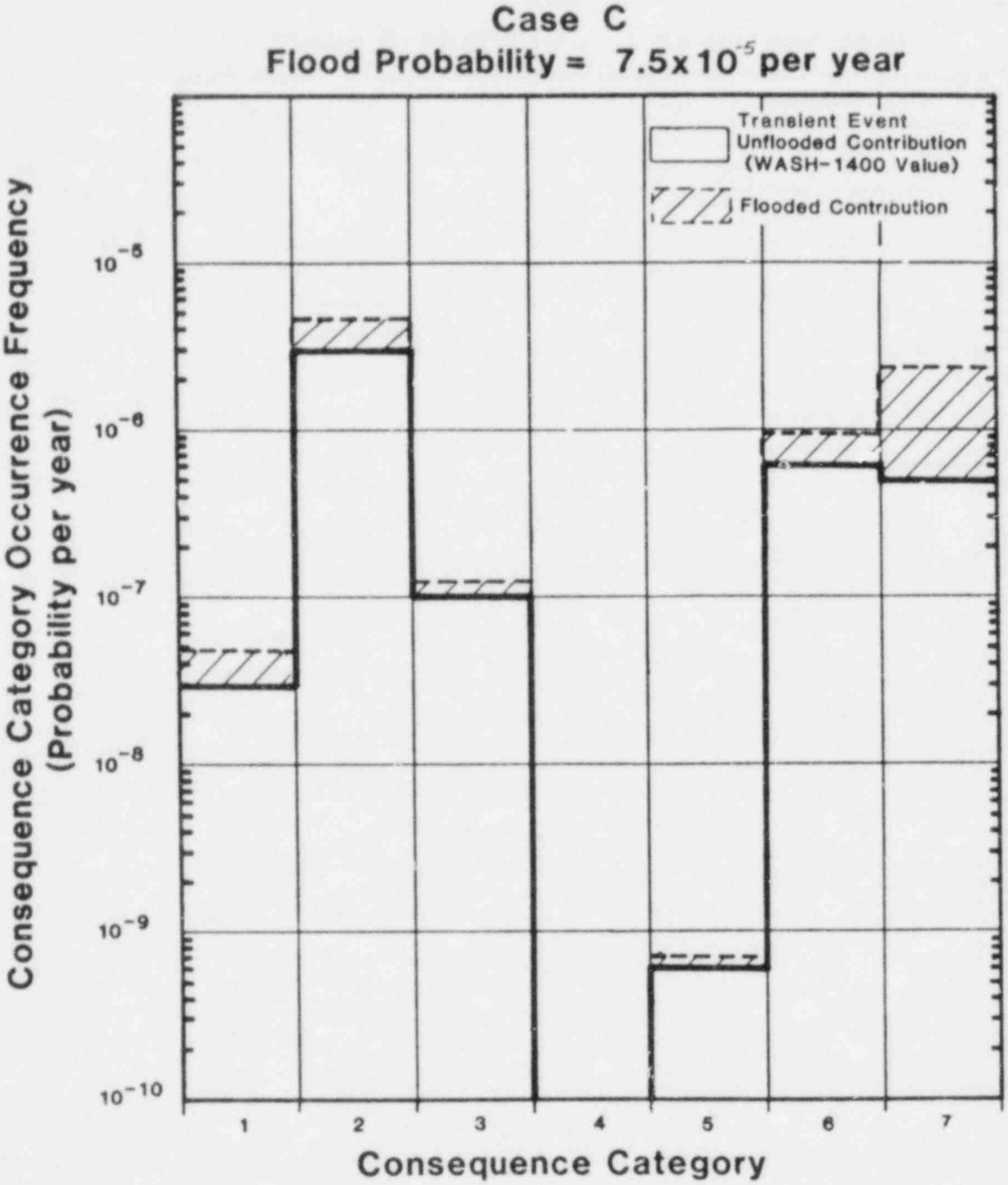

Figure E.6 Flooded Contribution to Individual Consequence Category Occurrence Frequencies for All Transient Event Accident Sequences and the MSVH Flood, Case C, Flood Probability = 7.5×10^{-5} per year

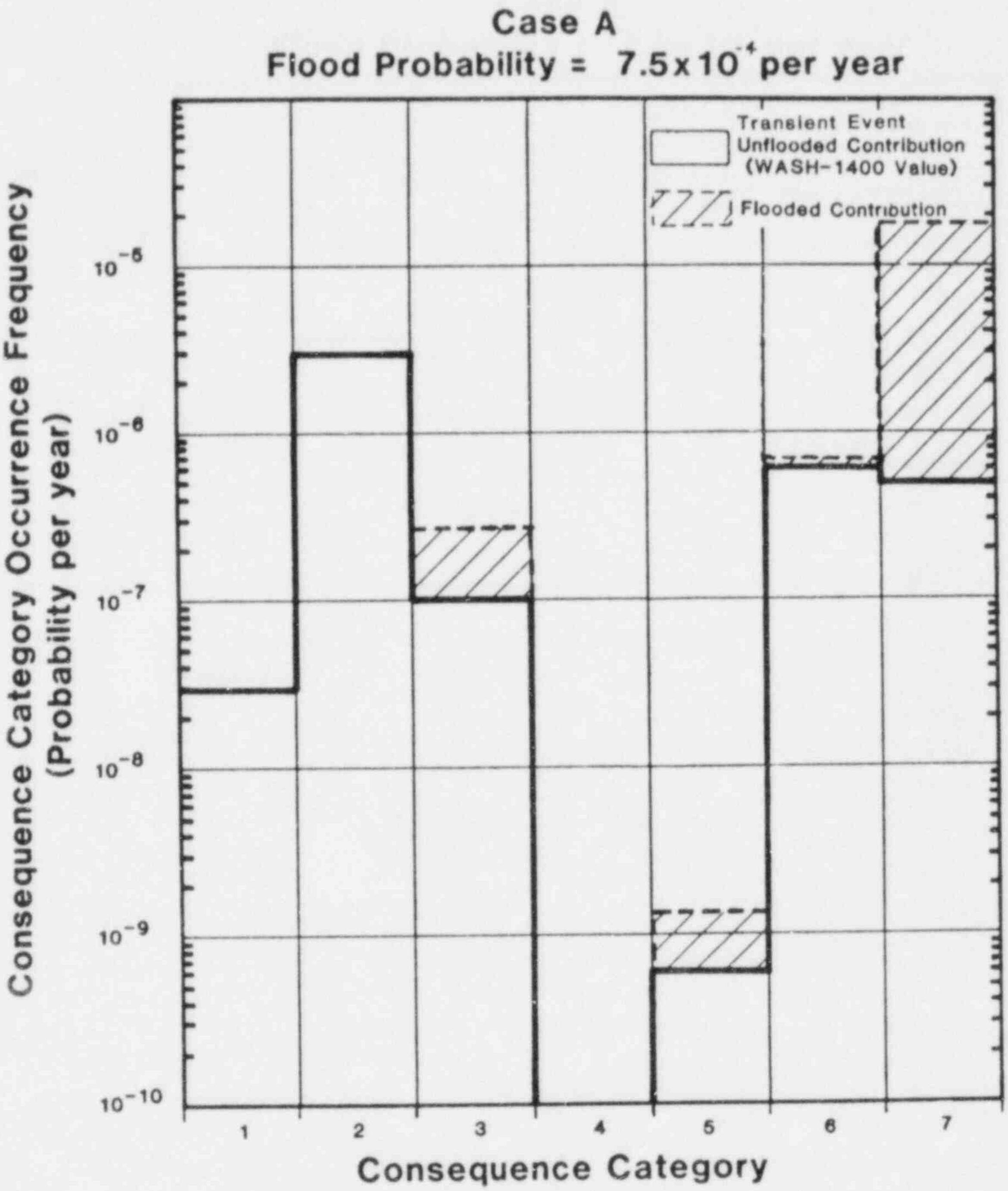

Figure E.7 Flooded Contribution to Individual Consequence Category Occurrence Frequencies for All Transient Event Accident Sequences and the MSVH Flood, Case A, Flood Probability $= 7.5 \times 10^{-4}$ per year

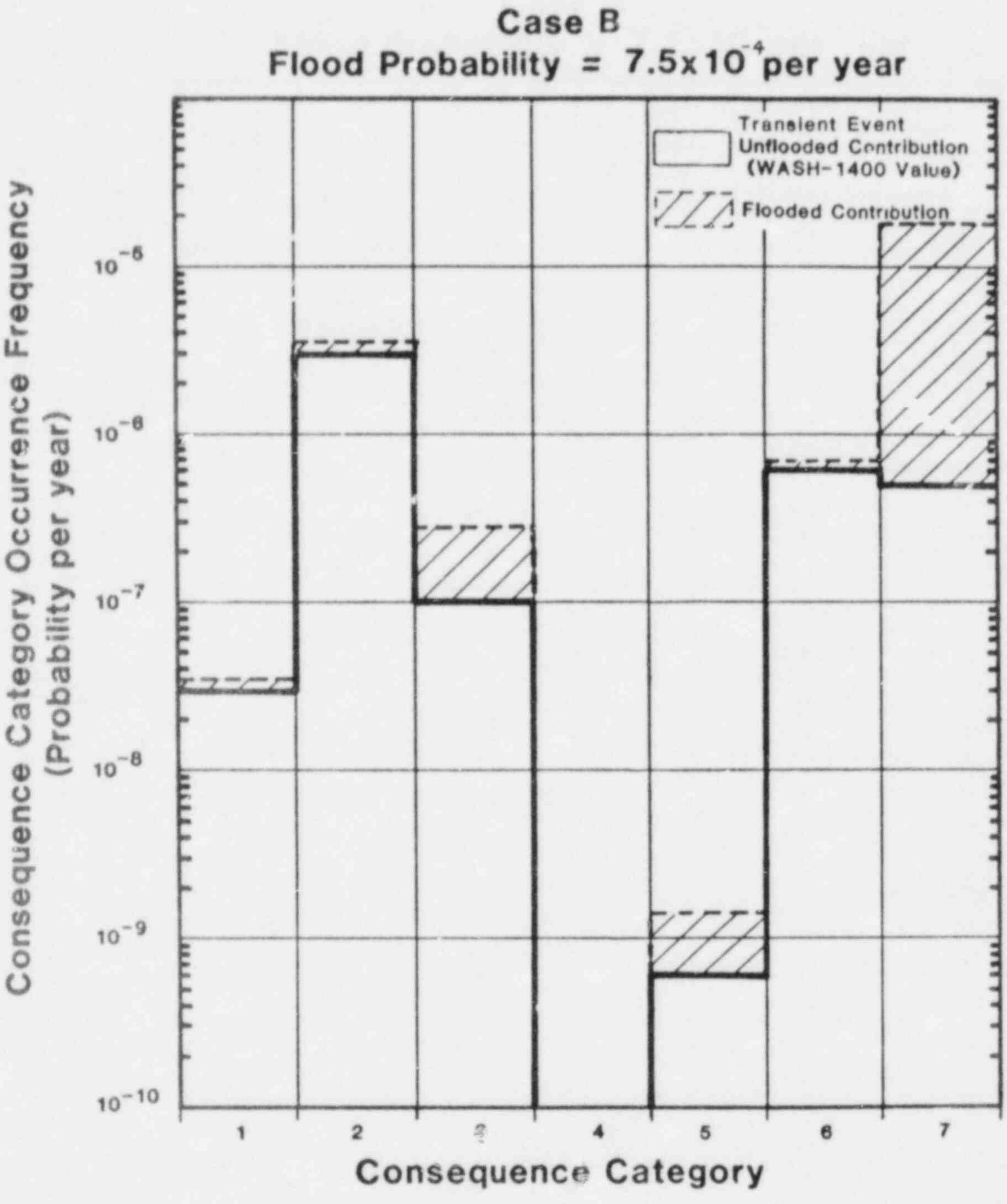

Figure E.8 Flooded Contribution to Individual Consequence Category Occurrence Frequencies for All Transient Event Accident Sequences and the MSVH Flood, Case B, Flood Probability = 7.5 x 10^{-4} per year

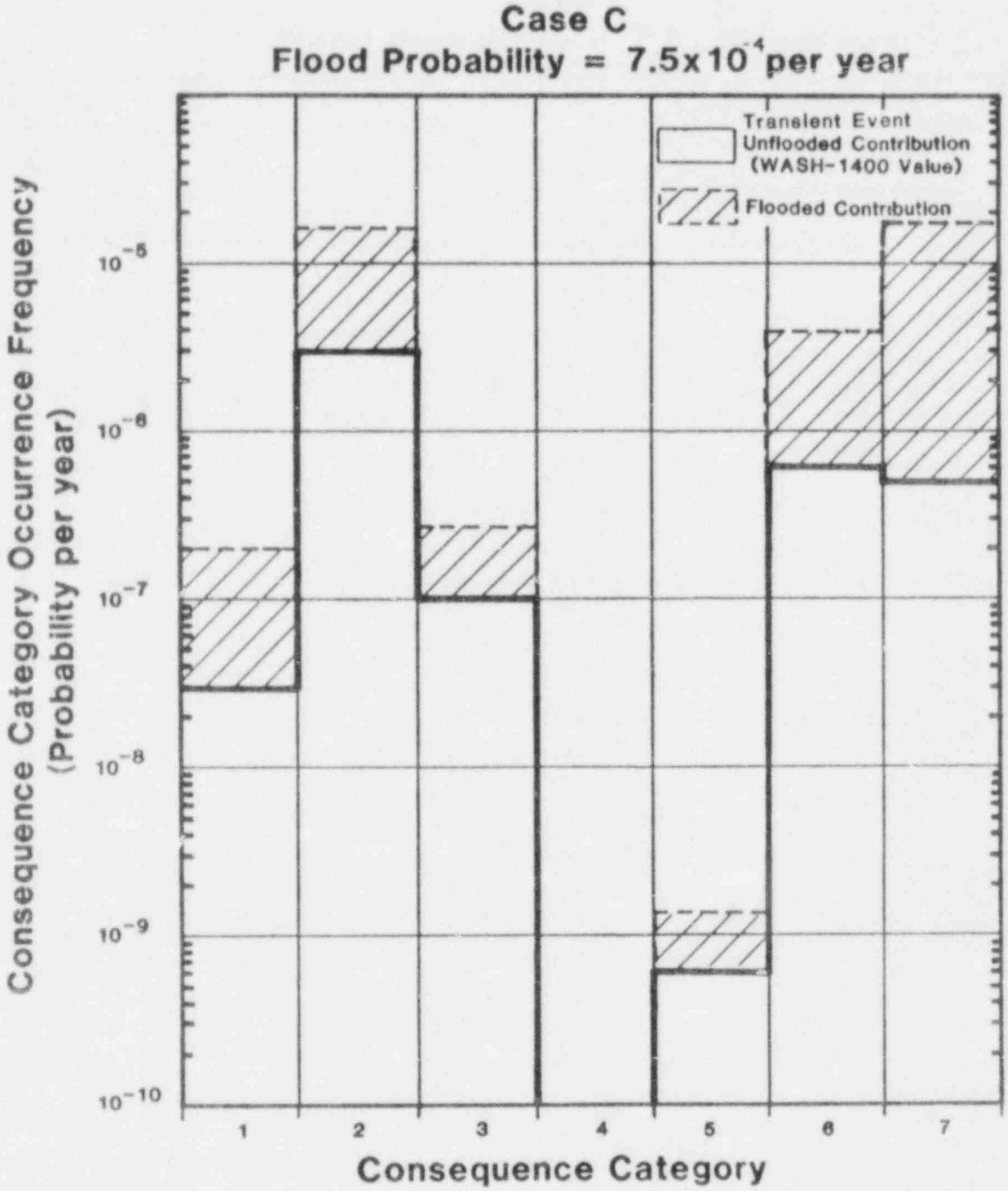

Figure E.9 Flood Contribution to Individual Consequence Category Occurrence Frequencies for All Transient Event Accident Sequences and the MSVH Flood, Case C, Flood Probability = 7.5×10^{-4} per year

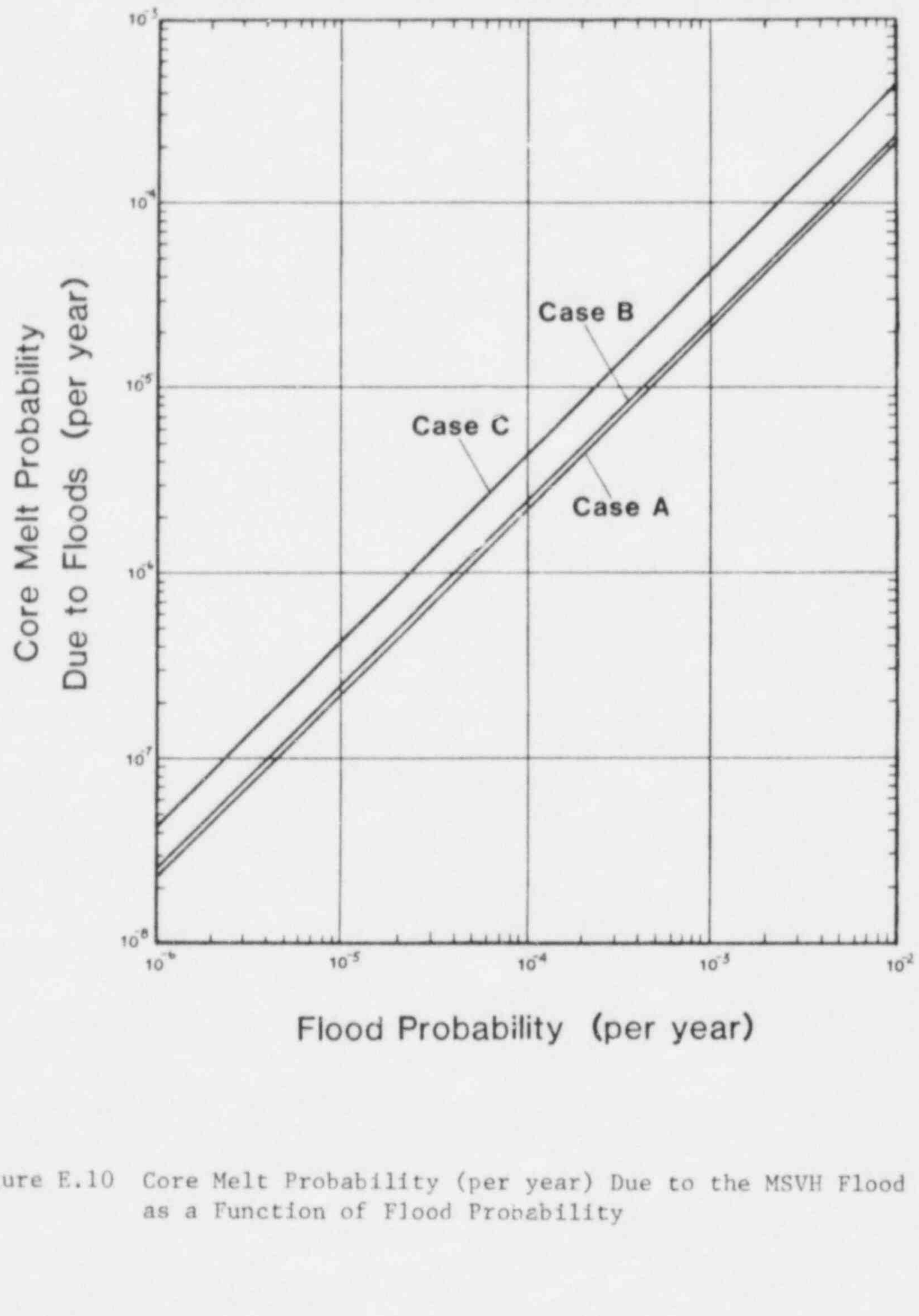

Figure E.10 Core Melt Probability (per year) Due to the MSVH Flood as a Function of Flood Probability

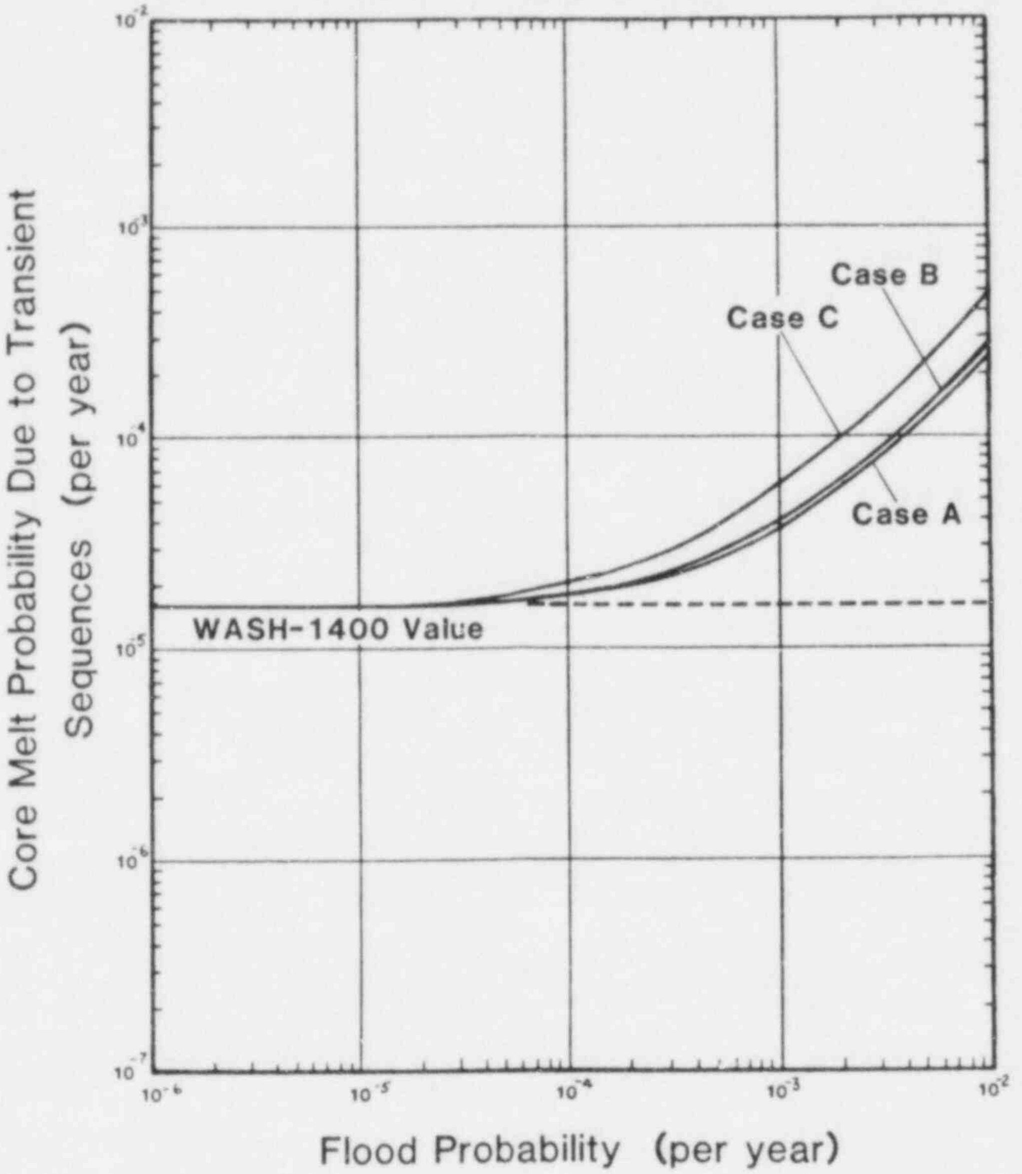

Figure E.11 Core Melt Probability (per year) Due to All Transient Event Accident Sequences, Including the Effects of the MSVH Flood, as a Function of Flood Probability

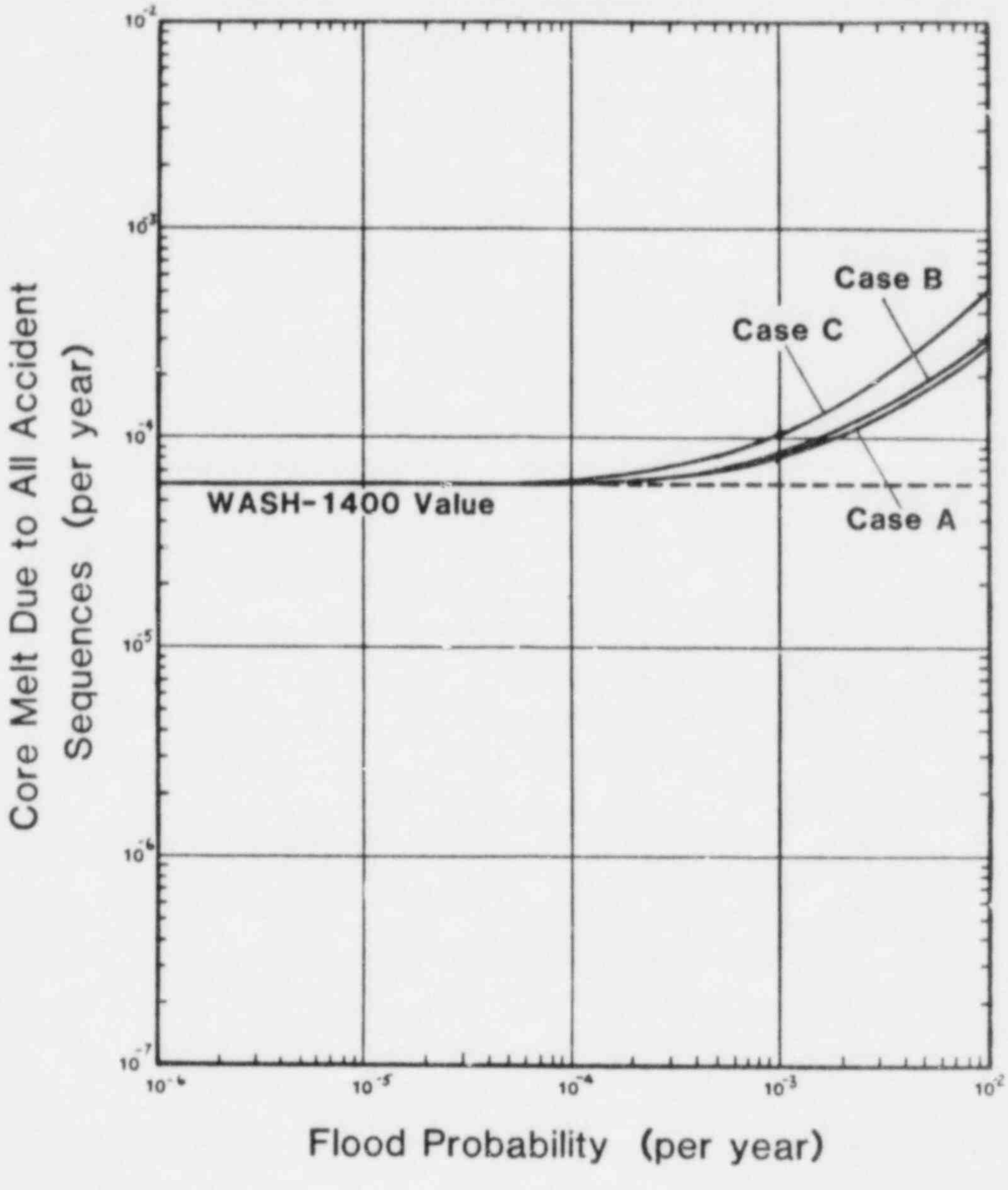

Figure E.12 Core Melt Probability (per year) Due to All Accident Sequences, Including the Effects of the MSVH Flood, as a Function of Flood Probability

NUREG/CR-2678
ORNL/TM-8314
Category Distribution RG

INTERNAL DISTRIBUTION

1- 2. L. S. Abbott
3. D. E. Bartine
4. W. B. Cottrell
5. T. E. Cole
6. J. Drago
7-10. G. F. Flanagan
11. P. M. Haas
12. H. Inhaber
13. H. E. Knee
14. F. C. Maienschein
15. A. L. Lotts
16. C. R. Richmond
17. D. B. Trauger
18. V. R. R. Uppuluri
19. A. Zucker
20. P. W. Dickson, Jr. (Consultant)
21. H. J. C. Kouts (Consultant)
22. W. B. Loewenstein (Consultant)
23. R. Wilson (Consultant)
24. Central Research Library
25. Y-12 Document Reference Section
26. Lab Records - ORNL RC
27. NSIC

EXTERNAL DISTRIBUTION

28- 31. D. P. Wagner, JBF Associates, Inc., 1630 Downtown West Boulevard, Knoxville, TN. 37919
32. M. L. Casada, JBF Associates, Inc., 1630 Downtown West Boulevard, Knoxville, TN. 37919
33. J. B. Fussell, JBF Associates, Inc., 1630 Downtown West Boulevard, Knoxville, TN. 37919
34. D. M. Rasmuson, EG&G-Idaho, Inc., P. O. Box 1625, Idaho Falls, ID. 83415
35. K. N. Fleming, Pickard, Lowe & Garrick, Inc., 17840 Skypark Boulevard, Irvine, CA. 92714
36. W. E. Vesely, Battelle Columbus Laboratories, 505 King Avenue, Columbus, OH. 43201
37. A. R. Buhl, Technology for Energy Corporation, 10770 Dutchtown Road, Knoxville, TN. 37922
38. N. D. Cox, EG&G-Idaho, Inc., P. O. Box 1625, Idaho Falls, ID. 83415
39. Boyer B. Chu, Electric Power Research Institute, 3412 Hillview Avenue, Palo Alto, CA. 94303
40. Bob Christie, Tennessee Valley Authority, Nuclear Engineering Branch, W70C726, 400 Commerce Avenue, Knoxville, TN. 37902
41. Joe Johnson, Tennessee Valley Authority, Power Operations Training Center, P. O. Box 2000, Daisy, TN. 37319
42. Zack Pate, Institute of Nuclear Power Operations, 1820 Water Place, Atlanta, GA. 30339
43. K. A. Solomon, Rand Corporation, 1700 Main Street, Santa Monica, CA. 90406
44. A. K. Bhattacharyya, Kuljian Corporation, 3700 Science Center, Philadelphia, PA. 19104
45. G. Apostolakis, Chemical, Nuclear & Thermal Engineering, 5532 Boelter Hall, School of Engineering & Applied Science, University of California-Los Angeles, Los Angeles, CA. 90024

NUREG/CR-2678
ORNL/TM-8314
Category Distribution RG

46. M. Stamatelatos, Torrey Pines Technology, P. O. Box 81608, San Diego, CA. 92138
47. Office of Assistant Manager of Reactor Research & Technology, U. S. DOE, ORO, Oak Ridge, TN. 37830
48- 49. U. S. DOE Technical Information Center, Oak Ridge, TN. 37830
50. P. K. Niyogi, Methodology Development Section, Risk Methodology & Data Branch, Division of Risk Analysis, Office of Nuclear Regulatory Research, U. S. Nuclear Regulatory Commission, Washington, D. C. 20555
51. S. R. Sturges, Methodology Development Section, Risk Methodology & Data Branch, Division of Risk Analysis, Office of Nuclear Regulatory Research, U. S. Nuclear Regulatory Commission, Washington, D. C. 20555
52-321. Given distribution as shown in Category RG, Systems & Reliability Reports.

☆U.S. GOVERNMENT PRINTING OFFICE 1982-546-067/67

120555078877 1 ANRG
US NRC
ADM DIV OF TIDC
POLICY & PUBLICATIONS MGT BR
PDR NUREG COPY
LA 212
WASHINGTON DC 20555