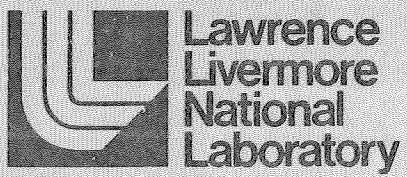
NUREG/CR-2015, Vol. 8, Rev. 1
UCRL-53021, Vol. 8, Rev. 1

Phase I Final Report—Systems Analysis (Project VII)

Seismic Safety Margins Research Program

J. E. Wells, L. L. George, and G. E. Cummings

Prepared for
U.S. Nuclear Regulatory Commission



This work was supported by the United States Nuclear Regulatory Commission under a Memorandum of Understanding with the United States Department of Energy.

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

and

National Technical Information Service
Springfield, Virginia 22161

NUREG/CR-2015, Vol. 8, Rev. 1
UCRL-53021, Vol. 8, Rev. 1
RD, RM

Phase I Final Report— Systems Analysis (Project VII)

Seismic Safety Margins Research Program

Manuscript Completed: November 1983
Date Published:

Prepared by
J. E. Wells, L. L. George, and G. E. Cummings

Lawrence Livermore National Laboratory
7000 East Avenue
Livermore, CA 94550

Prepared for
Division of Engineering Technology
Office of Nuclear Regulatory Research
U. S. Nuclear Regulatory Commission
Washington, D.C. 20555
NRC FIN No. A0130

ABSTRACT

This document reports on the Phase 1 efforts of the Systems Analysis Project to develop the tools and methods for computing the probability of radioactive release from a commercial nuclear power plant in the event of an earthquake.

CONTENTS

ILLUSTRATIONS

TABLES

FOREWORD

The Seismic Safety Margins Research Program (SSMRP) is an NRC-funded, multi-year program conducted by Lawrence Livermore National Laboratory (LLNL). One of the goals of the program is to develop a complete, fully coupled analysis procedure (including methods and computer codes) for estimating the risk of an earthquake-caused radioactive release from a commercial nuclear power plant. The analysis procedure is based upon a state-of-the-art evaluation of the current seismic analysis and design process and explicitly includes the uncertainties inherent in such a process. The results will be used to improve seismic licensing requirements for nuclear power plants.

The SSMRP was begun in 1978 when it became evident that an accurate seismic safety assessment must consider simultaneously all the interrelated factors that affect the probability of radioactive release. (In the traditional design procedure each factor is usually analyzed separately.) These closely coupled factors are:

- The likelihood and magnitude of an earthquake.
- The transfer of earthquake energy from a fault source to a power plant, a phenomenon that varies greatly with the magnitude of an earthquake.
- Interaction between the soil under the power plant and the structural response, a phenomenon that depends on the soil composition and the location of the fault source relative to the plant.
- Coupled responses of a power plant's buildings and the massive reactor vessels, piping systems, and emergency safety systems within.
- Numerous accident scenarios which vary according to the types of failures assumed and the success or failure of the engineered safety features intended to mitigate the consequences of an accident.

A nuclear power plant is designed to ensure the survival of all buildings and emergency safety systems in a worst-case ("safe shutdown") earthquake. The assumptions underlying this design process are deterministic. In practice, however, these assumptions are clouded by uncertainty. It is not possible, for example, to predict accurately the worst earthquake that will occur at a given site. Soil properties, mechanical properties of buildings, and damping in buildings and internal structures also vary significantly among plants.

To model and analyze the coupled phenomena that contribute to the total risk of radioactive release it is therefore necessary to consider all significant sources of uncertainty as well as all significant interactions. Total risk is then obtained by considering the entire spectrum of possible earthquakes and integrating their calculated consequences. In the SSMRP this approach to risk analysis is embodied in the seismic analysis chain comprising five steps: determining seismic input characteristics for a site, calculating the effects of soil-structure interaction, calculating major structure response, calculating subsystem response, and calculating probability of radioactive release.

The seismic input consists of the earthquake hazard in the vicinity of a nuclear power station, defined by an estimate of the seismic hazard function (i.e., the relationship between the probability of occurrence and a measure of the size of an earthquake) and a description of the free-field motion. The soil-structure interaction step in the chain transforms the free-field ground motion into basemat or in-structure response, accounting for the interaction of the soil with the massive, stiff structures in a nuclear power plant. Determination of the major structure response follows the soil-structure interaction step, where "major structure" commonly denotes a building, but may also include very large components. The final step in the traditional seismic analysis and design process is predicting subsystem structural response. An additional step in the SSMRP is the prediction of failure and subsequent risk of radioactive release.

In the SSMRP this methodology is implemented in three computer programs: HAZARD, which assesses the seismic hazard at a given site; SMACS, which computes in-structure and subsystem seismic responses; and SEISIM, which calculates structural, component, and system failure probabilities and radioactive release probabilities.

The SSMRP Phase I effort was organized into eight projects. In Project I, we chose Unit 1 of the Zion Nuclear Power Plant as an appropriate "typical" plant. In Project II, we developed the tools and models, including HAZARD, necessary to describe probabilistically the seismic hazard at the Zion site and to generate the appropriate acceleration time histories. In Project III, we provided as input to the first step in the SMACS calculational procedure the characterizations of soil, foundations, and structures at the Zion plant necessary to an analysis of the coupled soil-structure system. Major structure models were developed in Project IV as necessary input to the

SMACS computation carried out in Project VIII. In Project V, data were collected and models established for the pertinent piping subsystems to provide input to the SMACS computation. In Project VI we developed fragility curves - normal or lognormal distributions describing the probability of failure as a function of a critical response parameter - necessary for all components and structures whose failure is accounted for in the fault trees. In Project VII the event/fault trees are used to systematically describe the possible accident sequences that follow an earthquake. The SEISIM computer code accepts as input the accident sequences, initiating events, system descriptions, responses computed by SMACS, the set of fragility curves, and a seismic hazard curve for the Zion site to calculate the structural, component, and system failure probabilities and the probabilities of radioactive release. The SMACS computer code was developed in Project VIII to tie together the soil-structure interaction, structure response, and subsystem response calculations.

The results and technical products of each of the eight projects are described in separate volumes of the SSMRP Phase I Final Report. Volume 1 presents an overview of the Phase I effort.

This volume of the final report addresses the work performed under Project VII, Systems Analysis. The NRC technical monitor for Project VII was J. J. Burns. Science Applications, Inc. (SAI), Palo Alto, California and Bethesda, Maryland generated the fault trees and event trees used in our analysis, and Howard Lambert helped analyze these fault trees and event trees. Appendices C, D, and E are extracted from reports generated by SAI. J. H. Wiggins Co. of Redondo Beach, California developed the initial version of the computer code SEISIM. Enos Baker (EG&G, San Ramon, California) and Marilyn Kamelgarn (Lawrence Livermore National Laboratory) edited this report. We would also like to thank Lauri Dello, Frank Gilman, Edna Carpenter, Lynn Lewis, and the members of LLNL's Technical Information Department staff who contributed their efforts to its production.

EXECUTIVE SUMMARY

The Systems Analysis project was initiated with the following specific objectives:

1. Develop a computational procedure for estimating the relative importance of the factors contributing to reactor seismic safety. The procedure, which will give insights into seismic safety requirements, will be used to calculate failure and radioactive release probabilities and their uncertainties over a range of earthquake levels.

2. Develop event-tree/fault-tree models of nuclear power plants for incorporation into the computational procedure. These models will be used to calculate the required failure and release probabilities. For Phase I of this program, event-tree/fault-tree models of the Zion 1 Nuclear Power Plant were constructed.

The fault trees and event trees define the events whose probabilities we computed. A fault tree represents the failure of the systems called upon to mitigate the effects of an initiating event. The initiating events and system failure events are linked in accident sequences; the event trees describe this linkage. Each accident sequence of interest leads to core melt and fission product release.

The Systems Analysis project accounts for the fact that during an earthquake all components in a nuclear power plant, including the redundant critical components of the reactor systems, are simultaneously excited. For large earthquakes, the redundant components are just as likely to be highly stressed and to fail simultaneously. Because the failures of components given an earthquake are dependent, the calculation of system failure is more complex than the calculation of system failure considering only independent random failures (i.e., failures due to wear, corrosion, or maintenance or installation errors). The computer code SEISIM (Systematic Evaluation of Important Safety Improvement Measures) computes such dependent failure probabilities.

SEISIM computes event probabilities conditional on having earthquake peak acceleration within narrow intervals. We uncondition the SEISIM output event probabilities by multiplying them by the annual probability of having an earthquake with a given peak acceleration in one year in the specified interval and then summing over all intervals. The result is the probability of an earthquake and an event in one year.

Responses causing component failures are correlated because the responses result from the same earthquake. This correlation means failure events are dependent. Therefore, the probability of failure of several components is not the product of the component failure probabilities. This correlation is accounted for in the probability computation by using a procedure called multivariate interference analysis. The failure probability for dependent events is usually greater than the probability assuming independence.

Correlation is used to characterize dependent component failures. It yields a tractable method for computing failure probabilities of systems with dependent components. If component responses and strengths are normally or lognormally distributed and if component failure occurs when response exceeds strength, then correlation completely characterizes component dependence.

Ranking components and accident sequences according to their importance permits identification of components and cut sets that significantly contribute to the occurrence of any event. We use an importance measure because components may be in several cut sets. This measure is a function of the sum of the probabilities of cut sets containing a component (Lambert, 1975).

Other sensitivity measures in SEISIM are:

a. Discrete derivatives (slopes) of probabilities with respect to means and variances of component responses and strengths.
b. Derivatives of responses with respect to primary input variables such as earthquake intensity, soil parameters, etc.
c. Derivatives of probabilities with respect to parameters of distribution functions of response and strength.

We have developed the subroutines to compute these derivatives; they will be used in the Phase II sensitivity analyses.

SECTION 1: INTRODUCTION TO SYSTEMS ANALYSIS

1.1 OVERVIEW OF COMPUTATIONAL PROCEDURE

The Seismic Safety Margins Research Program (SSMRP) is an NRC-funded multi-year program directed towards developing a complete, fully coupled analysis procedure for computing the probability of radioactive release from a commercial nuclear power plant in the event of an earthquake. The goal of the program is to develop improved seismic licensing requirements. The analytical procedures under development are being demonstrated by application to the Zion Nuclear Power Plant.

The Systems Analysis project of the SSMRP developed the tools and methods for calculating the probability of release given the earthquake hazard; the computed structural, piping, and component responses; and the failure relations. The computer code SEISIM was developed to integrate these inputs and compute the probability of radioactive release.

In addition to developing tools to calculate the probability of release, the Systems Analysis project developed tools to generate importance and sensitivity measures which can be used to gain insight into what occurs during a seismic event. These include ranking components and systems, ranking the effect of input variables (e.g., soil modulus, soil depth, stiffness, and damping), and developing sensitivity measures based on changes in response and strength distribution functions.

The Systems Analysis project considers the pervasive nature of earthquake-induced ground shaking, which can compromise the redundancy built into nuclear plant systems. In order to protect against random failures (i.e., failure due to wear, corrosion, maintenance, or installation errors), redundant critical components of the plant system are provided. For example, at a point in a piping system where a valve must open following an accident, two valves in parallel are provided, so that if one valve should fail to open, the second valve could open and provide the necessary flow path. However, during an earthquake, all components in the reactor system are excited simultaneously. For large earthquakes, the redundant components are likely to be highly stressed, and thus are likely to fail simultaneously. The failures of the individual components cannot be assumed to be independent, and the calculation of system failure is more complex than the corresponding

calculation considering only independent random failures. The computer code SEISIM computes such dependent failure probabilities.

This report documents the Systems Analysis project's accomplishments in Phase I.

The computational procedure that has been developed is summarized in Fig. 1.1 and in the following four steps.

Step 1 Identify the set of all possible accident sequences of events which will occur before radioactive material is released. Note that different sequences will result from the success or failure of engineered safety systems. This step relies on event trees for describing the accident sequences.

Step 2 Identify the critical components (for example pipes, valves, etc.) which, if failed, may lead to risk to the public (for example, core melt followed by fission product release). This step uses fault tree techniques for implementation.

Step 3 Calculate the probability of all accident sequences for all possible initiating events at all credible earthquake levels. This requires:

- calculation of mechanical responses of all initiating events,
- calculation of the mechanical responses of all relevant engineered safety system components, and
- estimation of relevant component failure functions.

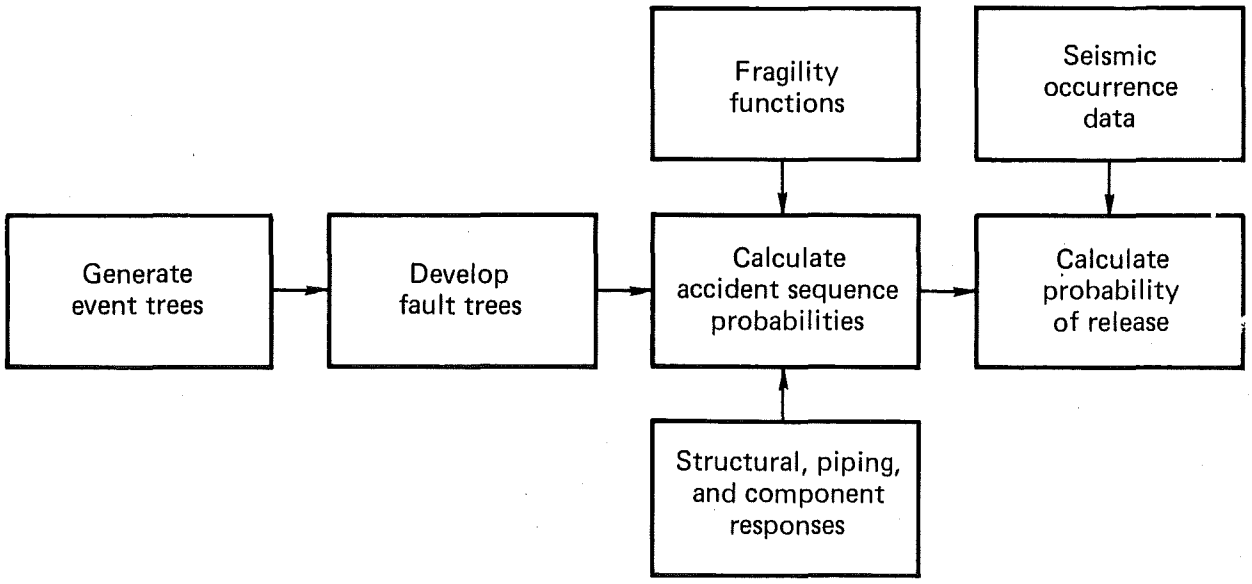


Figure 1.1. Overview of the computational procedure.

Step 4 Calculate the total risk by integrating the probabilities obtained in Step 3 with the earthquake hazard. This requires the estimation of seismic hazard curves.

1.2 OUTLINE OF REPORT

Section 2 of this report describes the fault trees and event trees generated for SSMRP.

Section 3 describes the probability computations for all events from component failures to releases. It also describes the sensitivity measures that have been implemented in the computer program SEISIM.

Section 4 contains conclusions and recommendations. The recommendations include further development of the computational procedure.

There are seven appendices.

- Appendix A, Glossary of Terms, defines the terms used in this report. This glossary is not exhaustive. For a more complete glossary, see LLNL Report UCRL-53001 (Smith, 1980).
- Appendix B, Glossary of Acronyms, describes the acronyms used in this report and the nuclear industry.
- Appendix C, Event Trees, provides the eight event trees generated for Zion 1 nuclear plant.
- Appendix D, System Descriptions and Fault Trees, describes those systems for which fault trees were generated.
- Appendix E, Basic Event Code, describes the 10-digit basic event code.
- Appendix F, Supporting Systems Analysis Studies, describes studies done in support of the Systems Analysis project.
- Appendix G, Release Category Definitions, provides definitions of the release categories used in this study.

SECTION 2: EVENT TREE AND FAULT TREE ANALYSIS IN SSMRP

2.1 INTRODUCTION

The event and fault trees were developed to provide for input to the SEISIM computer code (see Sec. 3 for SEISIM details). Because the SSMRP Phase I analysis is concerned with accidents which could cause core melt and radioactive release, our focus was on those initiating events which could result in core melt as a consequence of loss of coolant through leakage or boiloff. The type of initiating event determines which systems are required. Table 2.1 lists the initiating events in a hierarchical order. For the levels of earthquake acceleration considered, we assume that at least one initiating event in Table 2.1 occurs and that the set of initiating events is complete.

2.2 EVENT TREE ANALYSIS

Application of event tree methodology to risk assessments of nuclear power plants was introduced by WASH 1400. One of that study's goals was to estimate the probability of accidental release of radioactivity from nuclear power plants. This required the identification of the initiating events and accident sequences which, given the failure of safety systems, could result in core melt followed by a large radioactive release.

An event tree describes the sequences of events that may occur following an initiating event and identifies the systems which are required to mitigate an accident. Success or failure of the systems is determined by the use of fault trees. Fault trees are discussed in Sec. 2.3.

Figure 2.1, an example of an event tree, describes the possible accident sequences given a reactor vessel rupture (RVR). The RVR accident sequence RCEF shows that if you have a RVR, success of the containment spray injection system (CSIS) and the containment fan cooler system (CFCS) in the injection phase, failure of the CFCS in the recirculation phase, and failure of the residual heat removal system (RHRS), then a core melt will result. Note that all RVR sequences result in core melt.

WASH 1400 lists five functions which occur sequentially following an initiating event. These basic functions are:

a. Reactor shutdown (rapid shutdown of reactor to limit core heat production: RPS).

Table 2.1. Definitions of event tree initiating events.

1. Reactor Vessel Rupture (RVR)

   A vessel rupture large enough to negate the effectiveness of the ECC systems required to prevent core melt or a rupture of sufficient primary coolant piping in a pattern that negates the effectiveness of those same ECC systems.

2. Large LOCA (LLOCA)

   A rupture of primary coolant piping equivalent to the break of a single pipe whose inside diameter is greater than 6 in. but which does not negate the effectiveness of the ECC systems required to prevent core melt.

3. Medium LOCA (MLOCA)

   A rupture of primary coolant piping equivalent to the break of a single pipe whose inside diameter is greater than 3 in. but less than or equal to 6 in.

4. Small LOCA (SLOCA)

   A rupture of primary coolant piping equivalent to the break of a single pipe whose inside diameter is greater than 1.5 in. but less than or equal to 3 in.

5. Small-small LOCA (SSLOCA)

   A rupture of primary coolant piping equivalent to the break of a single pipe whose inside diameter is greater than 0.5 in. but less than or equal to 1.5 in.

6. Class 1 Transient (T1)

   Any abnormal condition in the plant which requires that the plant be shut down but which does not directly affect the operability of the PCS and does not qualify as a LOCA or vessel rupture.

7. Class 2 Transient (T2)

   Any abnormal condition in the plant which requires that the plant be shut down and does not qualify as a LOCA or vessel rupture but which causes the PCS to become inoperative.

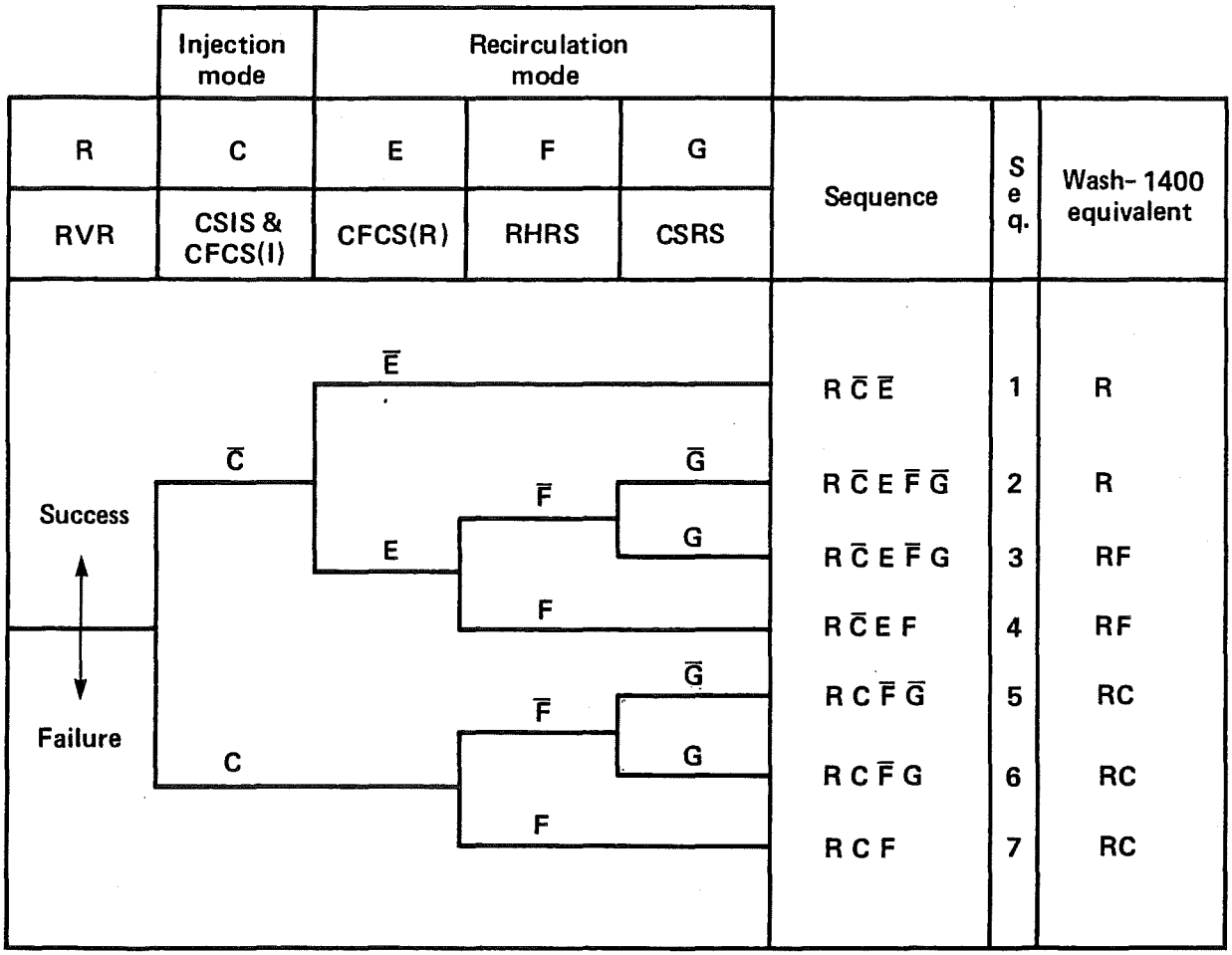


Figure 2.1. Reactor vessel-rupture event tree.

b. Emergency core cooling (core cooling to prevent release of radioactivity from fuel: ACC, SIS, CHG, AFWS, RHRS).
c. Post-accident radioactivity removal (removal of radioactivity from containment atmosphere: CSIS, CSRS, CFCS, CVCS).
d. Post-accident heat removal (removal of heat from containment to prevent overpressurization: CSRS, CFCS, CSIS, RHRS).
e. Containment integrity (prevention of dispersal of radioactivity to the environment containment building, containment isolation).

These functions are the basis for the LOCA event trees developed for Zion Unit 1. All of the systems that perform these functions require electrical power except for the reactor protection system (RPS) and the accumulators (ACC). However, the event trees for the SSMRP do not include electrical power

as an explicit event. We include the electrical power requirements in the fault trees for the systems. This approach provides a more accurate representation of the accident sequences since redundant cut sets can be excluded. Appendix C contains detailed event tree descriptions.

2.3 FAULT TREE ANALYSIS

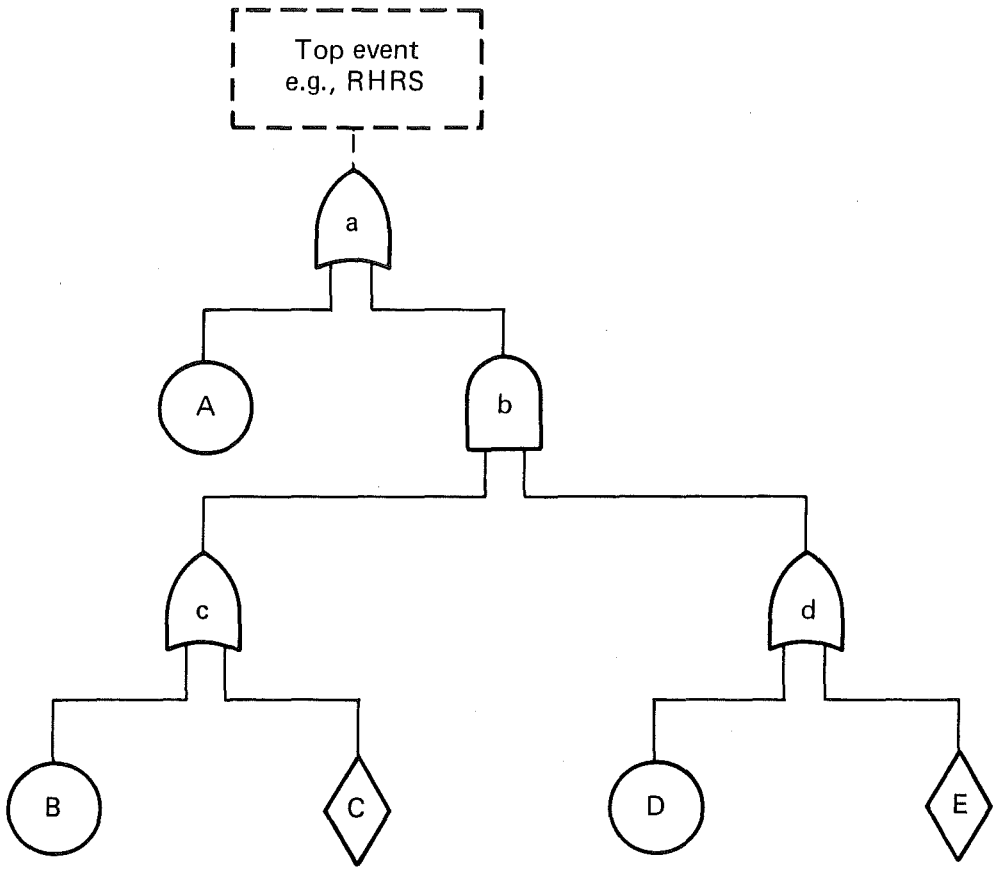
The fault tree analysis generates the system failure events identified by the event trees. Table 2.2 lists systems that appear on the event trees and indicates those that we generated in Phase I. The systems for which fault trees were developed were chosen on the basis of their importance to our analysis. These trees are defined in detail in Appendix D.

Fault tree analysis is a systems safety engineering technique that provides a systematic, descriptive approach to the identification of all possible system failure paths (Barlow and Lambert, 1975). An example of a fault tree is given in Fig. 2.2, which shows the combinations of events that lead to system failure, the top event in the fault tree. The top event is

Table 2.2. Zion 1 safety and supporting systems.

Systems listed on event trees	Supporting systems
Auxiliary feed water system[a]	Electric power[a]
Containment fan cooler system	Service water[a]
Containment spray system	Heating and ventilating system
Chemical volume and control system	Component cooling water system
Emergency core cooling system[a]	Instrumentation and control system
Charging pumps	
Safety injection system	
Residual heat removal system	
Accumulators	
Power conversion system	
Reactor protection system	

[a]Phase I fault trees



d = D∪E

c = B∪C

b = c∩d

a = A∪b

Minimal Cut Sets

1. A
2. B∩D
3. B∩E
4. C∩D
5. C∩E

Figure 2.2. Example of a system fault tree.

logically linked by branches and gates, which represent the Boolean operators, to the events that have a more basic cause--the basic events.

The system failure expressions determined from the fault trees are input into SEISIM in the form of minimal cut sets, the smallest sets of basic events that must take place in order for the top event to occur. (By using Boolean algebra, we can reduce all fault trees into unions of intersections of basic events. These intersections are known as cut sets.) Figure 2.2 also shows the corresponding minimal cut sets in Boolean form for the example fault tree, as required by SEISIM.

2.4 GENERATION OF MINIMAL CUT SETS

Once the fault tree models have been constructed, they need to be evaluated: i.e., minimal cut sets need to be generated. Two computer codes were used to determine the fault tree minimal cut sets. The first code, SETS (Worrell, 1978), evaluated all systems except the auxiliary feedwater system. One advantage of this code is that the output minimal cut sets can be used as input into SETS when generating accident sequence cut sets. The second code, FTAP (Willie, 1978), evaluated the auxiliary feedwater system. FTAP was used because it allowed us to run the program on a computer having virtual memory capability, thus enabling us to evaluate large fault trees.

2.5 CONSTRUCTING INITIATING EVENT CUT SETS

SEISIM accepts as input Boolean expressions which represent the initiating events. Several steps are required to generate initiating event input. The first step is to utilize an LLNL code called PIPE. PIPE accepts as input the upper and lower bounds for pipe break size and a pipe descriptor with its associated pipe size (inside diameter). The code PIPE generates a Boolean expression which can be reduced by SETS. This is done by analyzing all the break combinations to see if they fit the bounds. Those that meet this criteria are placed into the Boolean expression.

For example, say we wish to generate a Boolean expression in SETS format for a medium LOCA. The pipe-break upper bound in this case is 6 in. The pipe-break lower bound is 3.001 in. The user then gives a name to each pipe in the reactor coolant loop. These pipe names along with their associated pipe sizes are input into PIPE. PIPE determines the combination of pipe failures that cause the medium LOCA. This is done for each loop independently to make the number of computations reasonable. The four loops can then be put together using an OR gate prior to reduction by SETS.

The next step in this procedure is to take the output (a combination of pipe breaks in Boolean form) from PIPE and reduce this Boolean expression using SETS. In order to put SETS output in a form compatible with SEISIM, we process SETS output using the code SETSIM. This code takes the packed binary output generated by SETS and puts it in a form acceptable to SEISIM. SETSIM creates or adds to the basic event look-up table required by SEISIM (discussed

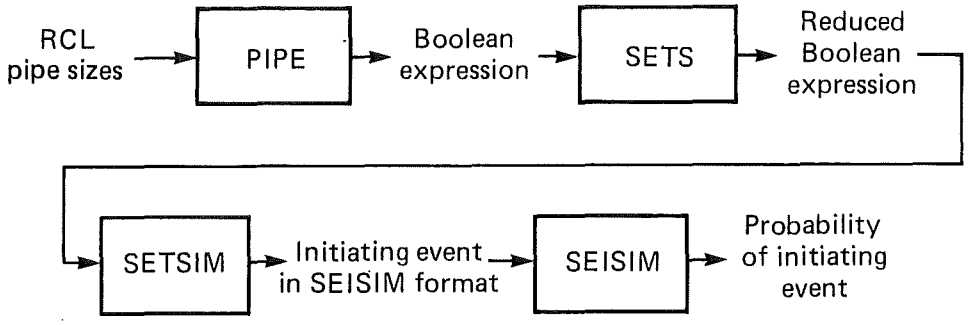


Figure 2.3. Computation of initiating event probabilities.

in Sec. 3) and creates or adds to the initiating event file. This procedure is illustrated in Fig. 2.3.

2.6 GENERATION OF ACCIDENT SEQUENCES

Zion 1 event trees contain 148 accident sequences that lead to core melt. Probabilistic culling, as depicted in Fig. 2.4, will be completed in Phase II using a new version of FTAP (Willie, 1978) and SETS (Worrell, 1981).

SEISIM accepts as input Boolean expressions which represent the accident sequences. Several steps are required in order to generate the Boolean expressions. This procedure is shown in Fig. 2.4. Solving for accident sequences as we do allows us to take into account those basic events that are common between systems (such as electric power).

2.7 CONTAINMENT FAILURE

Containment failure is defined as the failure to contain radioactive materials inside the containment building. The containment failure modes and their corresponding release categories were supplied by Science Applications, Inc., who based them on WASH 1400 and Diablo Canyon Amendment 52. The release categories are defined in Appendix G. The containment event tree lists five failure modes for the PWR containment: (1) containment rupture due to a steam explosion in the reactor vessel, (2) containment rupture due to hydrogen burning, resulting in containment overpressure, (3) containment rupture due to overpressure from other physical processes, (4) containment failure due to melt-through of the containment base mat by the molten core, and (5) failure

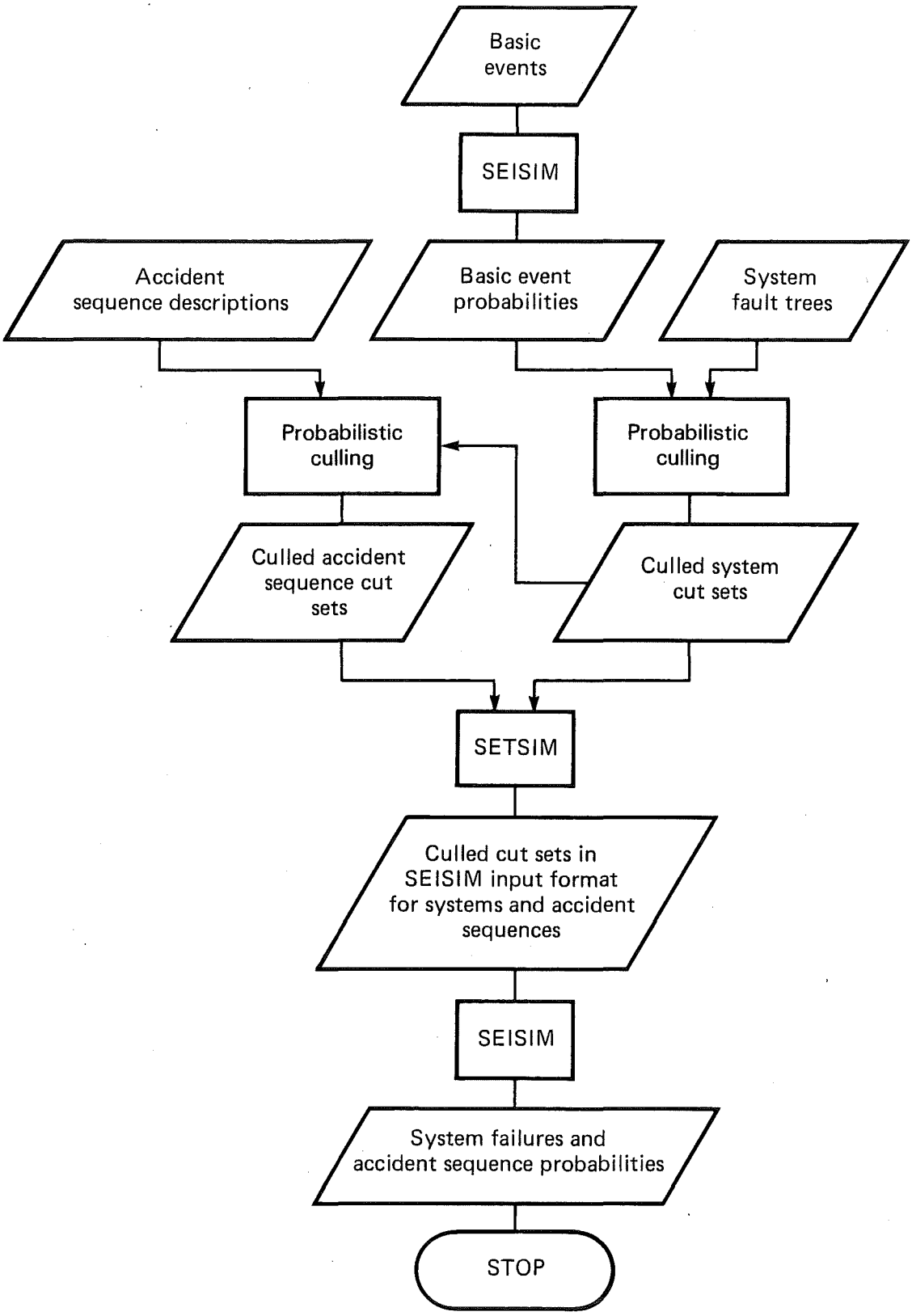


Figure 2.4. Computation of system failure and accident sequence probabilities.

of the containment to isolate (containment leakage). Note that each accident sequence has at least one containment failure mode associated with it. The containment event tree is discussed in detail in Appendix C.

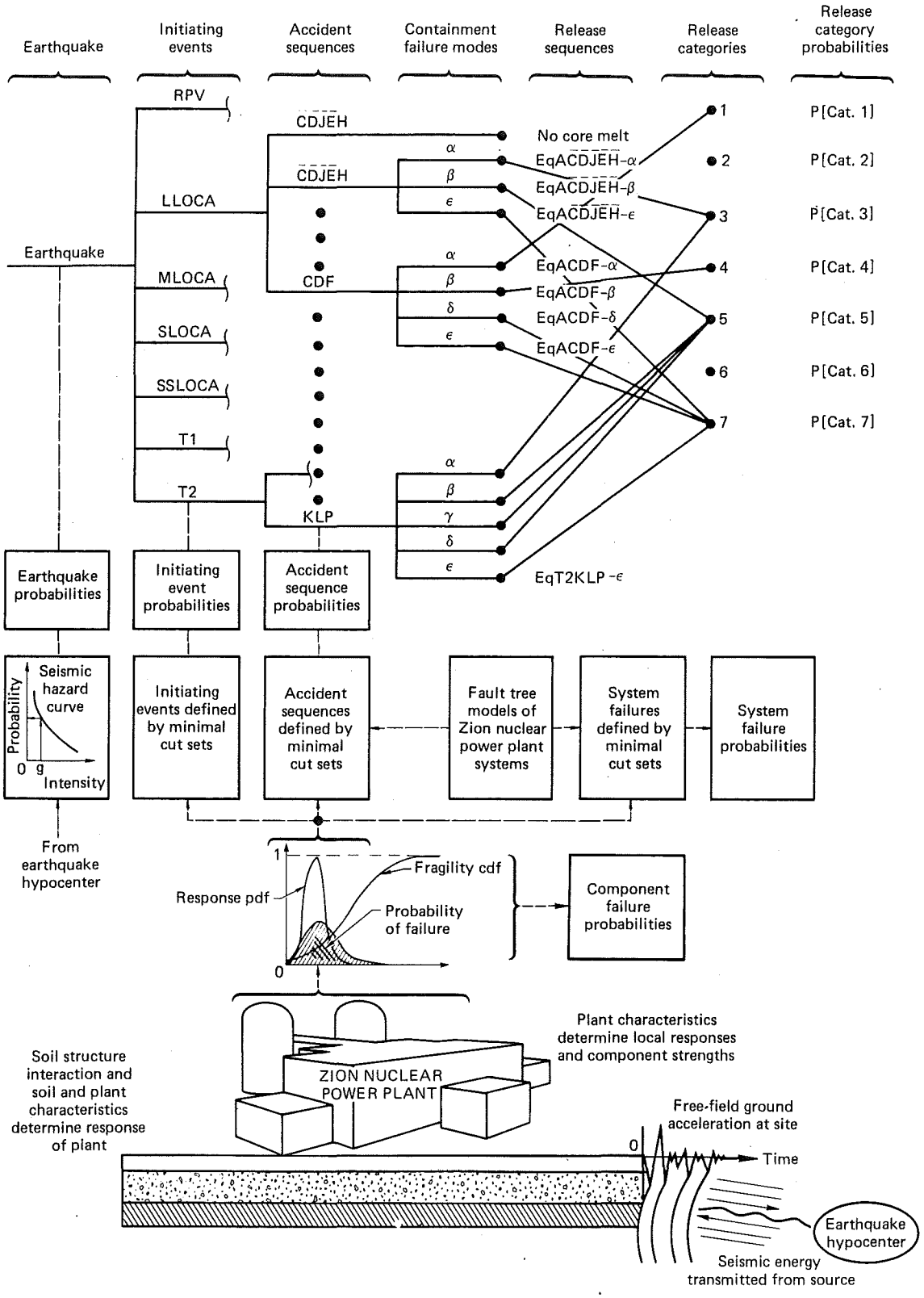


Figure 3.1. Description of the computational procedure embodied in SEISIM.

SECTION 3: COMPUTATIONAL PROCEDURE

3.1 INTRODUCTION

The calculation of radioactive release probabilities in a nuclear power plant subjected to an earthquake requires, first of all, the computation of the responses of components and structures to the earthquake. Next, a determination is made of the probability of failure of each component, structure, and system. The radioactive release probabilities can then be computed. The SEISIM code has been designed to compute these probabilities and to compute sensitivity measures.

Figure 3.1 presents a graphical description of the computational procedure embodied in the SEISIM code. Inputs to SEISIM (see Fig. 3.2) are the SMACS-generated local responses of the reactor structures and components to an earthquake. SEISIM uses this response data to compute the failure probabilities of structures and components using fragility functions. These responses and fragility functions are used to calculate system failure probabilities, initiating event probabilities, accident sequence probabilities, and radioactive release probabilities.

Boolean equations specify the logical failure relationships between structural, piping, and component failures within the nuclear reactor systems. These logical relationships, as discussed in Sec. 2, are input in the form of minimal cut set expressions which define the failure modes of systems in terms of their basic events.

SEISIM computes failure probabilities given dependence between basic events. SEISIM does this by computing the multinormal integral whose integrand is specified by the means, standard deviations, and correlations of responses and fragilities (Johnson and Kotz, 1972). SEISIM processes the inputs shown in Fig. 3.2 to derive the multinormal parameters. The probabilities are computed in the sequence as illustrated in Fig. 3.3. For structures and components, correlation between local responses is accounted for as well as correlation between component strengths (fragilities). For example, if the measured responses of two components are positively correlated, the components will tend to fail or survive together, with the probability of both failing being higher than if their responses were uncorrelated. Correlation between measured local responses is likely because

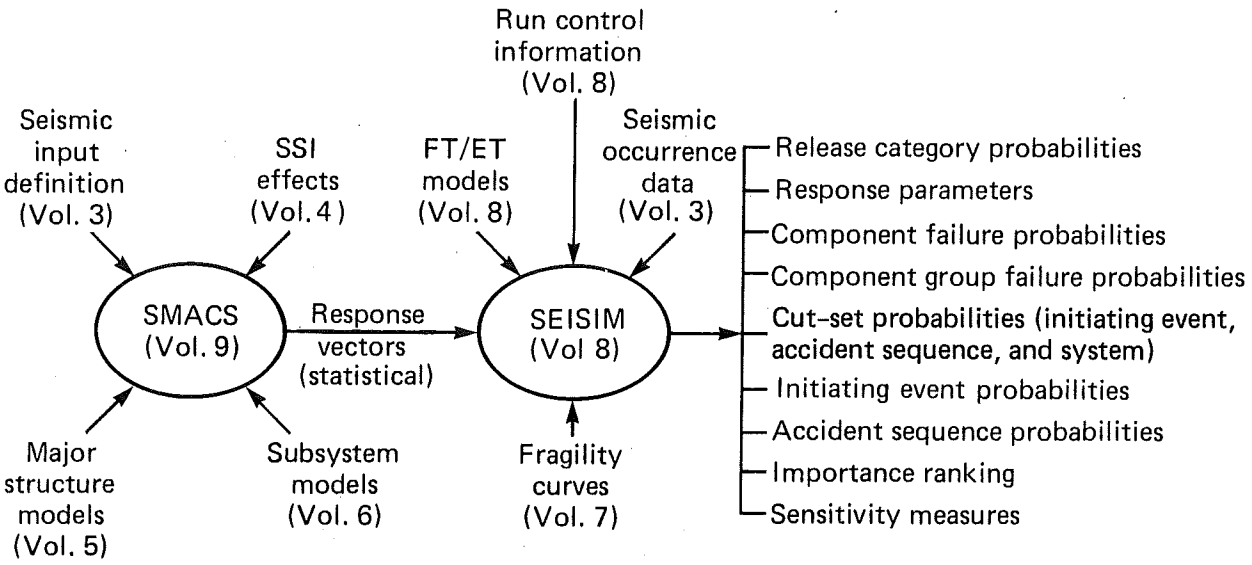


Figure 3.2. SEISIM inputs and outputs.

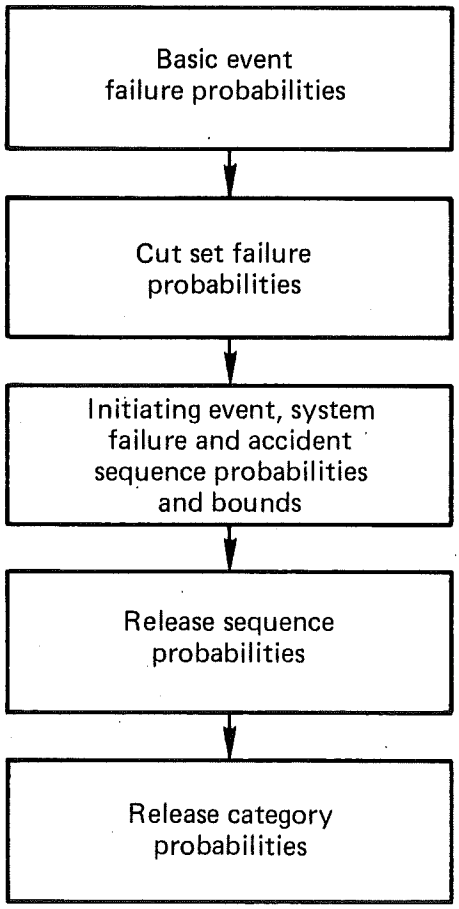


Figure 3.3. SEISIM probability computation sequence.

of the nature of the seismic forcing function and types of systems being analyzed.

The representation of all events in terms of multinormal random vectors allows characterization of dependence by covariances. Specifying the mean vector and covariance matrix completely determines multinormal probability density functions and all events related to multinormal random vectors (Johnson and Kotz, 1972, Vol. IV, Ch. 35). Other models of dependent events are either inappropriate or require more parameters. SEISIM has the capability of handling correlation between fragilities.

SEISIM distinguishes between random and modeling uncertainties. Random uncertainty, as implemented in the program design, represents the inherent randomness of responses and strengths. Random uncertainty occurs as a result of the randomness of the capacities of the structures and components to survive and the randomness of the local responses to the earthquake. Modeling uncertainty represents uncertainty in the distributions or parameters of models, which could be reduced by better modeling or more complete data.

Since it is desired to differentiate between the effects of these two sources of uncertainty, SEISIM computes partial derivatives of the release probabilities as functions of changes in the random and modeling parameters of the responses and fragilities.

There are two aspects of sensitivity analysis that are addressed by the computational methodology. One is the sensitivity of outputs to changes in significant input parameters. These are the partial derivatives.

Another aspect of sensitivity computation performed by SEISIM is called dominance analysis. The objective is to find the components, accident sequences, etc., that most influence the results. This analysis focuses on the event and fault tree models and helps postulate improvements in the seismic design procedure.

3.2 DESCRIPTION OF INPUTS

Figure 3.2 shows the five types of input required by SEISIM (1) structural, piping, and component responses; (2) fragility functions; (3) event-tree/fault-tree derived system failure models; (4) seismic occurrence data; and (5) run control information. These inputs are contained in the eight input files listed in Table 3.1.

3.2.1 Structural, Piping, and Component Responses

The response data are the peak responses computed using the computer program SMACS (see Vol. 9 of this report). These responses are associated with specific points within the reactor. They include structural, piping, and

TABLE 3.1. SEISIM input files.

File name	Contents
INFILE	Run control information: run name and description, integration error control, Hunter's bound control, integration partition counter, integration time limit, earthquake probability, etc.
LUFILE	Basic event look-up file: numbers associated with basic events.
FRFILE	Fragility and random event data: cdf indicators, means and standard deviations, and random event names, probability estimates, and standard deviation estimates, etc.
CRFILE	Cross reference file: acceleration-dependent basic event name, response number, and associated fragility function number.
REFILE	Response file: cdf indicators, primary input variable values, and sample responses.
ASFILE	Accident sequence file: initiating event name, accident sequence number, containment failure modes and associated probabilities and release categories, and cut sets.
IEFILE	Initiating event file: initiating event name and associated cut sets.
LCFILE	Logical component file: system name and associated cut sets.

component responses. For each response point, SMACS generates multiple sample responses. These sample responses are generated by inputting an array of time histories into SMACS.

SEISIM uses these responses to estimate the means, standard deviations, and covariances of the peak local responses resulting from the set of time histories. Option 1 of SEISIM assumes that the local responses are described by either normal or lognormal distributions.

A set of values of primary input variables is given for each set of time histories. This set of values includes SMACS input values such as soil depth, soil modulus, structural stiffness, and damping. This information will be used in our sensitivity studies to determine the effects these variables have on the probability of release.

3.2.2 Fragility Functions

A fragility function is a cumulative distribution function of strength at failure. It must be provided for every component. A response point may be the input for more than one component, with the other component being associated with a possibly different fragility function.

A fragility function, as used in SEISIM, defines the random strength or capacity of a component (or structural element). Note that a fragility function must have the same units as its associated response. Strengths are assumed to be normally or lognormally distributed; therefore, fragility functions can be uniquely defined by their mean strength and standard deviation.

The correlations among component fragilities can be accounted for in SEISIM by a user-specified fragility correlation matrix. For example, like components from the same manufacturer may have correlated strengths; so do welds made by the same welder or welding process.

3.2.3 System Failure Models

The system failure models, i.e., the event trees and fault trees, are described in Sec. 2 and Appendices C and D.

3.2.4 Seismic Occurrence Data

One input to SEISIM is earthquake probability. This input is required for unconditioning the SEISIM output on earthquake magnitude. Let G be the random variable denoting peak ground acceleration of the largest earthquake in one year at the Zion site. Each release category probability is computed in SEISIM conditional on the event that G is contained in one of the six acceleration intervals used in Phase I. SEISIM then multiplies the conditional release category probability by the probability G in each interval to get the probability of a release category and an earthquake in a given interval. The probabilities of the intervals were calculated based on the seismic hazard curve shown in Vol. 3.

3.2.5 Run Control Information

Run control information is information needed by SEISIM to determine which options to exercise and the size of input arrays.

Run control information includes the following elements:

- Unique run number
- An alphanumeric run label
- A textual description of the run
- Probability of the earthquake
- Number of accident sequences
- Number of logical component groups
- Number of initiating events
- Number of containment failure modes
- Number of release categories
- Number of like component groups
- Release category weights, etc.

For more complete information concerning run control information, see the SEISIM Users Manual.

3.3 DESCRIPTION OF OUTPUTS

The outputs generated by SEISIM are as follows (see also Fig. 3.2):

- Release Probabilities. These probabilities are calculated for the PWR release categories defined in WASH 1400 (see Appendix G). The

release probabilities are conditional on a given range of peak acceleration.

- Response Parameters. These parameters are estimates of the response means and standard deviations, response correlations, and covariance matrix.
- Component Failure Probabilities. A probability of failure is calculated for every fragility-related basic event. Note that these probabilities are not used in system, accident sequence, and release probability calculations where dependence of failures may occur. This is illustrated in Fig. 3.1.
- Component Group Failure Probabilities. These probabilities are computed for each system analyzed. Again, note that these probabilities are not used in accident sequence and release probability calculations.
- Cut Set Probabilities. These probabilities are computed for every cut set. They take into account the dependence among fragility related basic events. Section 3.4 discusses some details of the required calculations.
- Event Sequence Probabilities. These include both accident sequence and release sequence probabilities. The accident sequence probabilities are calculated from the cut set probabilities previously computed. The release sequence probabilities include the probabilities of the earthquake, the initiating event, accident sequence, and containment failure.
- Importance Rankings. Importance rankings provide the user with a measure that is related to an event's contribution to the probability of release. Importance measures are generated for basic events, systems, sequences, and primary input variables.
- Sensitivity Measures. SEISIM measures the rate of changes of release category probabilities to changes in the means and standard deviations of responses and fragilities.

3.4 SEISIM ALGORITHMS

SEISIM computes every accident sequence and system failure probability from cut set probabilities. Cut set probabilities are computed as described in Sec. 3.4.1. SEISIM has the capability of computing three different bounds

on the probabilities of system failures and accident sequences. The three bounds are discussed in Sec. 3.4.2.

SEISIM computes each release sequence probability by multiplying the initiating event and accident sequence probabilities by the probabilities of earthquake and containment failure. That is,

P [Release Sequence] = P [Earthquake] X
P [Initiating Event|Earthquake] X
P [Accident Sequence|Initiating Event and Earthquake] X
P [Containment Failure|Accident Sequence, Initiating Event and Earthquake].

The release category probabilities are computed by adding the probabilities of all release sequences that are associated with that release category.

SEISIM sensitivity analyses measure and rank the importance of components, component groups (such as systems or components of the same type), accident sequences, and primary input variables. The importance measure used to determine component group importance is similar to the Vesely-Fussel measure (Lambert, 1975). The importance measure of primary input variables is the derivative of a multivariate regression model of response means on standardized primary input variables.

The remainder of this section describes how cut set probabilities, bounds on system failure probabilities, bounds on accident sequence probabilities, and sensitivity and importance measures are computed.

3.4.1 Cut Set Probabilities

All probabilities of cut sets containing response dependent basic events are converted to multinormal integrals (Johnson and Kotz, 1972), and these integrals are then computed using numerical integration. SEISIM derives the appropriate multinormal parameters from inputs. If a cut set contains random failures as well as response-dependent failures, the probability of the response-dependent failures is multiplied by the probability of the random failures since we assume random failures are independent of response-dependent failures. The rest of this subsection describes computation of response dependent failures.

If a cut set contains more than one component then cut set failure is defined as all responses exceeding their associated strengths. Let $\underline{X} = (X_1,\ldots,X_n)$ and $\underline{Y} = (Y_1,\ldots,Y_n)$ denote the response and strength

vectors, with means $\mu_{\underline{X}}$ and $\mu_{\underline{Y}}$ for a cut set of order n, and let $\underline{Z} = \underline{X} - \underline{Y}$. Then

$$P[\text{failure}] = P\left[Z_1 > 0,\ldots,Z_n > 0\right]$$

$$= \int_0^\infty \cdots \int_0^\infty f_Z(z_1,\ldots,z_n)\, dz_1,\ldots,dz_n$$

where $f_Z(z_1,\ldots,z_n)$ is the joint pdf of $\underline{Z}$. If $\underline{Z}$ has a multinormal density, this integral is

$$P[\text{failure}] = \frac{1}{(2\pi)^{n/2}\,\Sigma_Z^{1/2}} \int_0^\infty \cdots \int_0^\infty \exp\left\{-1/2(z-\underline{\mu}_Z)' \left[\Sigma_Z\right]^{-1}(z-\underline{\mu}_Z)\right\} dz_1 \ldots dz_n$$

where $\underline{\mu}_Z = \underline{\mu}_X - \underline{\mu}_Y$ and Σ_Z is the covariance matrix of $\underline{Z}$. The covariance matrix Σ_Z can be illustrated as follows:

$$\begin{bmatrix} \sigma_{X_1}^2 + \sigma_{Y_1}^2 - 2\,\mathrm{COV}(X_1,Y_1) & \cdots & \mathrm{COV}(Z_1,Z_n) \\ \vdots & & \vdots \\ \mathrm{COV}(Z_n,Z_1) & \cdots & \sigma_{X_n}^2 + \sigma_{Y_n}^2 - 2\,\mathrm{COV}(X_n,Y_n). \end{bmatrix}$$

where $\mathrm{COV}(Z_i,Z_j) = \mathrm{COV}(X_i,X_j) + \mathrm{COV}(Y_i,Y_j) - \mathrm{COV}(X_i,Y_J) - \mathrm{COV}(X_j,Y_i)$. Other covariances are similar.

3.4.2 System Failure and Accident Sequence Probabilities

Because it is impractical to compute the exact probability of complicated events such as system failures and accident sequences, we represent system failures and accident sequences as the unions of cut sets and compute upper bounds on the probabilities of the unions.

SEISIM computes three upper bounds: (Let C_j denote cut set j.)

1. $1 - \prod_{j=1}^{k} (1 - P(C_j))$,

2. $\sum_{j}^{k} P(C_j)$, and

3. $\sum_{j}^{k} P(C_j) - \sum_{(i,j)\epsilon\tau} P(C_i \cap C_j)$

The first bound is the exact probability of a union of independent cut sets and is an upper bound on the probability of a union for associated cut sets of coherent systems (Barlow and Proschan, 1975, p. 35).

The second formula is an upper bound on the probability of a union. However, it does not account for interactions between cut sets and is, therefore, not an accurate bound when cut set probabilities are high.

The third formula (Hunter, 1976) is an improvement on the second because it is obtained by subtracting the probabilities of certain pairs of cut sets from the sum, thereby taking some interaction between cut sets into account. The selection of pairs is done to achieve maximum reduction in the sum and still have an upper bound on system failure probability. Limits on computation time can prevent the user from achieving maximum reduction in the sum using Hunter's bound.

3.4.3 SEISIM Importance Measures

SEISIM computes importance measures for components, component groups, accident sequences, response and strength parameters, and primary input variables. SEISIM then ranks components, systems, and variables on the basis of their importance measures. The ranking is done only for components, systems, and variables that have high ranking importance measures.

The importance measure of components and systems is related to the Vesely-Fussel measure (Lambert, 1975). It is the sum of probabilities of cut sets containing a component or system divided by the probability of some top event such as a release category. This is an approximation to the actual

importance of independent components because the sum of cut set probabilities is an upper bound on the probability of the union of cut sets containing a component. It is not appropriate for components whose failure may be dependent on other component failures in the same cut sets.

The importance measure of response and strength parameters computed in SEISIM is the slope of a chord obtained by dividing the change in a probability by the change in the parameter that caused the probability to change. Only means and standard deviations are changed. Deviatives of component and second order cut set probabilities are calculated with respect to means, standard deviations, and correlations.

The importance measures of accident sequences are their probabilities. The importance measures of primary input variables are the derivatives of multivariate regression models of mean responses on standardized primary input variables evaluated at nominal values of the variables. (Primary input variables are standarized by subtracting their means and dividing the differences by their standard deviations.) If the regression model is linear, the magnitude of the coefficients of standardized variables indicates their importance in mean response models. The regression is done by MULREG (IMSL, 1979) as part of SEISIM.

3.5 SEISIM COMPUTATIONAL FLOW DESCRIPTION

The SEISIM flow diagram is illustrated in Fig. 3.4. The subroutine names are those given in the design specification (Hudson, et al., 1979). This section describes what each subroutine does. Inputs are shown to the left of the subroutine where they are used. Outputs are shown to the right.

3.5.1 Preprocessor

Subroutine PREPROCESSOR reads all inputs and does some preliminary calculations. For example, it checks if inputs are properly formatted and consistent (e.g., containment failure probabilities must add to 1.0, the actual number of cut sets must equal the number specified in the input, etc.).

PREPROCESSOR reads a matrix of peak responses measured at various points on the reactor structure and at the components. Thirty time histories (in

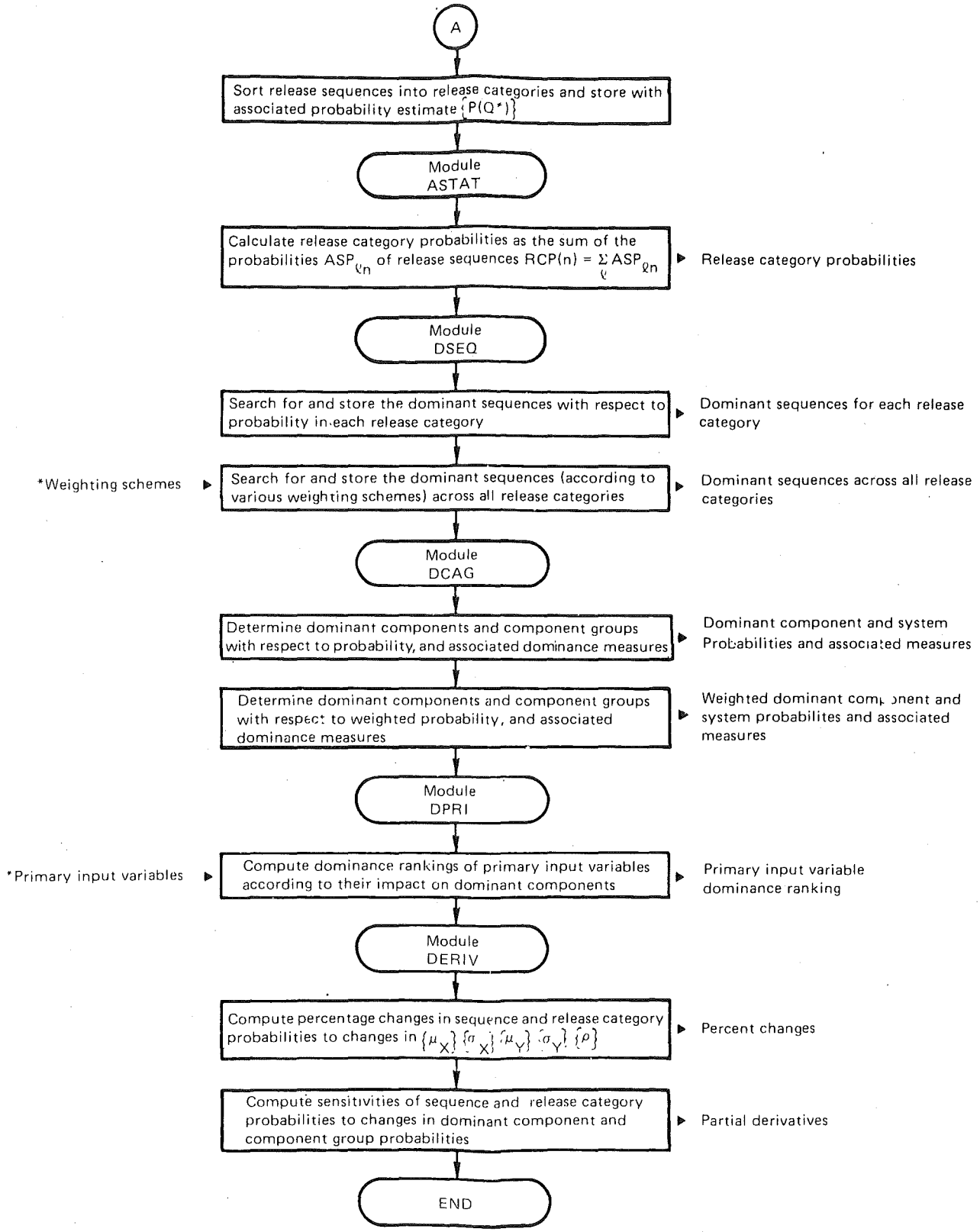
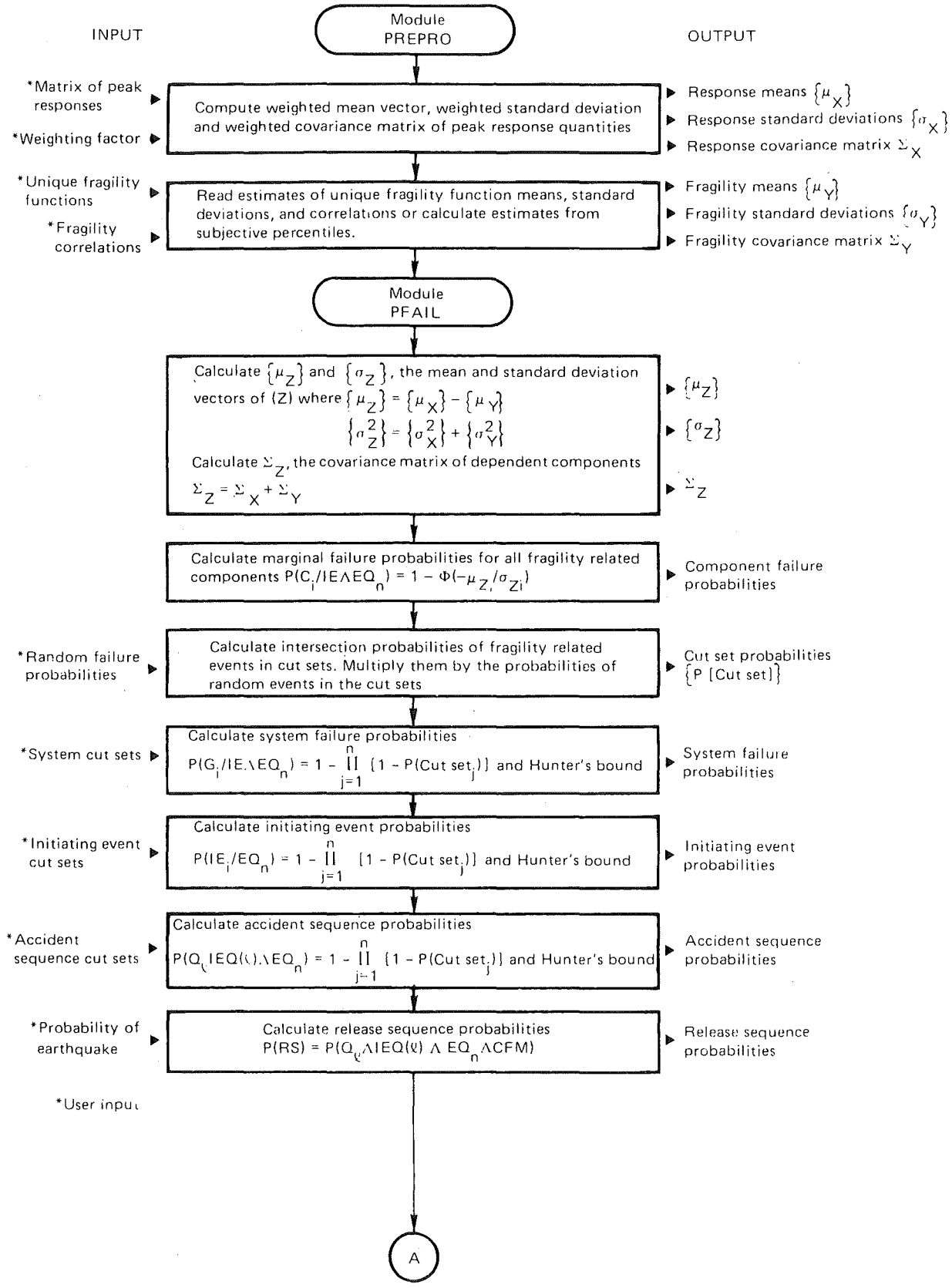


Figure 3.4. SEISIM flow diagram.


INPUT
Module PREPRO
OUTPUT
*Matrix of peak responses
*Weighting factor
Compute weighted mean vector, weighted standard deviation and weighted covariance matrix of peak response quantities
Response means $\{\mu_X\}$
Response standard deviations $\{\sigma_X\}$
Response covariance matrix Σ_X
*Unique fragility functions
*Fragility correlations
Read estimates of unique fragility function means, standard deviations, and correlations or calculate estimates from subjective percentiles.
Fragility means $\{\mu_Y\}$
Fragility standard deviations $\{\sigma_Y\}$
Fragility covariance matrix Σ_Y
Module PFAIL
Calculate $\{\mu_Z\}$ and $\{\sigma_Z\}$, the mean and standard deviation vectors of (Z) where $\{\mu_Z\} = \{\mu_X\} - \{\mu_Y\}$
$\{\sigma_Z^2\} = \{\sigma_X^2\} + \{\sigma_Y^2\}$
Calculate $\Sigma_{Z'}$ the covariance matrix of dependent components
$\Sigma_Z = \Sigma_X + \Sigma_Y$
$\{\mu_Z\}$
$\{\sigma_Z\}$
Σ_Z
Calculate marginal failure probabilities for all fragility related components $P(C_i/IE \wedge EQ_n) = 1 - \Phi(-\mu_{Z_i}/\sigma_{Z_i})$
Component failure probabilities
*Random failure probabilities
Calculate intersection probabilities of fragility related events in cut sets. Multiply them by the probabilities of random events in the cut sets
Cut set probabilities $\{P\ [Cut\ set]\}$
*System cut sets
Calculate system failure probabilities
$P(G_i/IE \wedge EQ_n) = 1 - \prod_{j=1}^{n} \{1 - P(Cut\ set_j)\}$ and Hunter's bound
System failure probabilities
*Initiating event cut sets
Calculate initiating event probabilities
$P(IE_i/EQ_n) = 1 - \prod_{j=1}^{n} [1 - P(Cut\ set_j)]$ and Hunter's bound
Initiating event probabilities
*Accident sequence cut sets
Calculate accident sequence probabilities
$P(Q_\ell/IEQ(\ell) \wedge EQ_n) = 1 - \prod_{j=1}^{n} \{1 - P(Cut\ set_j)\}$ and Hunter's bound
Accident sequence probabilities
*Probability of earthquake
Calculate release sequence probabilities
$P(RS) = P(Q_\ell \wedge IEQ(\ell) \wedge EQ_n \wedge CFM)$
Release sequence probabilities
*User input
A

Phase I) characterized site motion due to earthquakes with peak acceleration in each specified interval. These time histories were used to generate vectors of peak responses for each component. Each vector can be weighted. PREPROCESSOR computes the weighted sample mean vector and the sample covariance matrix for the peak response vectors. If the input specifies a response is lognormally distributed, PREPROCESSOR takes the natural logarithm of the response before it computes sample estimates.

PREPROCESSOR computes fragility means and standard deviations from inputs. If a fragility cdf is specified to be normal, PREPROCESSOR does nothing to the input mean and standard deviation. If a fragility cdf is specified to be lognormal, PREPROCESSOR computes the mean and standard deviation of the logarithm of strength from standard formulas (Kapur and Lamberson, 1977). PREPROCESSOR can estimate means and standard deviations from percentile input (George and Mensing, 1980). The estimates of means and standard deviations used in Phase I were computed from subjective percentiles and test data (see Vol. 7). Lognormal cdf's were specified for all fragility functions in Phase I. Correlations between component strength random variables were set to zero.

3.5.2 PFAIL

The heart of SEISIM is subroutine PFAIL. It computes failure probabilities for structural members, components, and cut sets subject to seismic loading. Every failure probability is a multivariate normal integral. Subroutine PCS, called by PFAIL, constructs the mean vector and covariance matrix of all random variables for events in a cut set. The required multivariate failure probability calculations are performed by subroutine MVNRM within PFAIL. This subroutine does numerical integrations to calculate each response-dependent cut set probability. The actual numerical integration computation is performed by subroutine MDQUAD. If there are any random failures in the cut set, their probabilities are multiplied by the multivariate normal integral representing the probability of response-dependent failures.

3.5.3 ASTAT

ASTAT places the release sequence probabilities in their appropriate release categories. It calculates release category probabilities by summing the release sequence probabilities in each release category.

3.5.4 DSEQ

Subroutine DSEQ searches for and stores important accident sequences and release sequences, both in terms of probability (within each release category) and according to various weighting schemes (across all categories). The weighting schemes are user-defined and may be the fraction of expected core inventory released in each release category for different isotopes. The weighting option allows a comparison between high probability/low release events and low probability/high release events.

3.5.5 DCAG

DCAG determines important accident sequences on the basis of their importance measures. DCAG uses the results to determine the important components, logical component groups (safety systems), and like component groups with respect to both probability (within each release category) and weighted probability (for each user-defined weighting scheme). Importance is determined by the importance measure defined in Sec. 3.4.3.

3.5.6 DPRI

DPRI computes the importance ranking of primary input variables according to their effect on the mean component responses. The primary input variables (such as soil stiffness, soil damping, structural stiffness, and structural damping) have values which have been used in the structural dynamic analysis to compute structural and component responses. DPRI first does multivariate linear regression of response on standardized primary input variables. The result is a matrix of coefficients of the variables in the regression model of mean responses. The largest value of these coefficients for a given response indicates the primary input variable with greatest importance for a response.

3.5.7 DERIV

DERIV measures the change of release category probability and other probabilities due to changes in the means and standard deviations of response and fragility.

3.6 SEISIM VERIFICATION AND LIMITATIONS

Verification of SEISIM has started. It is initially being verified using existing commercial software when possible (see Table 3.2), then by comparing results with known results. The IMSL (International Mathematical and Statistical Libraries, Inc.) subroutines have been validated on LLNL computers. All other software is currently being verified but appears to be generating valid solutions.

3.6.1 Verifications

Single and double component failure probabilities were computed by MDNOR and MDBNOR (IMSL, 1979). Three, four, and five dependent component failure probabilities were compared with MULTI (Wolff, 1981) and NQUAD (Genz and Malik, 1980). This comparison was found to be good.

3.6.2 Size and Theoretical Limitations of SEISIM

This section describes many of the limitations of SEISIM. Many of these limitations can be altered, depending on the application.

Limitations which can be changed include:

- Maximum number of fragility related basic events is 2,000.
- Maximum number of random events is 2,000.
- Maximum number of total basic events is 3,000.
- Cut sets can contain no more than 10 fragility related basic events.
- Cut sets may contain no more than 13 total basic events.
- Maximum number of cut sets for any one system or accident sequence is 5,000.

Table 3.2. SEISIM standard subroutines.

Name	Function	Source	Method of verification
RLMUL[a]	Multivariate regression programs	IMSL	Wide usage
CSORT	Sorting	J. H. Wiggins Co.	Inspection
INVERT	Invert a positive definite symmetric matrix	CACM Algorithm 66	Called by MVNRM
MATMUL	Matrix multiplication	J. H. Wiggins Co.	Called by MVNRM
MATIN, MATOUT	Matrix input and output	J. H. Wiggins Co.	Called by MVNRM
MDQUAD[a]	Multivariate integration by quadrature	Univ. of Wisconsin Computing Center	Wide usage-Comparison with MDBNOR and MULTI
NQUAD	Multivariate integration by quadrature	Genz and Malik, J.A.C.M.	Comparison with MDQUAD and MDBNOR
MULTI	Multivariate integration by Monte Carlo	Prof. R. Wolfe, Univ. of Cal., Dept. of I.E. and O.R.	Comparison with MDBNOR and MDQUAD
MVNRM[a]	Multivariate normal integrals	R. H. Milton, Technometrics	Comparison with MDBNOR and MULTI
VSORT	Sorting	J. H. Wiggins Co.	Inspection
WSTAT	Estimating mean vector and covariance matrix	J. H. Wiggins Co.	Inspection
MDNOR[a]	Single normal integral	IMSL	Wide usage-Comparison with tables
MDBNOR[a]	Bivariate normal integral	IMSL	
DMTOMS	Maximal spanning tree	Algorithm 422 CACM	Test problems
MDNRIS[a]	Invert the normal cdf	IMSL	Wide usage

[a]The subroutines called by these subroutines are presumed to be valid if the calling subroutine is valid.

- Integration time limit for calculating cut set probability is 5 CPU seconds.*
- Absolute error on each multinormal integral is set at less than $\pm 10^{-5}$.
- Maximum length of response vector is 51.
- Maximum number of peak responses in each vector is 350.
- Maximum number of fragility categories is 50.

Other limitations, however, are not easily changed. These include limitations due to our Option 1 methodology, such as requiring fragility and response distributions to be either normal or lognormal.

*Runs were made on a CDC 7600 computer.

SECTION 4: CONCLUSIONS AND PLANNED FUTURE WORK

4.1 CONCLUSIONS

We have demonstrated a method and developed a computer code for computing failure probability of large systems of dependent components. It can be used for any large system reliability analysis which has dependent failures and uses a Boolean failure model such as a fault tree.

4.2 PLANNED FUTURE WORK AND RECOMMENDATIONS FOR IMPROVING SEISIM

The following work is planned for the subsequent phases of the SSMRP.

1. Probabilistically cull fault trees and accident sequences to reduce the numbers of cut sets.
2. Conduct sensitivity studies to determine important components, systems, accident sequences, primary input variables, and response and fragility parameters.
3. Perform sensitivity analysis on systems not currently represented by fault trees in accident sequences. This will determine the error caused by simplification.
4. Program a more accurate upper bound on the probability of a union of cut sets representing accident sequences.
5. Construct statistical confidence intervals on the release histogram that simultaneously limit the probabilities in all release categories with a specified confidence coefficient. These intervals indicate the uncertainty due to sampling error in response and fragility data.
6. Program a Monte Carlo procedure into SEISIM and compare its results with the current analytical results. This will help verify the current version of SEISIM and may allow us to handle more and higher order cut sets. It will also allow us to eliminate the restriction of using normal and lognormal distributions on responses and fragilities.
7. Develop component importance measures appropriate for dependent events. The importance measures currently used are not always appropriate when dependent events are present.

8. Program SEISIM to model responses and fragilities as a mixture of lognormal and normal cdf's.

This list is by no means complete, but it does give the reader some idea of the work that is planned for Phase II. Implementation of these ideas will provide the SSMRP with a greater capability and more flexibility.

REFERENCES

Abramowitz, M., and I. A. Stegun (1965), Handbook of Mathematical Functions (Dover Publ., New York, NY).

Abramson, L. R. (April 1, 1976), "Constructing Correlated Random Variables with Fixed Marginals," ORSA/TIMS Joint National Meeting, Philadelphia, PA.

Ang, A. H.-S., and N. M. Newmark (November 1977), A Probabilistic Seismic Safety Assessment of the Diablo Canyon Nuclear Power Plant, Report to U.S. Nuclear Regulatory Commission (N. M. Newmark Consulting Engineering Services, Urbana, IL).

Barlow, R. E., and H. E. Lambert (1975), "Introduction to Fault Tree Analysis," Reliability and Fault Tree Analysis (SIAM, Philadelpha, PA).

Barlow, R. E., and F. Proschan (1975), Statistical Theory of Reliability and Life Testing - Probability Models (Holt, Rinehart, and Winston, New York, NY).

Bley, D. C., C. L. Cate, D. C. Iden, B. J. Garrick, and J. W. Hudson (September 1979), Seismic Safety Margins Research Program (Phase I), Project VII - Systems Analysis Event Tree Methodology Development, Report PLG-0110 (Pickard, Lowe, and Garrick, Inc., Irvine, CA).

Gallagher, L. J. (July 1971), "Algorithm 440, A Multidimensional Monte Carlo Quadrature with Adaptive Stratified Sampling," Collected Algorithms from ACM (Assoc. for Computing Machinery, New York, N.Y.).

Garcia, A. A., and J. E. Kelly (August 1979), Event Tree Development and Construction, SAI-003-79-BE (Science Applications, Inc., Palo Alto, CA).

Garcia, A. A., J. E. Kelly, P. J. Amico, W. J. Parkinson, and F. L. Leverenz (August 1979), Seismic Safety Margins Research Program (Phase I), Interim Report, Project VII Systems Analysis, Event Tree Development and Construction, Report No. SAI-003-79-BE, (Science Applications, Inc., Bethesda, MD 20014).

Genz, A. C., and A. A. Malik (1980, "Remarks On Algorithm 006, An Adaptive Algorithm for Numerical Integration over an N-Dimensional Rectangular Region," J. Computational and Applied Math, 6(4).

George, L. L., and J. E. Wells (May 1981), "The Reliability of Systems of Dependent Components," Proceedings of the ASQC Quality Congress (American Society of Quality Control, San Francisco, CA).

George, L. L. (Sept. 1981), Statistical Sensitivity Analysis Methods in SSMRP, unpublished draft (Lawrence Livermore National Laboratory, Livermore, CA).

George, L. L. (December 1978), System Interference Analysis (Department of Ind. Eng., Texas A & M University, College Station, TX).

George, L. L. (In preparation), Probability Computation Methods in SSMRP,UCID-18686, unpublished (Lawrence Livermore National Laboratory, Livermore, CA).

Haber, S. (1966), "A Modified Monte Carlo Quadrature," Mathematics of Computation 20, 361-368.

Haber, S. (1967), "A Modified Monte Carlo Quadrature II," Mathematics of Computation 21, 388-397.

Haber, S. (July - November 1968), "A Combination of Monte Carlo and Classical Methods for Evaluating Multiple Integrals," Bull. Am. Math. Soc. 74, 683-686.

Haber, S. (1969), "Stochastic Quadrature Formulas," Mathematics of Computation 23, 751.

Hoeffding, Wassily (ca 1965), "Asymptotically Optimal Tests for Multinomial Distributions," J. Roy Statist. Soc., Series B, pp. 369-408.

Huber, P. J. (1977), Robust Statistical Procedures (SIAM, Philadelphia, PA).

Hudson, J. M., and J. D. Collins (April 1980), "Prediction of Accident Sequence Probabilities in a Nuclear Power Plant Due to Earthquake Events," in Proc. Topical Mts. on Reactor Safety, Knoxville, TN (American Nuclear Society (ANS) and European Nuclear Society, La Grange, IL).

Hudson, J. D., Gasca, and J. D. Collins (April 1980), SEISIM Option 1 Design, Specification (Revision 1), J. H. Wiggins Company Technical Report 80-1366-1 (J. H. Wiggins Co., Redondo Beach, CA).

Hudson, J. M., J. D. Gasca, and B. Kennedy (July 1980), SEISIM Option 1 User's Manual, (Revision 1), J. H. Wiggins Company Technical Report No. 80-1366-2, 1650 (J. H. Wiggins Co., Redondo Beach, CA).

Hudson, J. M., and J. Gasca (1981), "Common Mode Failure in Nuclear Power Plants," in Proc. Reliability and Maintainability Symposium (IEEE, New York, NY).

Hunter, D. (1976), "An Upper Bound on the Probability of a Union," Journal of Applied Probability 13, 597-603.

International Mathematics and Statistics Library, Inc. (1979), IMSL Library Reference Manual, Vols. I and II, Edition 7 (IMSL, Houston, TX).

Johnson, N. L., and S. Kotz (1972), Distributions in Statistica: Continuous Multivariate Distributions (Wiley, New York, NY).

Kapur, K. C., and L. L. Lamberson (1977), Reliability in Engineering Design (Wiley, New York, NY).

Kevin, V., and M. Whitney (1971), "Algorithm 422, Minimal Spanning Tree," Collected Algorithms from ACM (Assoc. for Computing Machinery, New York, NY).

Lambert, H. E. (1975), "Measures of Importance of Events and Cut Sets in Fault Trees," Reliability and Fault Tree Analysis, pp. 83-84 (SIAM, Philadelphia, PA).

Lumel'skii, Ya. P. (1968), "Unbiased Sufficient Estimation of Probability for the Multivariate Normal Distribution," (in Russian) Vestnik Moskovskogo Universiteta, No. 6, pp. 14-17 (Moscow, Russia).

Milton, R. C. (1972), "Computer Evaluation of Multivariate Normal Integral," Technometrics 14(4), 881-889.

Moieni, P., G. Apostolakis, and G. E. Cummings (1980), Interim Report on Systematic Errors in Nuclear Power Plants, UCRL-15274, NUREG/CR-1722 (Lawrence Livermore National Laboratory, Livermore, CA).

Pacific Gas and Electric Co., (August 1977), Department of Engineering, Analysis of the Risk to the Public from Possible Damage to the Diablo Canyon Nuclear Power Station from Seismic Events, Dockets 50-275-OL and 50-323-OL (P G and E, San Francisco, CA).

Rackwitz, R., and B. Krzykacz (May 1978), "Structural Reliability of Reactor Systems," ANS Meeting on Probabilistic Analysis of Nuclear Reactor Safety (ANS, Los Angeles, CA).

Scheffé, H. (1959), The Analysis of Variance (Wiley, New York, NY).

Science Applications, Inc. (May 14, 1980), Zion Unit 1 Auxiliary Feedwater System Fault Tree, Draft Report, Seismic Safety Margins Research Program (SSMRP)(SRI, Palo Alto, CA).

Science Applications, Inc. (May 30, 1980), Zion Unit 1 Electrical Power System Fault Tree, Draft Report, Seismic Safety Margins Research Program (SSMRP)(SRI, Palo Alto, CA).

Science Applications, Inc. (June 27, 1980), Zion Unit 1 Service Water System Fault Tree, Draft Report, Seismic Safety Margins Research Program (SSMRP)(SRI, Palo Alto, CA).

Science Applications, Inc. (July 1980), Zion Unit 1 Emergency Core Cooling System Fault Tree, Draft Report, Seismic Safety Margins Research Program (SSMRP)(SRI, Palo Alto, CA).

Smith, P. D., D. L. Bernreuter, M. P. Bohn, T. Y. Chuang, G. E. Cummings, R. G. Dong, J. J. Johnson, R. W. Mensing, and J. E. Wells (1980), An Overview of Seismic Risk Analysis for Nuclear Power Plants, UCID-18680 (Lawrence Livermore National Laboratory, Livermore, CA).

Smith, P. D., and R. G. Dong (September 1980), Seismic Safety Margins Research Program (Phase 1), Definition of Terms, UCRL-53001 (Lawrence Livermore National Laboratory, Livermore, CA).

Smith, P. D., and R. G. Dong (December 1980), Seismic Safety Margins Research Program (Phase I) Interim Definition of Terms, UCRL-53001 (Lawrence Livermore National Laboratory, Livermore, CA).

Tukey, J. W. (1979), "Methodology and the Statistician's Responsibility for BOTH Accuracy AND Relevance," Journal of the American Statistical Association 74, 786-793.

U.S. Nuclear Regulatory Commission (1975), An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants, WASH 1400 (NUREG-75/014)(U.S. Nuclear Regulatory Commission, Washington, D.C.).

Van Marcke, E. H. (1973), "Matrix Formulation of Reliability Analysis and Reliability Based Design," Computers and Structures 4, 757-770.

Vesely, W. V., F. F. Goldberg, N. H. Roberts, and D. F. Haasl (Jan. 1981), Fault Tree Handbook, NUREG-0492 (U. S. Nuclear Regulatory Commission, Washington, D.C.).

Wall, I. B., M. K. Kaul, R. I. Post, S. W. Tagart, and T. J. Vinson (Feb. 1978), Seismic Safety Margins Research Program (Phase I) Project VII - Systems Analysis Specification of Computational Approach, UCRL-13985. Prepared by Nuclear Services Corporation, Campbell, CA (Lawrence Livermore National Laboratories, Livermore, CA).

Willie, R. R. (August 1978), Computer-Aided Fault Tree Analysis, ORC 78-14 (Operations Research Center, University of California, Berkeley, CA).

Wolff, R. W. (April 1981), Simulation Methods for Evaluating Seismic Methodology Procedures (Operations Research Center Report, University of California, Berkeley, CA).

Worrell, R. B., and D. W. Stack (Nov. 1978), A Sets User's Manual for the Fault Tree Analyst, NUREG/CR-0465, SAND77-2051 (Sandia Laboratories, Albuquerque, NM).

Worrell, R. B. (1981), "Notes on Changes to SETS Program," Unpublished (Sandia Lab, Albuquerque, NM).

APPENDIX A

GLOSSARY OF TERMS

ACCELERATION, ZPA. The zero period, free-field, peak acceleration due to an earthquake, usually measured in units of g = 32.2 ft/s^2.

ACCIDENT SEQUENCE. A sequence of failures or successes of safety systems caused by an initiating event. Accident sequences are branches of event trees. Several accident sequences are possible for a given event tree, each describing a different branch. Phase I SEISIM* runs analyzed only those sequences that result in core melt.

ASSOCIATION. A property of random variables. Random variables $T_1 \ldots T_n$ are associated if $\mathrm{cov}(\Gamma(T_1 \ldots T_n), \Delta(T_1 \ldots T_n)) > 0$ for all pairs of nondecreasing binary functions Γ and Δ. Association is a form of dependence [4]**.

BASIC EVENTS. The failure of system components, such as piping, valves, pumps, and relays. These events initiate paths through the fault trees.

BOOLEAN EXPRESSION. A set or event derived from any other sets or events in a sample space by $\cap$, intersection; U, union; and complement [1].

COMMON CAUSE FAILURE. Dependent failure events. For example, redundant components or systems are often installed; however, if they are all located in the same area of the plant, they will experience virtually the same vibration during an earthquake. If one system or component fails, the others will also tend to fail; thus the benefit of redundancy may be lost. Other examples of common cause failure are errors due to operator, test, maintenance, design, manufacturing, and construction; and other common environments (such as fire or flood).

COMPLEMENT (of a set). The complement of set A relative to a sample space S, denoted A' or A, is the set which consists of all elements of S that do not belong to $\bar{A}$.

---

*Seismic Evaluation of Important Safety Improvement Measures
**Numbers in brackets refer to the references listed at the end of the Glossary.

CONDITIONAL DISTRIBUTION FUNCTION. The distribution function of a random variable X (or the joint distribution of several random variables) when the values of one or more other random variables Y are held fixed, or some other event has occurred, $P[X < x | Y = y] = F_X(x|y)$.

CONDITIONAL PROBABILITY. For any two events--A and B--the conditional probability of A given B, denoted $P(A|B)$, is the probability that A will occur given that B has occurred or will occur.

CONFIDENCE COEFFICIENT. The probability, prior to taking a sample, that an interval estimator will contain the value of the parameter being estimated.

CONFIDENCE INTERVAL. An interval estimate, associated with a level of confidence, of the value of a parameter.

CONFIDENCE INTERVAL ESTIMATOR. An interval for which one can assert with a given confidence $1 - \alpha$, called the confidence coefficient, that the interval will contain the parameter it is intended to estimate. The end points of a confidence interval are referred to as the upper and lower confidence limits; they are generally values of random variables calculated from sample data. A confidence interval is said to be one-sided when only one of the limits is a value of a random variable, while the other limit is a constant or infinite.

CONFIDENCE SET (or region). A generalization of a confidence interval which applies to the simultaneous estimation of several parameters. See, for example, the discussion of confidence regions for the simultaneous estimation of the mean and the variance of a normal population, in Wilks [4] page 95. See also Scheffé [2] page 29, on confidence ellipsoids.

CORRELATED SAMPLES. Two samples consisting of paired data, such as crack depth and length, which have a non-zero sample coefficient of correlation.

CORRELATION. One measure of the linear functional dependence between two variables.

CORRELATION COEFFICIENT. (1) For two random variables X and Y, the ratio of their covariance and the product of their standard deviations $COV(X,Y)/\sqrt{VarX\ VarY}$. (2) A measure of the linear relationship between two quantitative variables, known also as the Pearson product-moment coefficient of correlation. This linear relationship is denoted by the letter r, and its values range from -1 to +1, where 0 indicates the absence of any linear relationship, -1 indicates a perfect negative (inverse) relationship, and +1 indicates a perfect positive (direct) relationship.

CORRELATION MATRIX. The matrix whose elements are correlation coefficients: that is, for i = j the element a_{ij} of the matrix is the correlation coefficient for the i-th and j-th variables, while $a_{ii} = 1$ for all i.

COVARIANCE. (1) The expected value of the product of the deviations of two random variables from their respective means, and (2) the sample measure of the "population" covariance usually evaluated by the sum of the products of the deviations of the sample values from their respective sample means divided by one less than the sample size.

CUMULATIVE DISTRIBUTION FUNCTION (cdf). A function F(t) used to describe the probability distribution of a random variable, whose values are the probabilities that a random variable assumes a value less than or equal to t for all values of t. The function is the area under the pdf for all values less than t.

CUT SET. A set of component failures which prevent a safety system from serving its intended function. The minimal cut set is the minimum set of component failures which renders a safety system inoperable. The top event of a fault tree is the union of all minimal cut sets. Cut sets for accident sequences are intersections of cut sets for the top events representing each system failure in the accident sequence (excluding system survivals).

ESTIMATE. A value or interval of values, based on a sample or other information, which is intended to approximate the unknown value of a parameter of a mathematical model.

ESTIMATOR. A function of sample or other information used to derive an estimate of the unknown value of a parameter of a mathematical model.

EVENT. In probability theory, an event is a subset of a sample space. Thus, "event" is the nontechnical term and "subset of a sample space" is the corresponding mathematical term. For example, the event of rolling a ten with a pair of dice is the subset which consists of the outcomes where the first die comes up four and the other six, where both dice come up five, and where the first die comes up six and the other four [1].

EVENT TREE. Defines sequences of system failures which may lead to the release of radioactive material. The probability of each system failure is determined by the use of fault trees generated for each system. Each tree is associated with an initiating event. Initiating events are defined in this Appendix. The event tree/fault tree method begins with an initiating event, tracks subsequent events based on the probability of failure of various safety systems, and determines the probability of various levels of radioactive material release.

EXPECTED VALUE. A random variable weighted with respect to its pdf.

EXPERIMENTAL DESIGN. The statistical aspects of the design (or planning) of an experiment are: (1) selecting the treatments (factors and their levels) whose effects are to be studied; (2) specifying a layout for the experimental units (plots) to which the treatments are to be applied; (3) providing rules according to which the treatments are to be distributed among the experimental units; and (4) specifying what measurements are to be made for each experimental unit. For each of these elements, the techniques to be used in the analysis of the results must be clear prior to the experiment [1].

EXPERIMENTAL ERROR. The errors, or variations, not accounted for by hypothesis. In the analysis of variance, their magnitude is estimated by the error sum of squares. Extraneous variables are the presumed cause of an experimental error. Such errors are often combined under the general heading, "chance variation." Note that in this sense the word "error" does not mean "mistake." See also Sampling Error [1].

HAZARD CURVE (seismic). The complement of the cdf of the peak acceleration of the largest earthquake that occurs in a specified time, usually one year. The ordinate is the probability of having at least one earthquake within the specified time with an acceleration exceeding a value on the axis of the curve.

INDEPENDENT EVENTS. Two events--A and B--are independent if and only if the probability that they will both occur equals the product of the probability of A and the probability of B.

INDEPENDENT RANDOM VARIABLES. Two or more random variables are independent if and only if the values of their joint distribution function are given by the products of the corresponding values of their individual (marginal) distribution functions. If random variables are not independent, they are dependent [1].

INITIATING EVENTS. Events which activate the safety systems of a nuclear power plant. An event tree is associated with each initiating event. Two major categories of initiating events are recognized: pressure-boundary rupture and transient initiation. These categories are subdivided according to the capabilities of the particular plant and safety systems activated. An example of a pressure-boundary rupture is the rupture of a large pipe. A transient initiation does not involve rupture; an example is the loss of the main steam system.

INTERSECTION (of two sets). The intersection of two sets--A and B--(denoted $A \cap B$) is the set which consists of all elements that belong to both A and B [1].

INTERVAL ESTIMATION. The estimation of a parameter in terms of an interval, called an interval estimator, for which one can assert with a given probability (or degree of confidence) that it contains the actual value of the parameter. See also Confidence Interval; Confidence Set (or region) [1].

LOSS FUNCTION. A numerical value, $L(a,\theta)$, which reflects the cost of experimentation and rewards and penalties for making good, poor, correct, or incorrect decisions. This numerical function is assigned to each pair (a,θ) of actions, a, taken by the experimenter and to values of the parameter, θ, under consideration [1].

MATHEMATICAL EXPECTATION. The mathematical expectation of a random variable, X, is given by the mean of its distribution and is denoted $E(X)$ or μ_X.

MEAN. (1) the expected value of a random variable; (2) the average of a sample; and (3) the arithmetic average of a set of numbers (e.g., the sum of n numbers divided by n).

MEDIAN. (1) For ungrouped data, the value of the middle item (or, by convention, the mean of the values of the two middle items) when the items in a set are arranged according to size. (2) For the distribution of a random variable, the value (or any one of the set of values) for which the distribution function equals 1/2, or a point of discontinuity--say x_0, such that the value of the distribution function is less than 1/2 for $x < x_0$ and greater than 1/2 for $x \geq x_0$ [1].

MODE. (1) A measure of location defined as the value of a random variable (or in the case of qualitative data, the attribute) which occurs with the highest frequency. Note that a set of data (or a distribution) can have more than one mode, or no mode at all, when no two values are alike. (2) For the distribution of a random variable, a mode is a value of the random variable for which the probability function or the probability density has a relative maximum [1].

MODEL. A representation of a theory, usually mathematical, which describes the inherent structure of selected aspects of a phenomenon, or process, which generates observed data. An equation which expresses a relationship among pertinent variables of a model is referred to as a model equation.

MONTE CARLO METHOD. A method of approximating solutions of problems in mathematics (and related problems in the natural and social sciences) by sampling from simulated random processes. Such sampling is usually performed with the use of random numbers and special computer techniques. Note that Monte Carlo methods are not necessarily random event simulations.

MUTUALLY EXCLUSIVE EVENTS. In probability theory, two events are mutually exclusive if and only if they are represented by disjoint subsets of the sample space; namely, by subsets which have no elements in common. An alternative definition is that two events are mutually exclusive if and only if their intersection has a zero probability [1].

PARAMETER. In statistics, a numerical quantity (such as the mean) which characterizes the cdf of a random variable or population. It is usually denoted by a Greek letter to distinguish it from a corresponding sample parameter.

POINT ESTIMATION. The estimation of a parameter by assigning it a unique value, called a point estimate. The merits of a method of point estimation are assessed in terms of the properties of the estimator which give rise to the particular estimate: for example, consistency, sufficiency, relative efficiency, minimum variance, and lack of bias [1].

PRIMARY INPUT VARIABLE. A variable in the seismic design chain: for example, soil modulus, soil depth, structural stiffness, and structural damping. The SEISIM code computes importance rankings of these primary input variables according to their effect on mean peak responses.

PROBABILITY. A function defined for the set of all events obtainable from events in a sample space by $\cap$, U, and complement. The values of the function lie in the real interval [0,1]. The function satisfies the axioms of probability.

PROBABILITY DENSITY FUNCTION (pdf). A nonnegative function used to describe the probability distribution of a random variable.

RANDOM EVENT. An event whose occurrence is not certain.

RANDOM SAMPLE. (1) A sample of size n from a finite population of size N is said to be random if it is chosen so that each of the $\binom{N}{n}$ possible samples has the same probability of being selected. Such samples are also referred to as simple, or unrestricted, random samples. (2) A set of observations constitutes a random sample of size n from an infinite population if the n observations are values of independent random variables having the same population distribution [1].

RANDOM VARIABLE. A variable which assumes the values in its range in a way describable by a probability distribution.

REGRESSION. The relationship between the conditional mean of a random variable and one or more independent variables. A mathematical equation expressing this kind of relationship is called a regression equation. When the regression equation is linear, the regression is also referred to as linear; when the regression equation represents a curve, the regression is termed curvilinear. The term "regression" was first used by Francis Galton in a study of the heights of fathers and sons. Galton observed a regression (or turning back) to the heights of their fathers from the heights of the sons [1].

REGRESSION ANALYSIS. The analysis of paired data (X_1,Y_1), (X_2,Y_2) ... (X_n,Y_n), where the Xs are constants and the Ys are values of random variables. A normal regression analysis is one in which the Ys are values of independent random variables which have normal distributions with the respective means, $a + bX_i$, and the common variance, σ^2. The term "regression" is also applied to the analysis of n-tuples of data, where the values of the independent variables are looked upon as constants, and the values of the dependent variable are values of random variables [1].

REGRESSION COEFFICIENT. (1) A coefficient in a regression equation. An example is the parameters a and b in the linear regression equation $Y = a + bX$. (2) Corresponding estimates. However, the preferable reference is "estimated regression coefficients."

RELEASE CATEGORIES. A measure of the type and amount of radioactive material released. These are functions of accident sequences and containment failure modes.

RELEASE SEQUENCE. The intersection of earthquake, initiating event, accident sequence, core melt, and containment failure.

RELEASE SEQUENCE PROBABILITY. The product of the probabilities of earthquake, initiating event, accident sequence, and containment failure.

RELIABILITY. The reliability of a product (component, unit, etc.) is the probability that it will perform within specified limits for at least a specified length of time under given environmental conditions. This can be stated mathematically with the following formula: $P[X > x]$, where X is the random variable representing the time to the first failure and is greater than some value, x.

RESPONSE SURFACE ANALYSIS. Statistical methods of prediction and optimization, including (among others) regression analysis and factorial experimentation. In particular, methods leading to experimental conditions for which the response of a dependent variable (or variables) is carried to the maximum or minimum degree, and the response of the dependent variable in the vicinity of the optimum point is studied [1].

SAMPLE DESIGN. A plan for obtaining a sample from a given population. The plan is completely specified before any data are collected. Alternate terms are "sampling plan" and "survey design." See also Stratified Random Sampling [1].

SAMPLE SPACE. In probability theory, a set of points (elements) which represents all possible outcomes of an experiment [1].

SAMPLING ERROR. The error in the value of an estimator caused by using sample data instead of the full population.

SEISIM. Systematic Evaluation of Important Safety Improvement Measures. This is a computer program that derives its inputs from

- seismic hazard curves,
- event and fault trees,
- response input vectors,
- fragility curves, and
- release category relationships.

It calculates

- probabilities of failure of components and systems,
- probabilities of accident sequences,
- probabilities of releases in each of the categories due to earthquakes,
- importance rankings, and
- sensitivity measures.

SENSITIVITY. (1) The degree of response to stimulation, or (2) the rate of change of one variable as other variables change [3].

SIMULATION. The artificial generation of random processes, usually by means of random numbers or computers, to imitate or duplicate actual physical processes. See also Monte Carlo Methods [1].

SPANNING TREE. A set of arcs (edges, links) that connects all nodes of a network.

STANDARD DEVIATION. (1) The standard deviation of a sample of size n ("sample standard deviation") is usually the square root of the sum of the squared deviations from the mean divided by n - 1. This is the most widely used measure of the variation of a set of data, and it is generally denoted by the letter s. To obtain the standard deviation, some statisticians prefer to divide by n, rather than by n - 1: for this reason the standard deviation has also been referred to as the root-mean-square deviation, and it may be described as the square root of the second moment about the mean. The square of the sample standard deviation is called the sample variance. (2) The standard deviation of the distribution of a random variable is given by the square root of the variance, and it is generally denoted by the Greek letter

σ : such a standard deviation is referred to as a population standard deviation.

SUBJECTIVE PROBABILITY. The interpretation of probabilities on the strength of a person's belief concerning the occurrence or nonoccurrence of events. This point of view is gaining in favor. The use of subjective probabilities is advocated in conjunction with methods of Bayesian inference [1].

SYSTEMATIC ERROR. A nonrandom error which introduces a bias into all the observations. One cause of such an error might be faulty or poorly adjusted measuring instruments [1].

TOP EVENT. The event on the top of a fault tree. A fault tree is constructed for each safety system. Under seismic excitation, components fail, which may lead to the system's inability to serve its safety functions. The system's inability to serve its safety functions is the top event for the fault tree.

UNCERTAINTY. (1) Randomness: we do not know the value of a random variable, but we know its cdf. (2) Uncertainty due to lack of knowledge: we do not know even the cdf of a random variable.

UNION. Given set A and set B, the union of A and B is all elements either in A or in B or in both [1].

VALUE. A real number.

VARIANCE. The square of standard deviation.

VARIANCE-COVARIANCE MATRIX. In multivariate analysis, a matrix for which the element a_{ij} is given by the covariance of the i-th and j-th random variables when $i = j$, and by the variance of the i-th random variable when $i = j$ [1].

REFERENCES

1. Freund, J. E. and F. J. Williams (1966), Dictionary/Outline of Basic Statistics (McGraw-Hill, New York, NY).

2. Scheffé, H. (1959), Analysis of Variance (Wiley, New York, NY).

3. Barlow, R. E. and F. Proschan (1975), Statistical Theory of Reliability and Life Testing: Probability Models (Holt, Rinehart, and Winston, New York, NY).

4. Wilks, S. S. (1963), Mathematical Statistics (Wiley, New York, NY).

APPENDIX B

GLOSSARY OF ACRONYMS

ACC	Accumulator(s)
AFW, AFWS	Auxiliary feedwater (system)
BOC	Bottom of core
CDF	Cumulative distribution function
CFC, CFCS	Containment fan cooler (system)
CFCS(I)	I = injection phase
CFCS(R)	R = recirculation phase
CHG	Charging pumps (system)
CL	(See listing following CR-VSE)
CP	Charging pump
CR	Containment rupture
CR-B	B = (hydrogen) burning,
CR-MT	MT = melt-through
CR-OP	OP = overpressure
CR-VSE	VSE = vessel steam explosion
CL	Containment leakage
	L = leakage
CSS	Containment spray system
CSIS	Containment spray injection system
CSRS	Containment spray recirculation system
CVCS	Chemical and volume control system
ECC, ECCS	Emergency core coolant (system)
ECF	Emergency core functionability
ECI	Emergency coolant injection
ECR	Emergency coolant recirculation
EP, EPS	Electric power (system)
ESF	Engineered safety feature(s)
ET	Event tree
FSAR	Final safety analysis report
HPIS	High pressure injection system

IE	Initiating event
LOCA	Loss of coolant accident
ALOCA	A = large
MLOCA	M = medium
S1LOCA	S1 = small
S2LOCA	S2 = small-small
LPIS	Low pressure injection system
MSIV	Main steam isolation valve
MWe	Megawatt electric
NPSH	Net positive suction head
PAHR	Post-accident heat removal
PARR	Post-accident radioactivity removal
PCS	Power conversion system
PDF	Probability density function
PWR	Pressurized water reactor
RCL	Reactor coolant loop
RCS	Reactor coolant system
RHR, RHRS	Residual heat removal (system)
RPS	Reactor protection system
RSS	Reactor safety study (WASH-1400)
RVR	Reactor vessel rupture
RWST	Refueling water storage tank
SAR	Safety analysis report
SEISIM	Seismic Evaluation of Important Safety Improvement Measures

SHA, SHAS	Sodium hydroxide addition (system)
SI, SIP, SIS	Safety injection [pump(s)] (system)
SSMRP	Seismic Safety Margins Research Program
SSR	Secondary steam relief
S/RV	Safety/relief valve
S/RV-O	O = failure to open
S/RV-R	R = failure to reclose
SW, SWS	Service Water (System)
TOC	Top of core

APPENDIX C

EVENT TREES

CONTENTS

ILLUSTRATIONS

TABLES

SECTION C.1: SEISMICALLY INDUCED INITIATING EVENTS

Loss of coolant by leakage occurs when there is a break in the primary coolant-system boundary. The most dangerous primary system break is one which prevents the reflooding of the core by the emergency core-cooling system (ECCS). Such a break is called a Reactor Pressure Vessel (RPV) rupture, and it is defined as a rupture large enough to negate the effectiveness of the ECC systems required to prevent core melt. Although this event is called a RPV rupture, it includes combinations of primary-system piping breaks that cannot be negated by the ECCS. The event tree for this event is shown in Fig. C.1.

The second most dangerous break is one in the primary system where the loss of coolant can be negated by successful operation of the ECCS. Such breaks are called Loss of Coolant Accidents (LOCAs), and event trees have been developed for four sizes of such breaks. These event trees are presented in Figs. C.2, C.3, C.4, and C.5. The four sizes were determined by evaluation of ECCS pump and accumulator combinations which would be capable of reflooding the core for the various size breaks. Breaks smaller than the smallest LOCA break for which an event tree was developed will not uncover the core because of the slow rate of coolant loss and the operation of the normal make-up water system.

The discussion thus far has been limited to pipe and vessel failures which lead to a LOCA. However, a PWR primary system also contains a pressurizer, steam generators, primary relief valves, and primary coolant pumps. Failures in any of these components could also lead to loss of coolant. The pressurizer (RCS) relief valves could rupture or fail to reclose, thus causing a loss of coolant. If such a failure occurs, the break size is equivalent to one of the LOCA sizes for which an event tree was developed. Like reasoning applies to a pressurizer rupture accident. Similarly, an external rupture of a primary coolant-pump seal can be categorized as a LOCA.

Failures involving the steam generators are more complex. Despite the fact that the steam generator tubes are part of the RCS boundary, tube-rupture accidents will result in a transient, not a LOCA. This situation is described in greater detail in Sec. C.4. Tube ruptures occurring simultaneously with a large LOCA in another part of the RCS would prevent successful ECCS

operation*: this result is caused by a secondary-system flow into the primary system resulting from the blow-down-induced pressure differential between the primary and secondary systems. This event is accounted for in the large LOCA event tree by the mitigating-system title, "Emergency Core Function" (Fig. C.2).

The concept of emergency-core function (ECF) is important in a seismic study. ECF failure is defined as a failure to cool the core even though the emergency coolant injection systems operate successfully. It is important that the ECCS operate not only as designed, but also that it perform its function of cooling the core in an accident. In a seismically induced event, ECCS function is of particular importance, and it depends on the system's reaction to structural failures. In the case of a random-failure analysis, such as the RSS, the ECF-failure mode may be dismissed on probabilistic grounds. This is not true for a seismic event, because additional loads are placed on important structures, and therefore the likelihood of failure coincident with a LOCA is increased.

In a seismic event, ECF failure can occur because of the following circumstances:

1. Excessive core bypass-flow due to structural failures of the core shroud or core supports, including the case in which the core drops to the bottom of the vessel.

2. Excessive core distortion and/or flow blockage resulting from structurally failed mechanical parts of the reactor coolant sysem being swept into the core.

3. Excessive core distortion from combined seismic and LOCA loadings.

4. Excessive fluid leakage from the steam generator into the reactor coolant system due to structural failures of the tubes or tube sheets. This could result in steam binding and cooling failure.

---

*This statement is taken directly from WASH-1400. It has not been justified by calculations in WASH-1400 or in this report. As a conservative measure, the statement is being left in this analysis until such time as it may be proven invalid.

In the RSS, failure of the ECF was assumed to be important only for large LOCA events, because only large LOCA loadings would be sufficient to cause structural damage. In a seismically-induced event which results in a LOCA of any size, the combined seismic and LOCA loadings may cause sufficient structural damage to fail the ECF. It is noted, however, that Item 4 still applies only to large LOCAs, because excessive fluid leakage from the secondary to the primary system will occur only if primary-system pressure is rapidly reduced below that of the secondary system, and this occurs only during large LOCAs. The Zion FSAR is somewhat ambiguous on this point: are the steam generators designed for combined seismic and other loadings? The effect of an earthquake on the steam generator tubes is not likely to be large except for large earthquakes. According to the Zion FSAR, the design-basis earthquake has virtually no effect on the tubes for vertical loadings. The horizontal loadings, however, may become important for large earthquakes. The design basis for the tubes was a 1.0-g load, so that combined accelerations in the horizontal direction near that amount may be troublesome. In addition, degradation of the steam generator tubes may result from the chemical treatments used on the feedwater. Therefore, earthquake loads which result in a large LOCA may also be large enough to damage degraded tubes and cause ECCS functionability difficulties. For these reasons, it is concluded that the most significant contributor to risk from seismically-induced ECF failure is likely to be Item 4.

In summary, all piping and components in the primary system have been analyzed for a leakage-type loss of coolant. The primary piping includes the main loops and all interfacing piping out to the first isolation component, such as a check valve or valve which is normally closed. Adequate coverage of the potential leakage-type loss of coolant has been achieved with the event trees shown in this Appendix.

The loss of coolant by boil-off occurs when insufficient heat is removed from the primary system. There are many ways in which this could occur. However, no matter which failure mode causes the initial problem, the same series of events are expected to mitigate the situation and prevent core melt. The first functional requirement is to shut down the reaction in the core, followed by removal of decay heat. The design used at Zion requires the relieving of excess pressure from the primary system, if decay heat is not being adequately removed, and the replacement of water lost by boil-off to

maintain adequate coolant volume during the temperature and pressure changes. Ultimately, to reach a cold-shutdown mode requires additional heat removal from the primary system.

The mitigating actions described above are all considered in the transient event trees shown in this Appendix. All of these actions are concerned with prevention of core melt due to loss of coolant by boil-off. The initiating event that could be the cause of the potential boiloff can occur in either the primary or secondary coolant systems or in their supporting systems. These initiators have been defined as transient events. Events which in themselves are not transients, but which lead to transient events, still require the same mitigating systems and are therefore considered within the transient event trees presented in this Appendix.

Two transient event trees have been constructed for this study to describe two classes of transients: those which leave the power conversion system (PCS) operable, and those which disable the PCS. Although these two classes have been treated separately, the plant response is functionally identical for both classes and is explained in detail in Secs. C.4.1 and C.4.2.

All initiating events that can lead to a core melt have been taken into consideration. We conclude that the seven accident initiators in this report adequately cover all events that could lead to a core melt if they are not properly mitigated.

All components which carry primary coolant have been analyzed for potential leak paths. In considering all seismically induced events which could lead to primary coolant boil-off, we placed all those transients together which require the same mitigating functions.

We have discussed only those potential seismically induced initiating events for which we developed event trees. We assumed in our discussions that all other potential initiators--such as steam relief valves failing in the open position--are merely subevents of the event trees which we have developed. In considering and defining the initiating events which require event tree development, a general philosophy has been applied which assures that the significant initiators have been selected and all other potential initiators are subsets of them. Table C.1 contains a summary of the initiating events discussed in this Appendix. Each initiating event is explained in greater detail in Secs. C.2, C.3, and C.4.

Table C.1. Definition of event tree initiating events.

Reactor Vessel Rupture (RVR)	A vessel rupture large enough to negate the effectiveness of the ECC systems required to prevent core melt or rupture of sufficient primary coolant piping in a pattern that negates the effectiveness of those same ECC systems.
Large LOCA (LLOCA)	A rupture of primary coolant piping equivalent to the break of a single pipe whose inside diameter is greater than 6 in., but which does not negate the effectiveness of the ECC systems required to prevent core melt.
Medium LOCA (MLOCA)	A rupture of primary coolant piping equivalent to break of a single pipe whose inside diameter is greater than 3 in. but less than or equal to 6 in.
Small LOCA (SLOCA)	A rupture of primary coolant piping equivalent to break of a single pipe whose inside diameter is greater than 1.5 in. but less than or equal to 3 in.
Small-small LOCA (SSLOCA)	A rupture of primary coolant piping equivalent to break of a single pipe whose inside diameter is greater than 0.5 in. but less than or equal to 1.5 in.
Class 1 Transient (T1)	Any abnormal condition in the plant which requires that the plant be shut down but which does not directly effect the operability of the PCS and does not qualify as a LOCA or vessel rupture.
Class 2 Transient (T2)	Any abnormal condition in the plant which requires that the plant be shut down and which directly affects the operability of the PCS, causing it to become inoperative, but does not qualify as a LOCA or vessel rupture.

Events which occur in the steam generators are an example of initiating events which are a subset of the initiators presented in this study. The tubes and the tube sheet in each steam generator are the interface between the primary and secondary systems of a PWR. A break in this interface results in water from the reactor-coolant system leaking into the secondary system. The RCS pressure and level will drop until the low pressurizer pressure trip-point is reached. High radiation readings would be sensed in the secondary system, and the operator should act to isolate the leaking steam generator(s) from the rest of the RCS by closing the associated loop-isolation valves. If the operator responds correctly and isolates the leaking steam generator(s), the leak will be stopped and the accident will be a transient event. This particular incident will cause loss of the PCS; therefore, the plant response will be represented appropriately by the Class 2 transient (without PCS) event tree. If the operator fails to isolate the leaking steam generator, the RCS will blow-down. This accident will still fit the definition of a transient for the following reasons:

1. The RCS is blowing down to the secondary system, which has a back pressure of 1000 psi. Thus, blow-down stops at 1000 psi, rather than at the 40 psi of a LOCA (which blows down to the containment). As a result, much less coolant is lost. Examination of the Zion FSAR indicates that the pressure will equalize before the core is uncovered, and ECCS reflood will not be required.

2. No coolant will be blown into the containment. Therefore, the containment-pressure control functions and the functions of PAHR and PARR will not be required. Therefore, the plant responds to this action as it would to a transient. Since the PCS will also be lost, the plant response will be properly represented by the Class 2 transient event tree.

In both of the above accidents, some radiation will be released to the public through the steam-generator atmospheric (secondary) steam-relief valves (SSR). This would be equivalent to a containment failure by containment leakage, which is covered on the containment-event tree (see Sec. C.5).

Thus all possibilities resulting from a steam generator tube rupture event have been examined and found to be subsets of the initiators chosen for the SSMRP.

SECTION C.2: VESSEL-RUPTURE EVENT TREE

A reactor vessel-rupture event is defined as a vessel rupture large enough to negate the effectiveness of the ECC systems. It is therefore assumed that a vessel-rupture initiating event results in a core melt followed by containment failure and a radioactive release. Given a core melt, the only important mitigating systems are the containment building and its associated safety systems. The availability of those systems will, obviously, have an effect on the consequences of a vessel-rupture accident.

The vessel-rupture event tree developed for the SSMRP is shown in Fig. C.1. It includes the functions of post-accident heat removal (PAHR) and post-accident radioactivity removal (PARR) from the containment in both the injection and recirculation phases. In the injection phase, PAHR is accomplished by operation of (1) the CFCS(I), (2) the CSIS, or (3) a combination of the CFCS(I) and the CSIS. PARR during this phase is performed by (1) the CFCS(I) or (2) the CSIS.

In the recirculation phase, PAHR is accomplished by (1) the CFCS(R) or (2) a combination of the CSRS and the RHRS. PARR in this phase is performed by (1) the CFCS(R) or (2) the CSRS.*

The event tree was constructed by considering the timing sequence of the accident as well as the functionability/operability relationships between systems. First, the heat and radioactivity removal capabilities of the CSIS and CFCS(I) during the injection phase are considered in event C. Given the success or failure of these systems in the injection mode, they are then considered during the recirculation mode. It is necessary to consider the CFCS and CSRS separately in this mode because the CFCS will fail in the recirculation mode if it failed in the injection mode, while the CSRS can succeed if the CSIS fails because sufficient water will accumulate in the containment sump as a result of the vessel rupture to permit the RHR pumps to drive the CSRS headers and nozzles. Finally, given event F, heat removal from the containment is provided by the RHRS in those cases where the CFCS(R) does not function. Descriptions of the events and their success criteria are compiled in Table C.2.

---

*It is noted that the Sodium Hydroxide Addition System (SHAS) also contributes to PARR. However, its contribution is not significant enough to consequent reduction to merit inclusion in the ET. (See WASH-1400, Appendix I, Sec. 2.1.3.1)

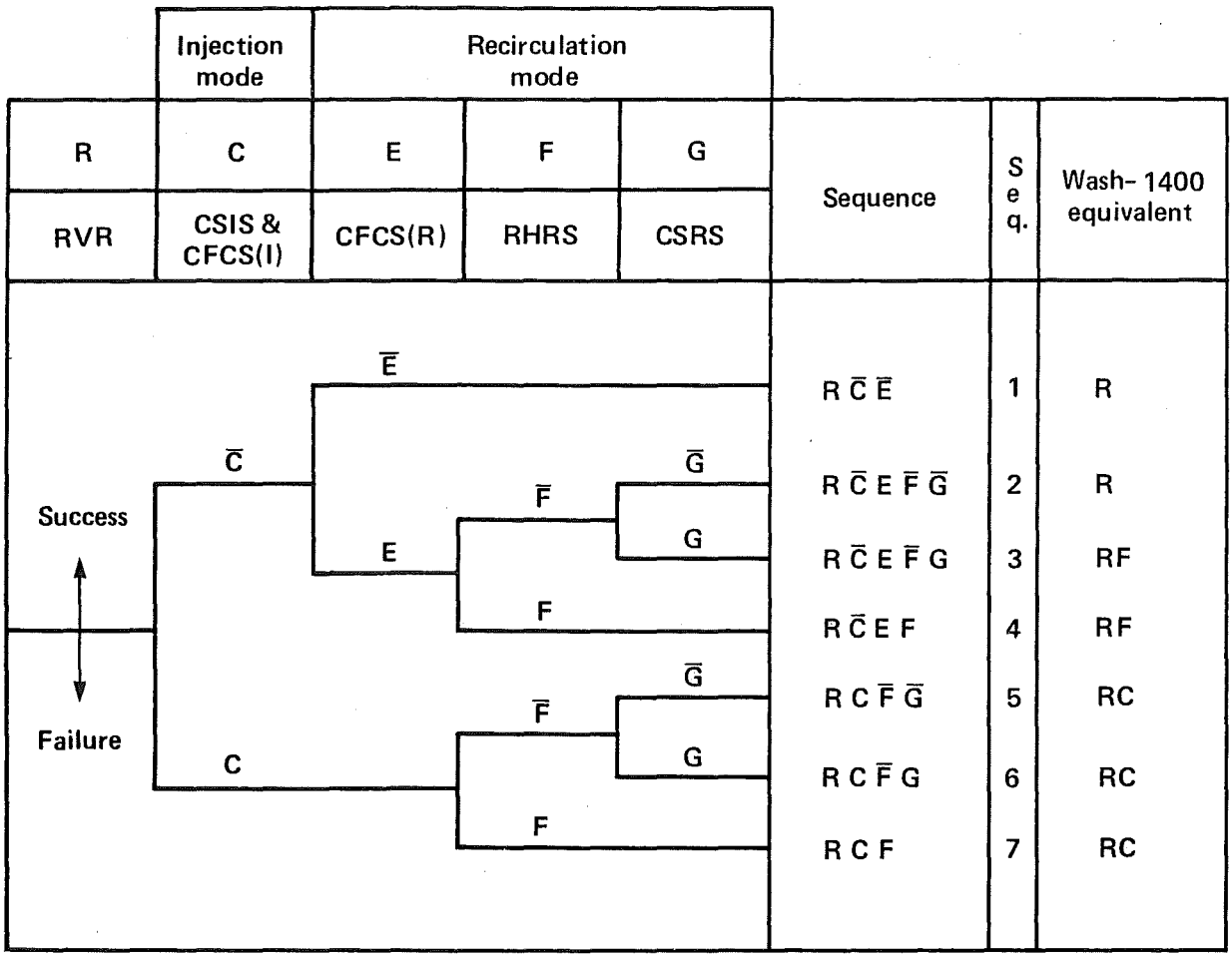


Figure C.1. Reactor vessel-rupture event tree.

Table C.2. Definition of events used on the vessel-rupture event tree.

Event	Name	Description
C	CSIS & CFCS(I)	Containment Spray Injection System & Containment Fan Cooler System (Injection Phase). The CSIS & CFCS(I) are designed to remove heat from the containment atmosphere to prevent overpressurization during the injection phase of a LOCA.[a] The CFCS consists of five fan-cooler units which condense the steam in the containment atmosphere. The heat removed from the steam is passed to the service water system. The CSIS consists of three containment spray pumps (two motor-driven, one diesel-driven) which deliver water from the RWST to spray headers in the containment. This spray condenses the steam in the containment atmosphere. Success is defined as (1) at least three out of five containment fans passing heat to the service water system, or (2) at least one out of three containment spray pumps delivering water to the containment atmosphere through the spray nozzles of the spray headers.
E	CFCS(R)	Containment Fan Cooler System (Recirculation Phase). The CFCS(R) is designed to remove heat from the containment to prevent overpressurization and help prevent core melt over the long term following a LOCA. The CFCS consists of five fan-cooler units which condense the steam in the containment atmosphere. The heat removed from the steam is passed to the service water system. Success is defined as at least three out of five containment fan units passing heat to the service water system.

Table C.2. (Continued)

Event	Name	Description
F	RHRS	Residual Heat Removal System. The RHRS is designed to remove heat from the containment to help prevent core melt and containment overpressure. The heat is removed by passing the water which has accumulated in the containment sump through heat exchangers. The exchangers cool the water by passing the heat to the component cooling-water system and then to the service water system. The RHRS consists of two RHR pumps, which take suction from the containment sump; two RHR heat exchangers, which take discharge from the pumps; the component cooling-water system, which circulates water in a closed loop, taking heat from the RHR heat exchangers and passing it out from component cooling-water heat-exchangers; and the service water system, which takes heat from the component cooling-water system and discharges it to the environment. (The component cooling-water system is shared by the two Zion units.) Success is defined as at least one out of two RHR pumps delivering water from the containment sump through its respective RHR heat exchanger; the component cooling-water system passing water through the same heat exchanger and removing the heat; and the service water system taking the heat from the component cooling-water system.
G	CSRS	Containment Spray Recirculation System. The CSRS is designed to remove heat from the containment atmosphere to help prevent containment overpressure during the recirculation phase of a LOCA.[a] The CSRS consists of two RHR pumps delivering water from the containment sump to spray headers in the containment. This spray condenses the steam in the containment atmosphere.

Table C.2. (Continued)

Event	Name	Description
		Success is defined as at least one out of two RHR pumps delivering water from the containment sump to the containment atmosphere through the spray nozzles of the spray headers.

[a]It is recognized that both the containment spray system and the containment fan cooler system have a functional capability to perform PARR; however, their relative efficiencies in performing this function have not been determined. It has therefore been assumed for this analysis that the difference in these efficiencies is not significant enough to result in substantially different consequences. This assumption greatly simplifies the event trees.

SECTION C.3: LOSS OF COOLANT ACCIDENTS

The process of constructing the loss of coolant accident (LOCA) event trees for the SSMRP involved two distinct but closely related steps. The first consisted of defining the ranges of break sizes for which event trees would be constructed. The second step was the development of the required trees. This section discusses the development of the event trees, with detailed explanations of the logic of the trees and descriptions of the various events on the trees and the success criteria established for them.

In order to define the various LOCA break sizes for the SSMRP seismic analysis of Zion, we examined the Zion FSAR and reviewed WASH-1400 and the Diablo Canyon Study. This evaluation resulted in the LOCA break sizes and the ECCS success requirement definitions for these LOCA break sizes. Both are given in Table C.3.

C.3.1 LARGE LOCA EVENT TREE

A large LOCA event is a rupture of primary coolant piping equivalent to the break of a single pipe whose diameter is greater than 6 inches (i.e., a break of one or more primary system pipes whose total cross-sectional area is greater than 28.3 $in.^2$), but which does not, in and of itself, negate the effectiveness of the ECC systems required to prevent core melt.*

The large LOCA event tree (ET) is shown in Fig. C.2. This event tree includes the functions of post-accident heat removal (PAHR), post-accident radioactivity removal (PARR), core reflood, and long-term heat removal. The event tree was constructed by considering the timing sequence of the accident, as well as the functionability/operability relationships between systems. Event A on the tree represents the large LOCA accident-initiator. Event C considers the heat- and radioactivity-removal capabilities of the SCIS and

*Breaks which would qualify as large LOCA events, but which also negate the effectiveness of the ECC systems required to prevent core melt, are conservatively defined as equivalent to a reactor vessel-rupture event.

Table C.3. Definition of events used on the LOCA event trees.

Event	Name	Description
C	CSIS & CFCS(I)	Containment Spray Injection System & Containment Fan Cooler System (Injection Phase). The CSIS & CFCS(I) are designed to remove heat from the containment atmosphere to prevent overpressurization during the injection phase of a LOCA.[a] The CFCS, which consists of five fan cooler units, condenses the steam in the containment atmosphere. The heat removed from the steam is passed to the service water system. The CSIS consists of three containment spray pumps (two motor- driven, one diesel-driven) which deliver water from the RWST to spray headers in the containment. This spray condenses the steam in the containment atmosphere. Success is defined as (1) at least three out of five containment fans passing heat to the service water system, or (2) at least one out of three containment spray pumps delivering water to the containment atmosphere through the spray header nozzles.
D	ECI	Emergency Coolant Injection. The ECI system is designed to replenish the water lost from the reactor coolant system (RCS) through the LOCA break. ECI for Large LOCA. ECI consists of four accumulators filled with borated water (held at 600 psi by pressurized nitrogen) which inject into the RCS cold legs, and two RHR pumps injecting water from the RWST into the RCS cold legs. Success is defined as injection into the RCS cold legs of at least one out of two RHR pumps (taking suction from the RWST), and at least three out of four accumulators.

Table C.3. (Continued)

Event	Name	Description
		ECI For Medium LOCA. ECI consists of four accumulators filled with borated water (held at 600 psi by pressurized nitrogen) which inject into the RCS cold legs, along with two CP and two SIP injecting water from the RWST into the RCS cold legs. Success is defined as injection into the RCS cold legs of (1) two out of two SIP (taking suction from the RWST) and at least three out of four accumulators, or (2) at least one out of two CP and one out of two SIP (taking suction from the RSWT) and at least three out of four accumulators. ECI For Small LOCA. ECI consists of two CP and two SIP injecting water from the RWST into the RCS cold legs. Success is defined as injection into the RCS cold legs of (1) at least one out of two CP and one out of two SIP or, (2) two out of two SIP taking suction from the RWST. ECI For Small-small LOCA. ECI consists of two CP and two SIP injecting water from the RWST into the RCS cold legs. Success is defined as injection into the RCS cold legs of (1) one out of two CP and one out of two SIP, or (2) two out of two CP, or (3) two out of two SIP taking suction from the RWST.
E	CFCS(R)	Containment Fan Cooler System (Recirculation Phase). The CFCS(R) is designed to remove heat from the containment to prevent overpressurization and help prevent core melt over the long term following a LOCA.[a] The heat removed from the steam is passed to the service water system.

Table C.3. (Continued)

Event	Name	Description
		Success is defined as at least three out of five containment fan units passing heat to the service water system.
F	RHRS	Residual Heat Removal System. The RHRS is designed to remove heat from the containment to help prevent core melt and containment overpressure. The heat is removed by passing the water which has accumulated in the containment sump through heat exchangers. The exchangers cool the water by passing the heat to the component cooling-water system, and from there to the service water system. The RHRS consists of two RHR pumps taking suction from the containment sump; two RHR heat exchangers which take discharge from the pumps; the component cooling-water system, which circulates water in a closed loop, taking heat from the RHR heat exchangers and passing it out from component cooling-water heat exchangers; and the service water system, which takes heat from the component cooling-water system and discharges it to the environment. (The component water-cooling unit is shared by the two Zion units.) Success is defined as at least one out of two RHR pumps delivering water from the containment sump through its respective RHR heat exchanger, the component cooling-water system passing water through the same heat exchanger and removing the heat, and the service water system taking the heat from the component cooling-water system.

Table C.3. (Continued)

Event	Name	Description
G	CSRS	Containment Spray Recirculation System. The CSRS is designed to remove heat from the containment atmosphere to help prevent containment overpressure during the recirculation phase of a LOCA.[a] The CSRS consists of two RHR pumps delivering water from the containment sump to spray headers in the containment atmosphere. Success is defined as at least one out of two RHR pumps delivering water from the containment sump to the containment atmosphere through the spray header nozzles.
H	ECR	Emergency Coolant Recirculation. The ECR system is designed to recycle back to the core the water spilled to the containment. The water keeps the core covered and removes decay heat during the recirculation phase of a LOCA. This process helps prevent core melt. ECR for Large LOCA. ECR consists of two RHR pumps injecting water from the containment sump into the RCS cold legs. Success is defined as at least one out of two RHR pumps taking suction from the containment sump and discharging to the RCS cold legs.

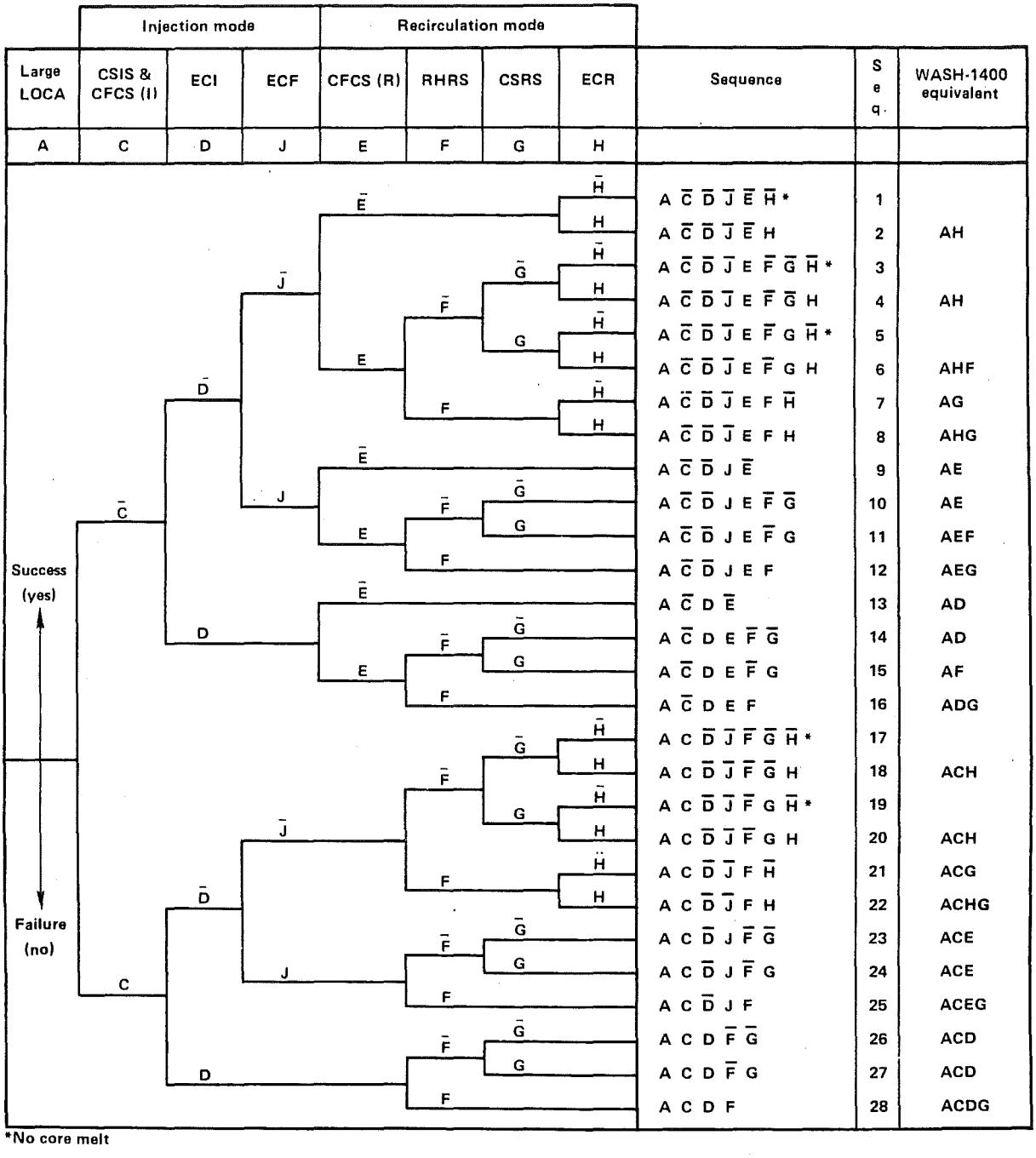
[a]It is recognized that both the containment spray system and the containment fan cooler system have a functional capability to perform PARR; however, their relative efficiencies in performing this function have not been determined. It has therefore been assumed for this analysis that the difference in their efficiencies is not significant enough to result in substantially different consequences. This assumption greatly simplifies the event trees.

Table C.3. (Continued)

Event	Name	Description
		ECR For Medium LOCA. ECR consists of two RHR pumps, two SIP, and two CP injecting water from the containment sump into the RCS cold legs. Success is defined as (1) at least one out of two RHR pumps, or (2) two out of two SIP, or (3) at least one out of two CP and one out of two SIP taking suction from the containment sump and discharging to the RCS cold legs. ECR For Small LOCA. ECR consists of two CP and two SIP injecting water from the containment sump into the RCS cold legs. Success is defined as (1) at least one out of two CP and one out of two SIP, or (2) two out of two SIP taking suction from the containment sump and discharging to the RCS cold legs. ECR For Small-small LOCA. ECR consists of two CP and two SIP injecting water from the containment sump into the RCS cold legs. Success is defined as (1) one out of two CP and one out of two SIP, or (2) two out of two CP, or (3) two out of two SIP taking suction from the containment sump and discharging to the RCS cold legs.
J	ECF	Emergency Core Functionability. This event is not a system. It is included to take into account the possibility that even if ECI succeeds, it may be ineffective in cooling the core. This could occur, for example, as a result of serious core damage which occurs prior to or during ECI.

Table C.3. (Continued)

Event	Name	Description
		Given that ECI is successful, success is defined as the ability of ECI to cool the core.
K	RPS	Reactor Protection System. The RPS is designed to shut down the nuclear reaction in the core if an abnormal condition exists. The purpose is to reduce the amount of heat which is produced and make it possible to put the plant in a safe condition. Success is defined as bringing the reactor to a subcritical (shutdown) condition.
L	AFWS & SSR	Auxiliary Feedwater System & Secondary Steam Relief. The AFWS & SSR is designed to remove heat from the RCS to help prevent core melt. Water is added to the steam generators by three AFW pumps (two motor-driven, one steam-turbine-driven) which take suction from the condensate storage tank or the service water system. The water is allowed to boil in the steam generator, removing heat from the RCS. This steam is then released through the SSR valves. Success is defined as at least one out of three AFW pumps delivering water to the steam generators from either the condensate storage tank or the service water system, and release of the created steam through the SSR valves.



Seq.	Sequence	WASH-1400 equivalent
1	A C̄ D̄ J E H̄ *	
2	A C̄ D̄ J E H	AH
3	A C̄ D̄ J E F̄ G H̄ *	
4	A C̄ D̄ J E F̄ G H	AH
5	A C̄ D̄ J E F G H̄ *	
6	A C̄ D̄ J E F G H	AHF
7	A C̄ D̄ J E F H̄	AG
8	A C̄ D̄ J E F H	AHG
9	A C̄ D̄ J Ē	AE
10	A C̄ D̄ J E F̄ Ḡ	AE
11	A C̄ D̄ J E F̄ G	AEF
12	A C̄ D̄ J E F	AEG
13	A C̄ D Ē	AD
14	A C̄ D E F̄ Ḡ	AD
15	A C̄ D E F̄ G	AF
16	A C̄ D E F	ADG
17	A C D̄ J F̄ G H̄ *	
18	A C D̄ J F̄ G H	ACH
19	A C D̄ J F̄ G H̄ *	
20	A C D̄ J F̄ G H	ACH
21	A C D̄ J F H̄	ACG
22	A C D̄ J F H	ACHG
23	A C D̄ J F̄ Ḡ	ACE
24	A C D̄ J F̄ G	ACE
25	A C D̄ J F	ACEG
26	A C D F̄ Ḡ	ACD
27	A C D F̄ G	ACD
28	A C D F	ACDG

Figure C.2. Large LOCA event tree.

CFCS(I) during the injection phase. Event D represents emergency core injection (ECI) or core reflood. The success criteria for this function have been previously defined. Event J is emergency core functionability (ECF). In event J, the ECI functions but, due to other factors, it is unable to reflood

the core effectively. Events C, D, and J collectively make up the injection phase of the response to initiating event A.

The events which make up the recirculation phase are considered next. The first of these is event E, which represents the recirculation capability designed into the CFCS(R). Event F represents heat removal from unspecified damage or failures within the pressure vessel itself, so that ECI containment is provided by the RHRS for those cases where the CFCS(R) fails. Event G represents the recirculation capability of the containment spray system or CSRS. The CFCS and CSRS are treated as separate events in this mode due to the assumption that the CFCS will fail in the recirculation mode if it failed in the injection mode, but the CSRS can succeed if the CSIS fails because sufficient water will accumulate in the containment sump as a result of the large LOCA to permit the RHR pumps to drive the CSRS headers and nozzles. Event H represents emergency coolant recirculation (ECR). This event is concerned with the continual flow of water to the vessel in order to keep the core covered once it has been reflooded in the injection mode. Descriptions of the events and their success criteria are compiled in Table C.3.

Of the 28 sequences in Fig. C.2, the 5 marked with asterisks do not result in core melt. The fact that non-melt sequence numbers 5 and 19 are present illustrates one of the differences between the plant designs analyzed in the RSS and this study. In these sequences, failure of both CFCS(R) and CSRS (events E and G) implies that steam in containment will not be condensed: the result is eventual rupture of the containment from overpressure. In the RSS, containment failure results in failure of the ECR function, since the PWR system design analyzed in the RSS required pressure in the containment to supply enough net positive suction head (NPSH) to operate the recirculation pumps. If the containment ruptures, sufficient NPSH to the pumps is lost, and the pumps will activate and fail, causing loss of ECR and eventually core melt. The plant used in the present study does not require pressure in the containment to provide sufficient NPSH to the ECR pumps, so the ECR can function even if the containment fails (as it will for sequences 5 and 19). Thus, core melt can be prevented as long as both the ECR and RHRS are successful.

In three other ways this large LOCA event tree differs from the equivalent tree in the RSS: (1) the addition of the CFCS, (2) the decision not to include electrical power, and (3) the sodium hydroxide addition (SHA) system. Loss of electrical power will be considered in the fault trees of the systems requiring electrical power. The SHA system was not included because its

contribution to th post-accident radioactivity removal (PARR), based on WASH-1400 results, is not significant enough to consequent reduction to merit inclusion in the E

In summary, th large LOCA ET identifies 28 accident sequences involving the operation (and operability) of 6 safety systems: the CSIS & CFCS(I), ECI, CFCS(R), RHRS, CSR , and ECR. Successful operation of these systems will prevent a large LO event from resulting in a core melt accident.

C.3.2 MEDIUM LOCA EVENT TREE

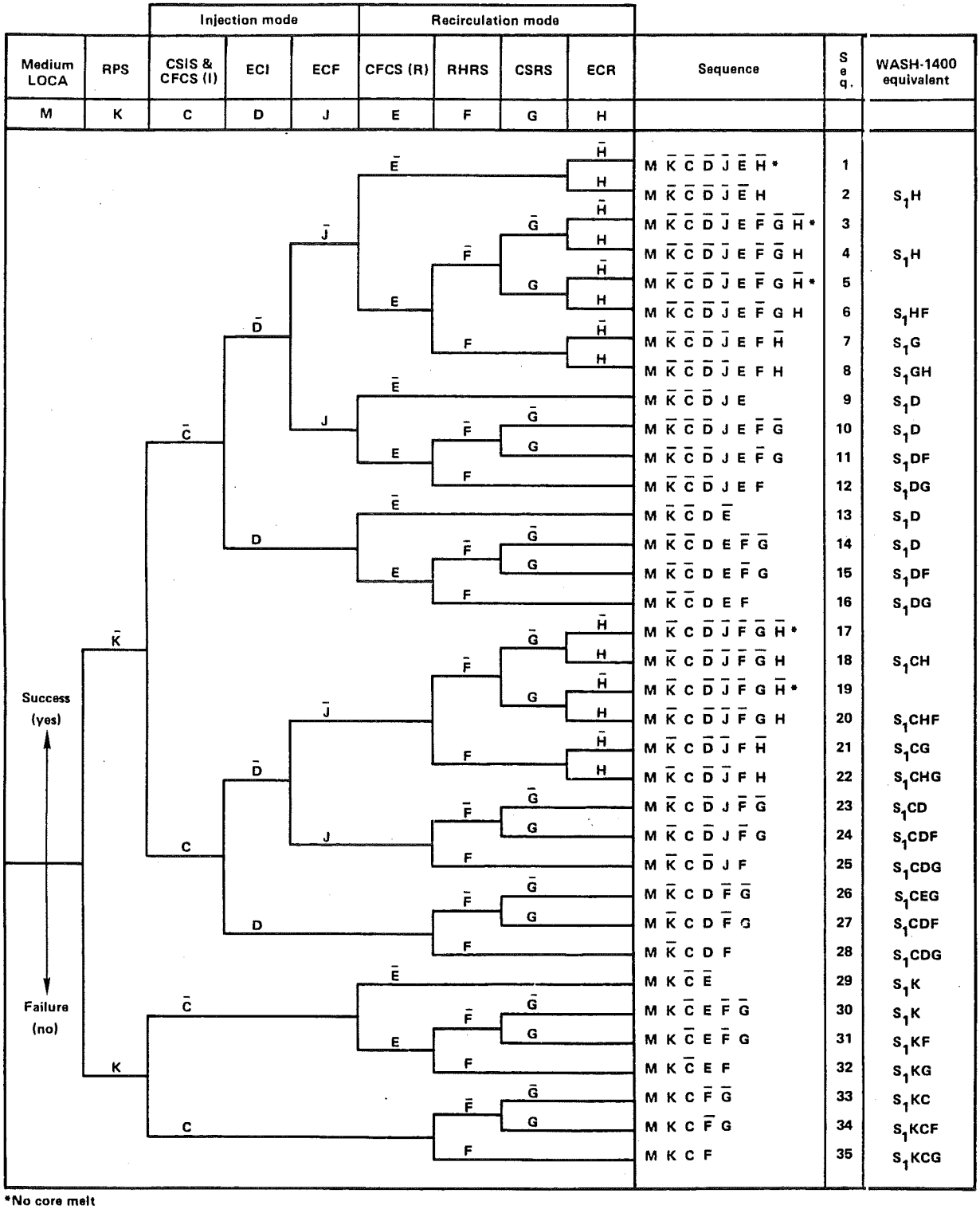
A medium LOCA vent is defined as a rupture of primary coolant piping equivalent to the eak of a single pipe whose diameter is greater than 3 in., but less than or e al to 6 in.

The medium LOC event tree developed for Zion is shown in Fig. C.3. This ET contains one ev it more than the large LOCA tree for Zion. The addition is event K, the React Protection System (RPS), which was not required in the large LOCA tree be use the very rapid blow-down and replacement of the coolant (and moder or) with highly borated water would bring the reactor to a subcritical point. The same effect would not occur in the medium LOCA (nor in the small or small small LOCAs) because of the slower rate of blow-down. Thus, RPS is neces ry on the medium LOCA event tree. It is also important to note that the ECI d ECR functions (event D and H) have different success criteria for the m lium LOCA than they do for the large LOCA. Descriptions of the events and the success criteria are compiled in Table C.3.

There are five sequences which do not result in core melt. These sequences are nomi lly identical to the five non-melt sequences on the large LOCA tree. The re oning behind this conclusion was given in Sec. C.3.1.

In summary, th medium LOCA event tree identifies 35 accident sequences involving the ope tion or operability of 7 safety systems: the RPS, CSIS and CFCS(I), ECI, CFCS R), RHRS, CSRS, and ECR. Successful operation of these systems will prev a medium LOCA event from resulting in a core melt accident.

Although the 3 did not define a medium LOCA, the medium LOCA event tree for Zion is very milar to the RSS small LOCA event tree.



*No core melt

Figure C.3. Medium LOCA event tree.

C.3.3 SMALL LOCA EVENT TREE

A small LOCA event is defined as the rupture of primary coolant piping equivalent to the break of a single pipe whose diameter is greater than 1.5 in. (approximately), but less than or equal to 3 in.

The small LOCA event tree developed for Zion is shown in Fig. C.4. This tree is logically identical to the medium LOCA tree because there are no significant differences in the functions required for the plant response to that break. The difference between the two break categories concerns only the success criteria for the ECI and ECR (events D and H). Descriptions of the events and their success criteria are compiled in Table C.3.

Since the small and medium LOCA event trees are logically identical, all of the descriptive text on the medium LOCA tree in Sec. C.3.2 applies to the small LOCA tree.

The small LOCA event tree for Zion is a newly developed tree that was not done for the RSS.

C.3.4 SMALL-SMALL LOCA EVENT TREE

A small-small LOCA event is defined as the rupture of primary coolant piping equivalent to the break of a single pipe whose diameter is greater than 0.5 in. but less than or equal to approximately 1.5 in.

The small-small LOCA event tree developed for Zion is shown in Fig. C.5. The ET contains one event more than the small and medium LOCA trees for Zion. The addition is event L [the Auxiliary Feedwater System and Secondary Steam Relief (AFWS and SSR)], which was not required in the larger break LOCAs because the high blow-down rate would remove sufficient core heat to reduce RCS pressure. This would not occur in the small-small LOCA because of the slower blow-down. Thus, the AFWS and SSR are required to remove the excess heat. As in the previous trees, the success criteria for ECI and ECR (events D and H) for the small-small LOCA differ from that of the other LOCA trees. Descriptions of the events and their success criteria are compiled in Table C.3.

There are five sequences which do not result in core melt. These sequences are nominally identical to the five non-melt sequences on the other LOCA trees. The reasoning behind this conclusion was given in Sec. C.3.1.

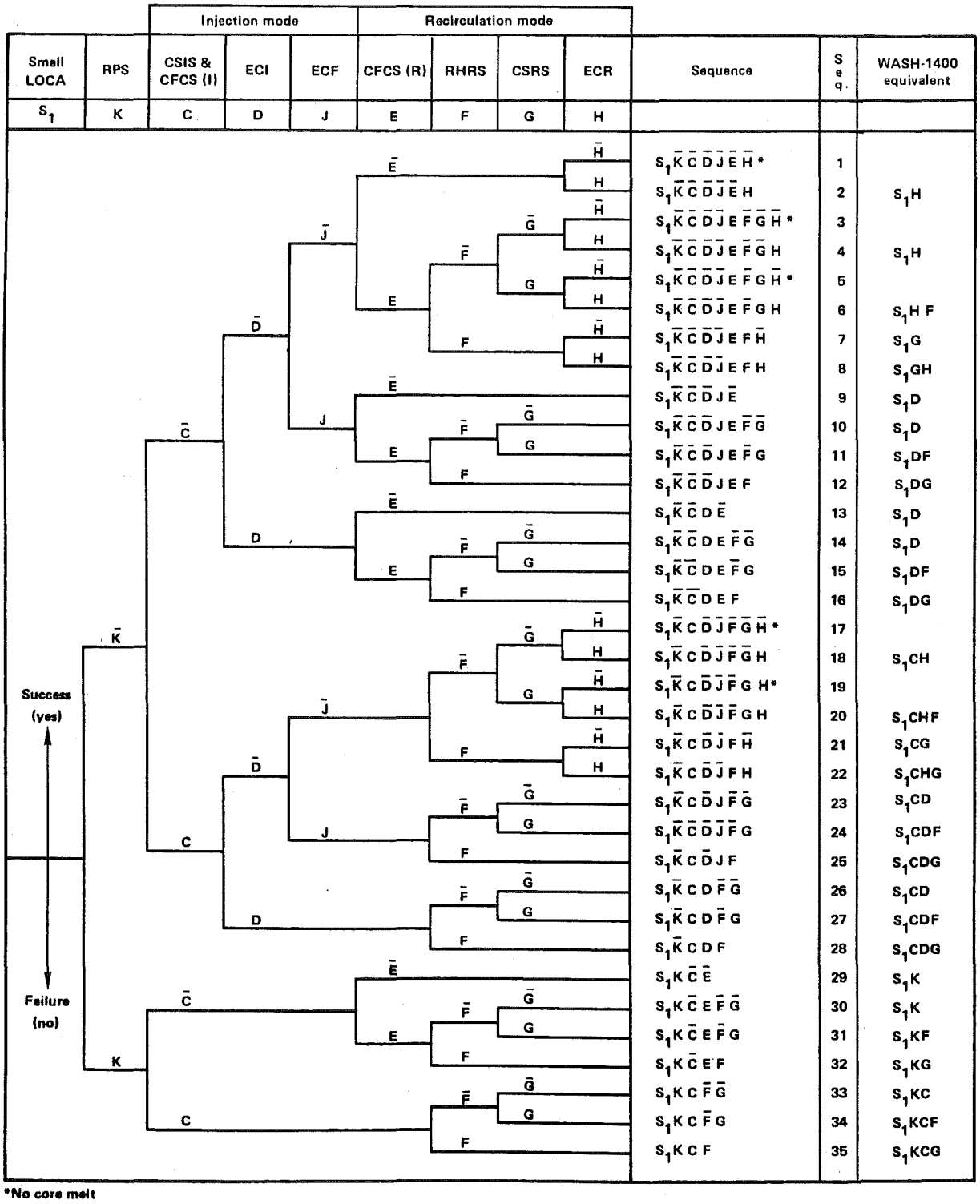


Figure C.4. Small LOCA event tree.

In summary, the small-small LOCA event tree identifies 42 accident sequences involving the operation or operability of 8 safety systems: the RPS, AFWS & SSR, CSIS & CFCS(I), ECI, CFCS(R), RHRS, CSRS, and ECR. These systems will help to prevent a core melt accident sequence which could result from a small-small LOCA. This ET is similar to the RSS small-small LOCA event tree.

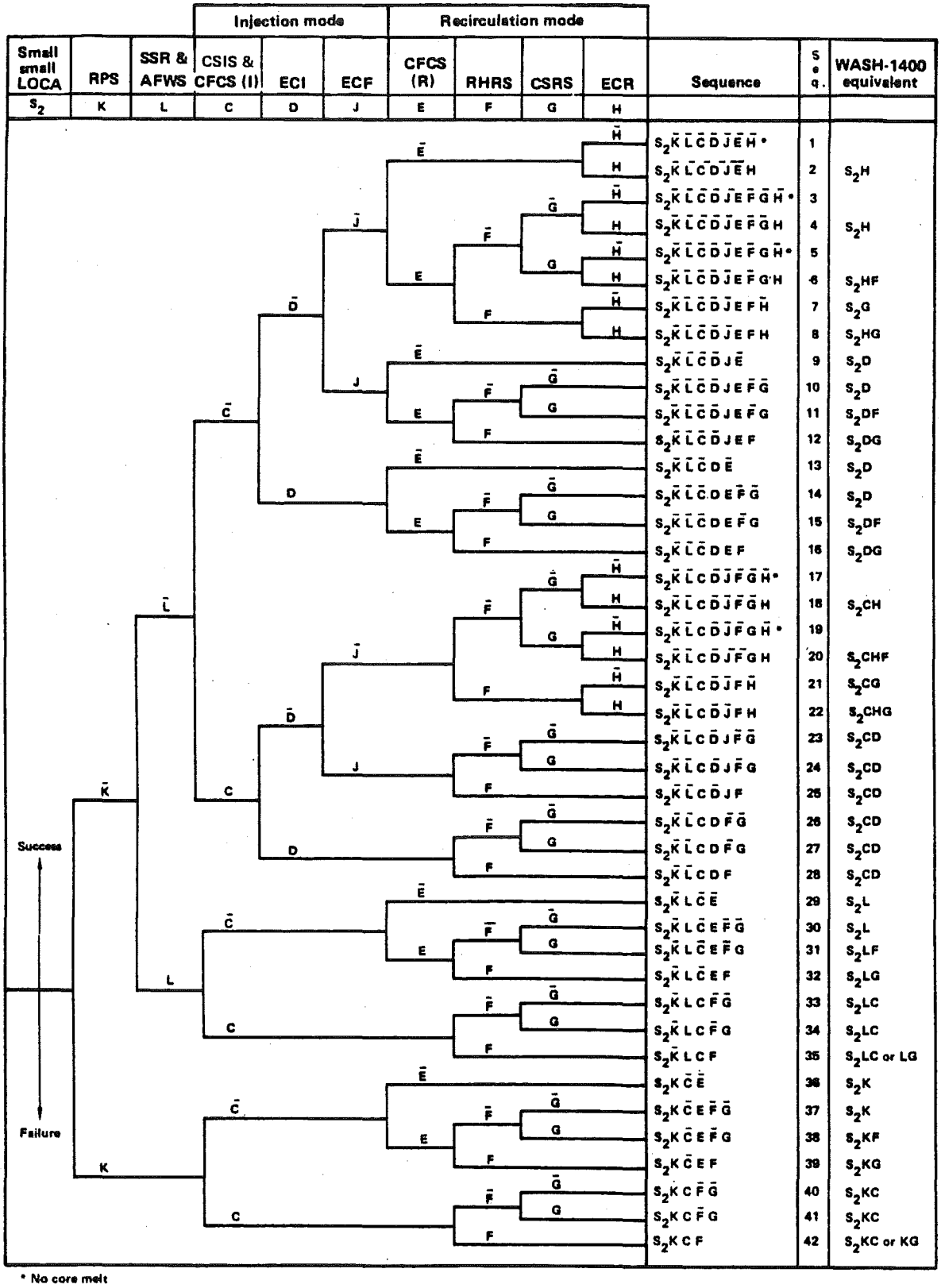


Figure C.5. Small-small LOCA event tree.

SECTION C.4: TRANSIENTS

A transient event is any abnormal condition in the plant which requires plant shutdown but does not qualify as a LOCA or vessel rupture: i.e., the condition does not involve a rupture of primary coolant piping equivalent to the break of a single pipe whose diameter is greater than 0.5 in.

A careful review of the Zion FSAR and other sources of information on plant operations indicated that there are two classes of transients to be considered. The first consists of those transient events which leave the power conversion system (PCS) capable of removing heat--i.e., the main steam, turbine bypass, condenser, condensate, and feedwater systems are still operating. (Note that the circulating water system is also required for heat removal.) Examples of Class 2 initiating events are loss of main feedwater, loss of condenser vacuum, main steam-line break, and loss of offsite power. A rule of thumb: transients which initiate a reactor trip-signal, followed by an eventual turbine trip-signal, will usually fall in the first class; transients which initiate a turbine trip-signal, followed by an eventual reactor trip-signal, will usually fall in the second class. The event trees for the two classes are discussed in detail in Secs. C.4.1 and C.4.2.

It is important to know that a transient can lead to LOCA. This would happen if a pressurizer relief or safety valve stuck open. This type of accident could transform a transient event into a small, medium, or large LOCA, depending on which valves stick open. A more detailed discussion of this scenario is included in the following sections.

C.4.1 TRANSIENTS WITH PCS (T1) EVENT TREE

A transient with PCS event is defined as any abnormal condition in the plant which (1) requires that the plant be shut down, (2) does not directly affect the operability of the PCS, and (3) does not qualify as a LOCA or a vessel rupture. That is, all of the systems which make up the PCS (main steam, turbine bypass, condenser, condensate, and feedwater) are still operating, and there is no rupture of RCS piping equivalent to the break of a single pipe whose diameter is greater than 0.5 in. This type of transient will henceforth be referred to as a Class 1 transient (T1).

The event tree developed for transients with PCS (T1) is shown in Fig. C.6. The event tree includes all the functions required to bring the plant to a cold shutdown condition. Shutting down of the nuclear reaction is accomplished by the RPS. Removing the heat from the RCS is accomplished by either (a) the PCS or (b) the AFWS and SSR. Prevention of RCS overpressure is accomplished by S/RV-O. S/RV-R prevents the transient from becoming a LOCA. The CVCS maintains the water level in the reactor vessel, and the RHRS allows the plant to be brought to a cold shutdown. Descriptions of the events and their success criteria are compiled in Table C.4.

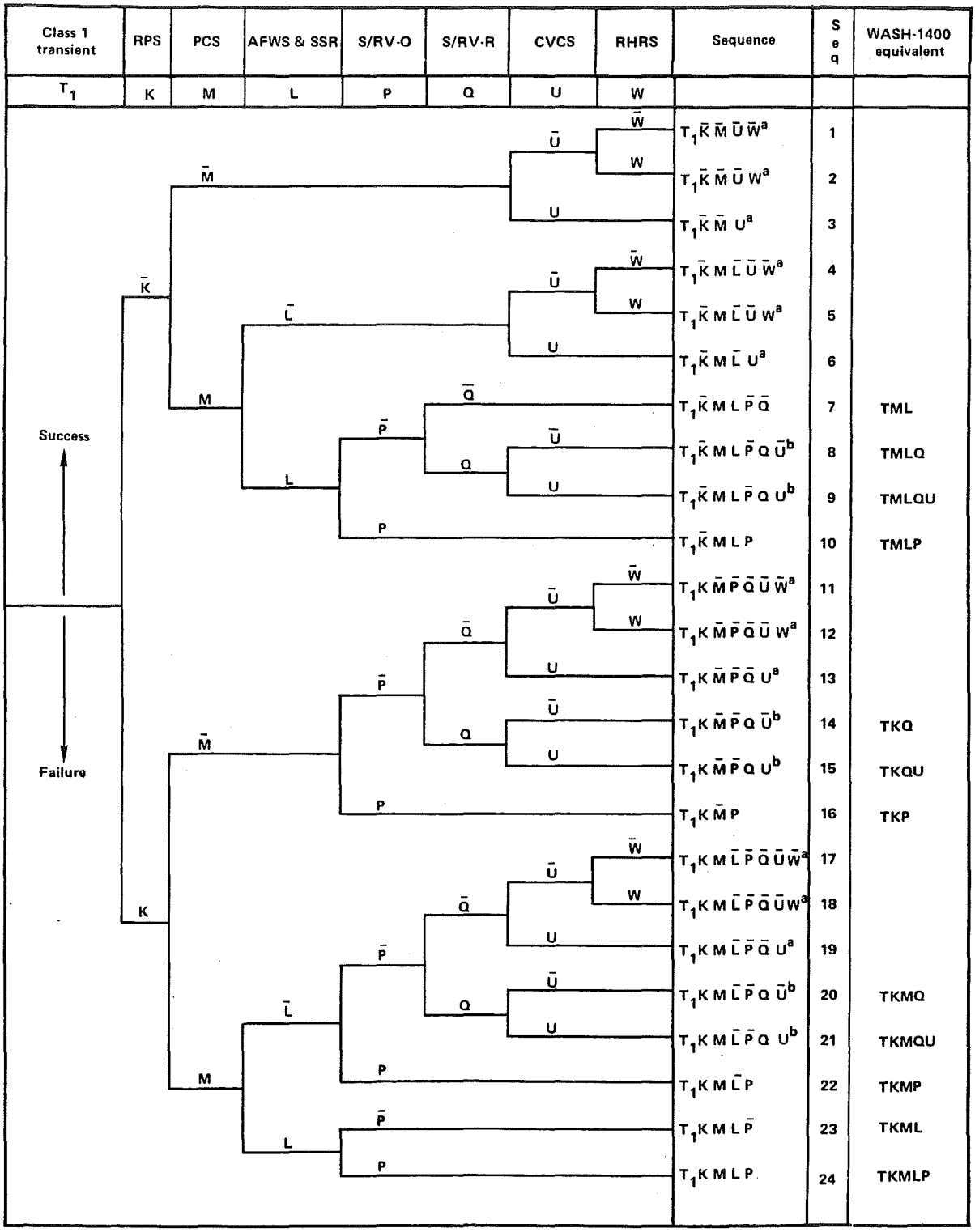
There are six sequences on the event tree which lead to LOCAs. These are indicated on Fig. C.6. It is important to note that even though core melt is conservatively indicated for these sequences, core melt is avoidable if the LOCA-mitigating systems are capable of functioning.

In summary, the Class 1 transient event tree identifies 24 accident sequences involving the operation (and operability) of 7 mitigating systems: the RPS, PCS, AFWS & SSR, S/RV-O, S/RV-R, CVCS, and RHRS. Successful operation of these systems will prevent a Class 1 transient from resulting in core melt.

C.4.2 TRANSIENT WITHOUT PCS (T2) EVENT TREE

A transient without a PCS event is defined as any abnormal condition in the plant which (1) requires that the plant be shut down, (2) causes the PCS to become inoperative, and (3) does not qualify as a LOCA or vessel rupture. That is, one or more of the systems which make up the PCS (main steam, turbine bypass, condenser, condensate, or feedwater) is no longer operating, and there is no rupture of RCS piping equivalent to the break of a single pipe whose diameter is greater than 0.5 in. This type of transient will henceforth be referred to as a Class 2 transient (T2).

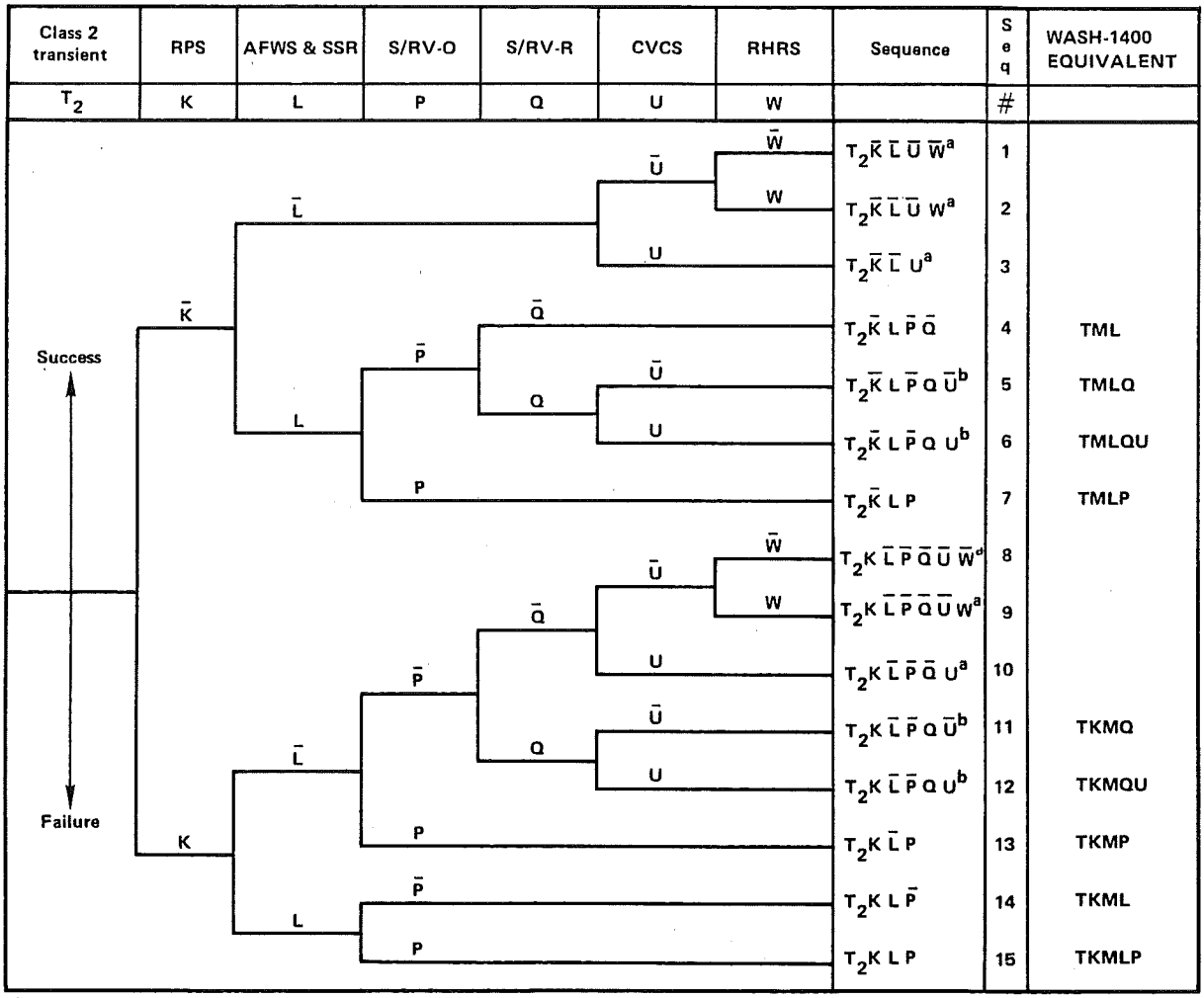
The event tree developed for a Class 2 transient (T2) is shown in Fig. C.7. It includes the same functions as the Class 1 transient tree discussed in Sec. C.4.1. The difference between the two trees is that in T2 the PCS will not be available to remove heat from the RCS, so that only the AFWS & SSR will be able to perform this function. Descriptions of the events and their success criteria are compiled in Table C.4.



[a] No core melt

[b] These accident sequences include the events safety relief valve opens and fails to reclose which initiates a small-small LOCA. The small-small LOCA event tree is appended to the footnoted sequences.

Figure C.6. Class 1 transient event tree.



[a]No core melt.

[b]These accident sequences include the events safety relief valve opens and fails to reclose which initiates a small-small LOCA. The small-small LOCA event tree is appended to the footnoted sequences.

Figure C.7. Class 2 transient event tree.

Table C.4. Definition of events used on transient-event trees.

Event	Name	Description
K	RPS	Reactor Protection System. The RPS is designed to shut down the nuclear reaction in the core if an abnormal condition exists. The purpose is to reduce the amount of heat which is produced and make it possible to put the plant in a safe condition. Success is defined as bringing the reactor to a subcritical (shutdown) condition.
M	PCS	Power Conversion System. The PCS is designed as the normal method of removing heat from the RCS. Steam created in the steam generators is sent through the main steam lines to the main turbine or turbine bypass and on to the condenser. The condensate is then pumped through the condensate and feedwater systems and returned to the steam generator to be turned into steam again. For a transient, success is defined as sending the steam from the steam generators to the condenser by way of the turbine bypass, condensing it, and then returning the condensate to the steam generator by using the condensate and feedwater pumps.
L	AFWS & SSR	Auxiliary Feedwater System and Secondary Steam Relief. The AFWS & SSR is designed to remove heat from the RCS to help prevent core melt. Water is added to the steam generators by three AFW pumps (two motor-driven, one steam-turbine-driven) which take suction from the condensate storage tank or the service water system. The water is allowed to boil in the steam generator, removing heat from the RCS. The resultant steam is then released through the SSR valves.

Table C.4. (Continued)

Event	Name	Description
		Success is defined as at least one out of three AFW pumps delivering water to the steam generators from either the condensate storage tank or the service water system, and release of the created steam through the SSR valves.
P	S/RV-O	Safety/Relief Valves - Open. The pressurizer S/RVs are designed to relieve excess pressure in the RCS in order to prevent possible subsequent damage to the RCS piping and vessels. Small amounts of excess pressure are relieved by one or both of the two power-operated relief valves (PORVs). If the pressure spike is excessive, or the PORVs fail to open, pressure will be relieved by one, two, or three of the three safety valves (SVs). Success is defined as the opening of the necessary number of S/RVs to prevent RCS overpressurization.
Q	S/RV-R	Safety/Relief Valves - Reclose. The pressurizer S/RVs are also designed to reclose once the excess RCS pressure has been relieved. This reclosing keeps most of the water inventory within the RCS, preventing a LOCA-type accident. Success is defined as the reclosing of all the S/RVs which opened, once the excess RCS pressure is relieved. If any PORVs are stuck open and the operator realizes what is happening, he can manually close a motor-operated block valve, which will stop flow through the PORVs. This valve closure will satisfy the success criteria.
U	CVCS	Chemical and Volume Control System. The CVCS is designed to maintain water inventory in the RCS for most normal operations and transients. Excess water is drained from

Table C.4. (Continued)

Event	Name	Description
		the RCS and eventually brought to the volume-control tank. If water is needed, it is added from the volume-control tank by three charging pumps. During a transient, success is defined as maintaining water inventory in the RCS above the core.
W	RHRS	Residual Heat Removal System. The RHRS is designed to bring the reactor to cold shutdown once the RCS temperature has been brought down to about 350°F and the pressure to 400 PSI. The RCS is cooled by passing the RCS water through heat exchangers which cool the water by passing the heat to the component cooling-water system, and from there to the service water system. The RHRS consists of two RHR pumps which take suction from the Loop A hot leg; two RHR heat exchangers which take discharge from the pumps and which themselves discharge back to the RCS; the component cooling-water system,[a] which circulates water in a closed loop, taking heat from the RHR heat exchangers and passing it out from component cooling-water heat exchangers; and the service water system, which takes heat from the component cooling-water system and discharges it to the environment. Success is defined as at least one out of two RHR pumps delivering water from the Loop A hot leg through its respective RHR heat exchanger and back to the RCS, the component cooling-water system passing water through the same heat exchanger and removing heat, and the service water system taking the heat from the component cooling-water system.

[a]The component cooling-water system is shared between the two Zion units.

There are six non-melt sequences on the event tree. These are indicated in Fig. C.7. The reason for declaring these to be non-melt sequences is the same as that described in Sec. C.4.1 for the Class 1 transient tree. The sequences numbered 1 - 3 on the Class 2 transient tree correspond to the sequences numbered 4 - 6 on the Class 1 transient tree. The sequences numbered 8 - 10 on the Class 2 transient tree correspond to the sequences numbered 17 - 19 on the Class 1 transient tree.

There are four sequences on the event tree which lead to LOCAs. These are also indicated in Fig. C.7. The explanation of these sequences is detailed in interrelationship 6 in Sec. C.4.1 and is the same as that for the similarly indicated sequences on the Class 1 transient tree.

In summary, the Class 2 transient event tree identifies 15 accident sequences involving the operation (and operability) of 6 mitigating systems: the RPS, AFWS & SSR, S/RV-O, S/RV-R, CVCS, and RHRS. Successful operation of these systems will prevent a Class 2 transient from resulting in a core melt.

SECTION C.5: CONTAINMENT

This section describes the development of a containment event tree applicable to the SSMRP and explains the basic concept and results of the event-tree construction process.

The containment event tree (ET) developed for the Zion PWR for use in the SSMRP analysis of earthquake-initiated events is shown in Fig. C.8. It is similar to the ET developed for random events in the Reactor Safety Study (RSS). This ET identifies the same five failure modes for the PWR containment as follows:

(1) containment rupture due to a steam explosion in the reactor vessel;

(2) containment rupture due to hydrogen burning, resulting in containment overpressure;

(3) containment rupture due to overpressure from other physical processes;

(4) containment failure due to melt-through of the containment base mat by the molten core; and

(5) failure of the containment to isolate--i.e., containment "leakage."

It was determined that no new physical processes inside the containment would

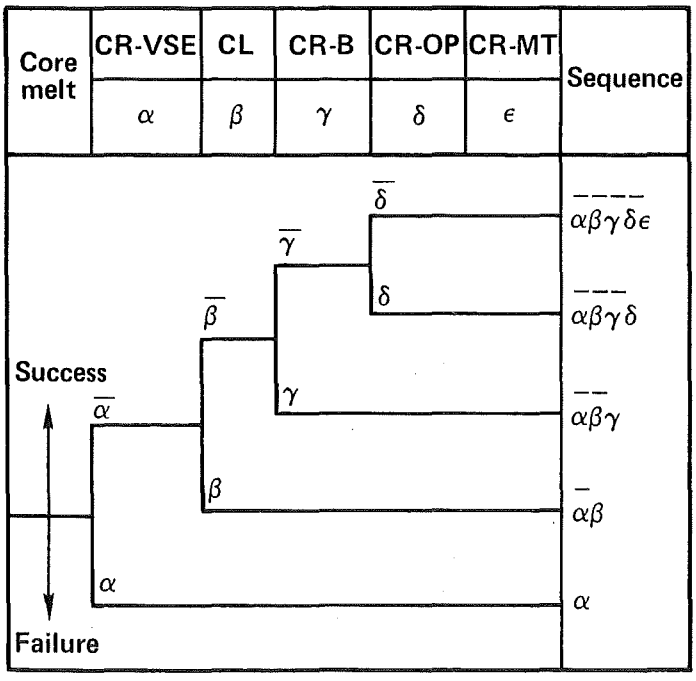


Figure C.8. Containment event tree.

contribute to additional failure modes for an earthquake-initiated event. This result was based upon the general design of the Zion plant, as well as the framework of the analysis developed for the SSMRP. Definitions of the events used on the tree are compiled in Table C.5.

The prime concern of containment analysis is the identification of the physical processes which can result in containment failure. An understanding of these physical processes is, in itself, of great importance in determining the consequences of a nuclear accident, because the consequences are dependent upon the timing of the radioactive release, the energy present in the containment at the time of containment failure, and the particular containment failure-mode which occurs. This information is developed from evaluations of the accident sequences which are individually coupled to the containment event tree. The containment event tree thus provides the basic focal point for translation of an accident sequence into its associated environmental consequences.

Because an earthquake-initiated structural failure of the containment may result in ESF failures caused by falling objects, accumulated debris, or other common-mode events, a number of ambiguities may arise in the analysis of earthquake-initiated events. The difficulties arise when an attempt is made to treat possible common-mode effects directly in the containment event tree. Common-mode effects--such as damage caused by falling objects--should be included in the specific-system fault trees rather than in the event trees. Common-mode effects are identified when the Boolean failure equations of system-fault trees are combined to find the cut sets for a particular accident sequence. This approach prevents the difficulties experienced by the RSS as a result of removing electric power failure from the system-fault trees and incorporating it as an event in the LOCA event trees. The containment ET developed here considers only the sequence of events associated with the physical processes of a particular event sequence.

To summarize: the analysis has shown that a containment event tree similar to that developed in the RSS is applicable to earthquake-initiated accidents. The effects of secondary failures resulting from structural failures within containment will not be treated in the ETs: these common-mode faults of concern will be included within the fault trees developed for the various systems so that these faults can be evaluated directly. The containment-failure modes and the radioactive release magnitude categories (used for grouping the various accident sequences) will be the same as those

used in WASH-1400. The only difference will lie in the relative probabilities of the various containment failure modes as the earthquake being considered increases in magnitude.

Table C.5. Definition of events used on the containment event tree.

Event	Name	Description
α	CR-VSE	Containment Rupture - Vessel Steam Explosion. Steam flashing caused by the interaction of the molten core with water in the bottom of the reactor vessel causes vessel overpressure and subsequent shattering of the vessel. Missiles resulting from the shattered vessel rupture the containment.
β	CL	Containment Leakage. Failure of the containment to completely isolate.
γ	CR-B	Containment Rupture - Burning. Hydrogen accumulated in the containment ignites, causing instantaneous overpressure, which ruptures the containment.
δ	CR-OP	Containment Rupture - Overpressure. Steam created in the core and released to the containment is not condensed by the containment ESF systems. The result is a slow buildup of containment pressure until overpressure occurs, which ruptures the containment.
ϵ	CR-MT	Containment Rupture - Melt-through. The molten core melts through the bottom of the reactor vessel and the containment-base mat, thereby breaching the containment.

APPENDIX D

SYSTEM DESCRIPTIONS AND FAULT TREES

CONTENTS

ILLUSTRATIONS

TABLE

SECTION D.1: INTRODUCTION

This Appendix discusses the systems in Zion 1 for which fault trees were generated: ECCS (Sec. D.2), AFWS (Sec. D.3), SWS (Sec. D.4), and EPS (Sec. D.5). The generation of fault tree models for each system is also discussed. This work was based on the Zion Nuclear Power Station FSAR and detailed drawings and written procedures for the Zion plant. In addition, we visited the Zion plant to gain firsthand knowledge of system and component placement and orientation within the plant. Information not contained in any of the sources listed above was obtained from plant personnel and other sources.

SECTION D.2: EMERGENCY CORE COOLING SYSTEM

This section will consider the response of the Emergency Core Cooling System (ECCS) to seismically-induced LOCAs of various sizes. The ECCS includes two phases of operation: the injection phase and the recirculation phase. The major difference between the two is the source of water being pumped into the primary coolant system. The injection phase takes water from the refueling water storage tank, and the recirculation phase takes it from the containment sump. These processes are detailed in the following subsection, D.2.1. Section D.2.2 discusses the fault tree models constructed for the ECCS.

D.2.1 ECCS SYSTEM DESCRIPTION

In response to a LOCA, the ECCS is called upon to reflood the core if necessary and keep it covered. Before describing how the ECCS accomplishes this, we repeat the success criteria defined for the ECCS in Appendix C. This information is shown in Table D.1.

Table D.1. Definition of ECCS equipment success requirements for LOCA events at Zion Unit 1.

LOCA size (equivalent diam.)	Injection mode (ECI)	Recirculation mode (ECR)
Large Breaks > 6"	1/2 LPIS[a] + 3/4 ACC	1/2 LPIS
Medium 6" ≥ Breaks > 3"	1/2 CP + 1/2 SIP + 3/4 ACC or 2/2 SIP + 3/4 ACC	1/2 CP + 1/2 SIP or 2/2 SIP or 1/2 LPIS
Small 3" ≥ Breaks > 1.5"	1/2 CP + 1/2 SIP or 2/2 SIP	1/2 CP + 1/2 SIP or 2/2 SIP
Small-small 1.5" ≥ Breaks > 0.5"	1/2 CP + 1/2 SIP or 2/2 SIP or 2/2 CP	1/2 CP + 1/2 SIP or 2/2 SIP or 2/2 CP

[a]The RHR pumps are used for LPIS because there are no separate LPIS pumps.

As shown in Table D.1, the ECCS is made up of three pumping systems and the accumulators. Different combinations of these systems can be used in responding to different break sizes. The following components are part of ECCS.

1. Two centrifugal charging pumps (CP)
2. Two high head safety injection pumps (SIP)
3. Two residual heat removal pumps (RHR)
4. Two residual heat exchangers
5. Four accumulator tanks (one on each loop)
6. One boron injection tank (BIT)
7. Refueling water storage tank (RWST)
8. All related valves and piping

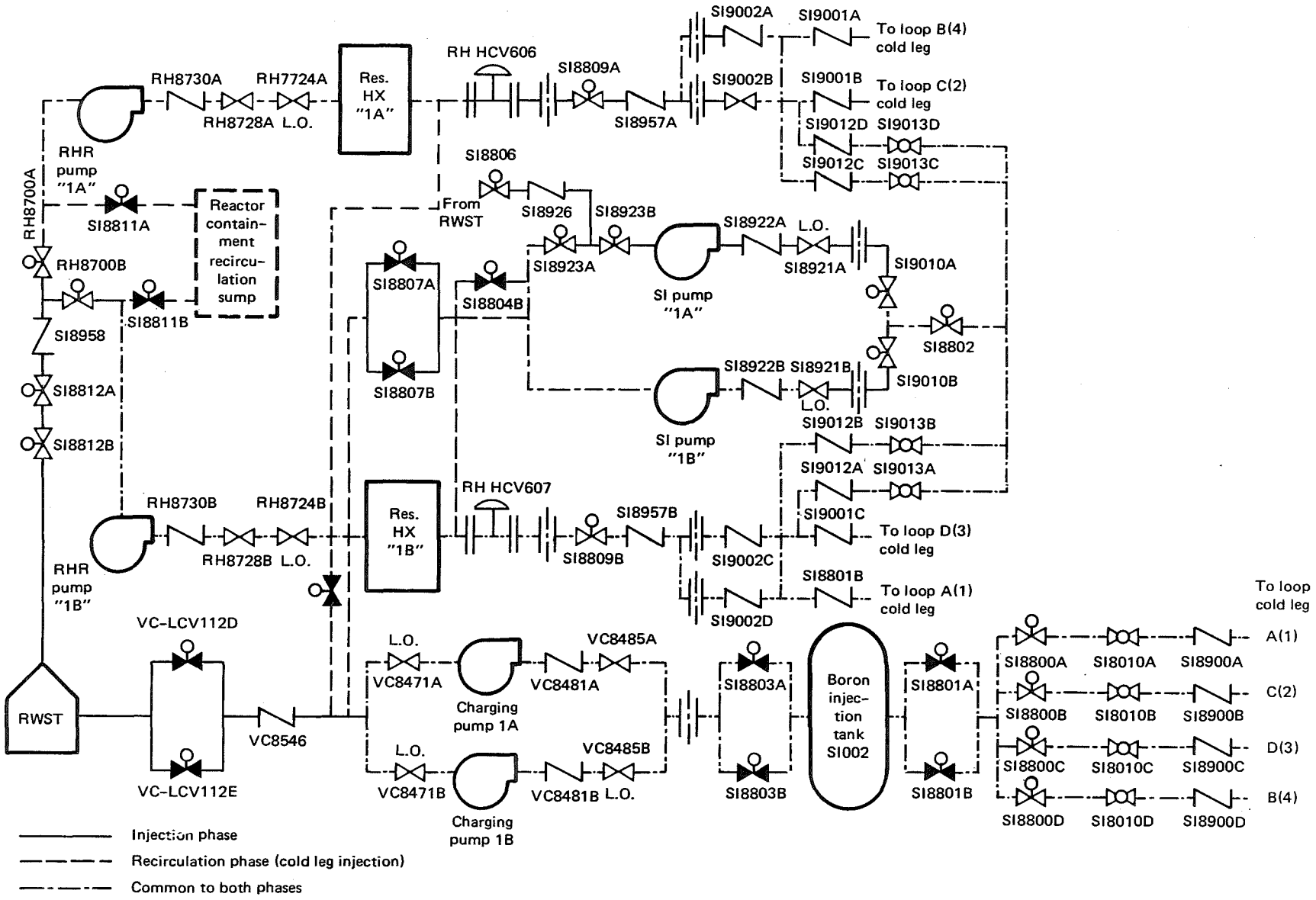


Figure D.1. Description of ECCS.

All of the systems which make up the ECCS are designed to the Seismic Class 1 design code. The accumulator tanks are located inside containment but outside the missile barrier. The refueling-water storage tank is located between the auxiliary and containment buildings. All the pumping systems take suction in the injection phase from this storage tank. All the other system components are located in the auxiliary building. Figure D.1 is a single-line diagram showing the major components of the ECCS.

D.2.1.1 Accumulators

There are four accumulator tanks, one for each cold leg of the primary coolant system. The accumulator system is the only passive system in the ECCS. In the event of a large or medium LOCA, the borated water in the accumulators is injected into the primary system as soon as the pressure of the primary system drops below that of the accumulators (650 psig normal pressure). The accumulators are maintained at their pressure by compressed nitrogen gas. The only action required to inject the borated water into the primary system cold legs is the mechanical action of opening two swing-disc check valves in series. It should be noted that in a less than medium size break the primary system pressure will not drop below 650 psig as a result of the blow-down.

D.2.1.2 Centrifugal Charging Pumps

Two high pressure centrifugal charging pumps are provided. These two pumps serve as part of the Chemical and Volume Control System (CVCS) during normal plant operation. In an accident, these pumps are isolated from the CVCS by a safety injection signal and used to supply high pressure borated water to the primary system at a rate of 150 gpm each. During the injection phase operation of ECCS, these pumps take water from the refueling water storage tank (RWST) and inject the water into the primary coolant system via the boron injection tank.

The discharge pressure of 2670 psig for these pumps enables them to inject high boron concentrated water into the primary coolant in the event of a transient or small-small LOCA. In the transient event, the boron concentration aids in poisoning the reaction; however, in the small-small LOCA, it not only poisons the reaction, it also maintains the core water

inventory. The charging pumps can pump water into the primary system at normal or above normal operating pressures: this feature differentiates the charging pumps from the safety injection (SI) and residual heat-removal (RHR) pumps.

During the recirculation phase of operation, the charging pumps take water from the containment sump via RHR Pump 1A. If this pump fails, but the crosstie valves between the SI and charging pumps are opened, the charging pumps can take water from RHR Pump 1B.

D.2.1.3 Safety Injection Pumps

Two high pressure safety injection pumps are part of the ECCS and provide water for the primary coolant system at the rate of 400 gpm each when the primary system pressure drops below 1520 psig. Above a pressure of 1520 psig, the SI pumps recirculate the water back to the RWST. During the injection phase, the SI pumps take water from the RWST to supply borated water to the four primary coolant cold legs. During recirculation, these pumps take water from the containment sump via RHR Pump 1B. If this pump fails, but the crosstie valves between the SI and charging pumps are opened, the SI pumps can also take water from RHR Pump 1A.

D.2.1.4 Residual Heat Removal Pumps

Two low pressure RHR pumps deliver large quantities of borated water (3000 gpm for each pump) when the primary system pressure drops below 170 psig. Before the primary system pressure drops below 170 psig, these pumps take water from the RWST during the injection phase and recirculate the water back to the RWST. The operator initiates the recirculation phase of the ECCS operation when the first low level alarm in the RWST has been reached or when the amount of water in the containment sump provided by containment spray pumps and leakage from the break is enough to provide the required Net Positive Suction Head (NPSH) for the RHR pumps. During the recirculation phase, the RHR pumps take water from the containment sump and recirculate the water back to the four cold legs through residual heat exchangers. In another mode of the recirculating phase, after approximately 19 hours into the accident and in order to complete the subcooling of the core, the recirculation water is injected into the hot legs.

D.2.2 ECCS FAULT TREE MODEL

Four separate fault trees have been developed for accumulator tanks, RHR pumps, safety injection pumps, and centrifugal charging pumps. These fault trees are not included in this report. The top event for the accumulator tree is defined as "insufficient flow from two or more accumulator tanks on demand." Failure of each accumulator leg is analyzed in detail for failure which would prevent it from dumping into its respective cold leg.

The top event for the second fault tree is defined as "insufficient flow to the reactor coolant cold legs from RHR pumps." In the tree, failure of the RHR system is defined as the failure of both RHR pumps to provide sufficient cooling to all four primary loop cold legs. A fault tree has been developed for safety injection pumps with the top event "insufficient flow to the reactor coolant cold legs from SI pumps," which also means failure of both SI pumps to provide cooling to all four cold legs. A fault tree has been developed for failure of the centrifugal charging pumps: the top event is "insufficient flow to the reactor coolant cold legs from charging pumps." These fault trees then will input to the fault trees defined in Figs. D.2 to D.5 to produce fault trees for ECCS failure, depending on the size of the break in the primary system. Note that Figs. D.2 through D.5 are for the injection mode. It becomes evident that, in some cases, the top event required for the failure of safety injection or charging pumps is failure of either of the two SI or charging pumps, rather than failure of both pumps.

As mentioned before, the three active systems of ECCS operate in two phases, injection and recirculation. These two phases of operation have been identified in the fault tree by house events, which function as switches (either 1 or zero) in the fault tree to turn on or off different subtrees associated with each phase of operation. For example, if house event IP (Injection Phase) is set equal to 1 and house event RP (Recirculation Phase) is set equal to zero, then the fault tree is a logic model of the failure of the system during the injection phase of operation.

During the recirculation phase of ECCS operation, safety injection and centrifugal charging pumps take suction from residual heat exchangers 1B and 1A, respectively. To improve redundancy, a crosstie pipe with two parallel, normally closed, motor-operated valves is provided between the safety injection and charging pumps suction headers: this provides all four safety injection and charging pumps with coolant through one residual heat exchanger

in the event of failure of the other residual heat exchanger. During recirculation, safety injection pumps take suction either directly from the residual heat exchanger 1B (event RH-SI in SI fault tree which transfers from RHR fault tree event R88) or from residual heat exchanger 1A via charging pump pipes (event CP-SI in the safety injection fault tree, which transfers from charging pumps fault tree event C150). Centrifugal charging pumps, during recirculation, take suction either directly from residual heat exchanger 1A (event RH-CP in the charging pumps fault tree, which transfers from event R57 in RHR fault tree) or from residual heat exchanger 1B via safety injection pipes (event SI-CP in the charging pumps fault tree, which transfers from event S67 in the safety injection fault tree).

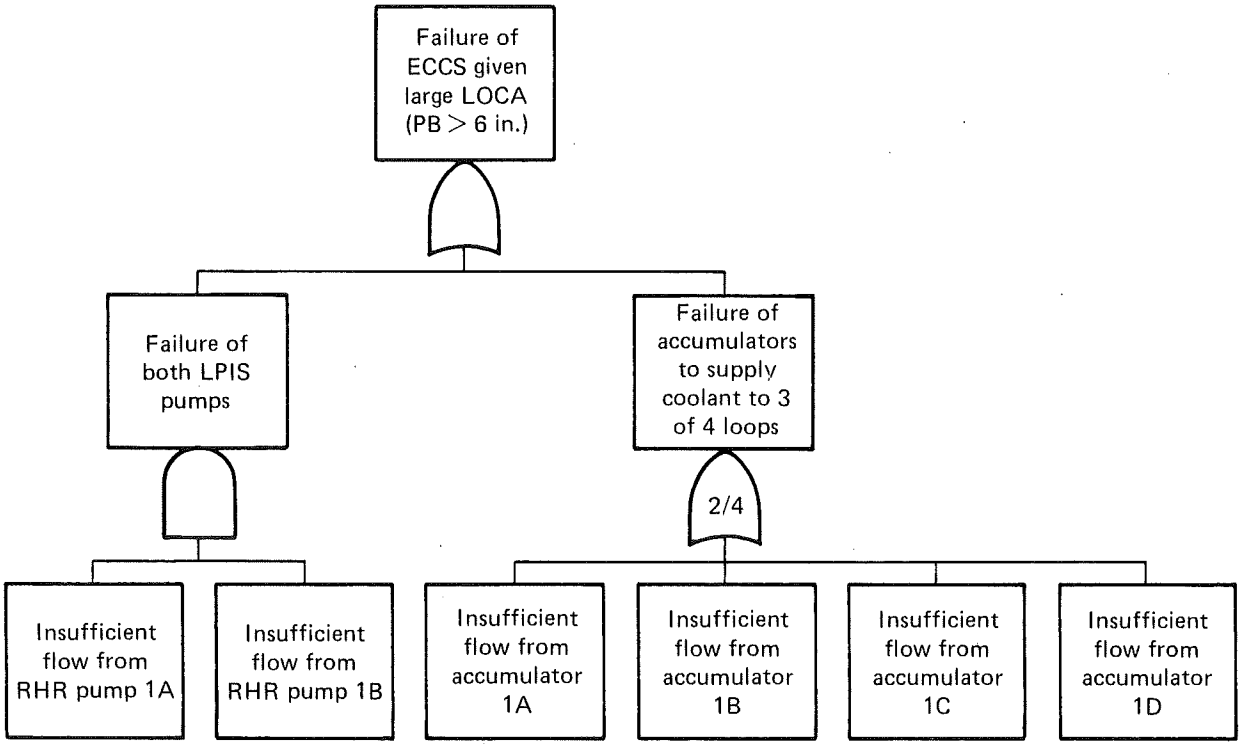


Figure D.2. Failure of ECCS given large LOCA (injection mode).

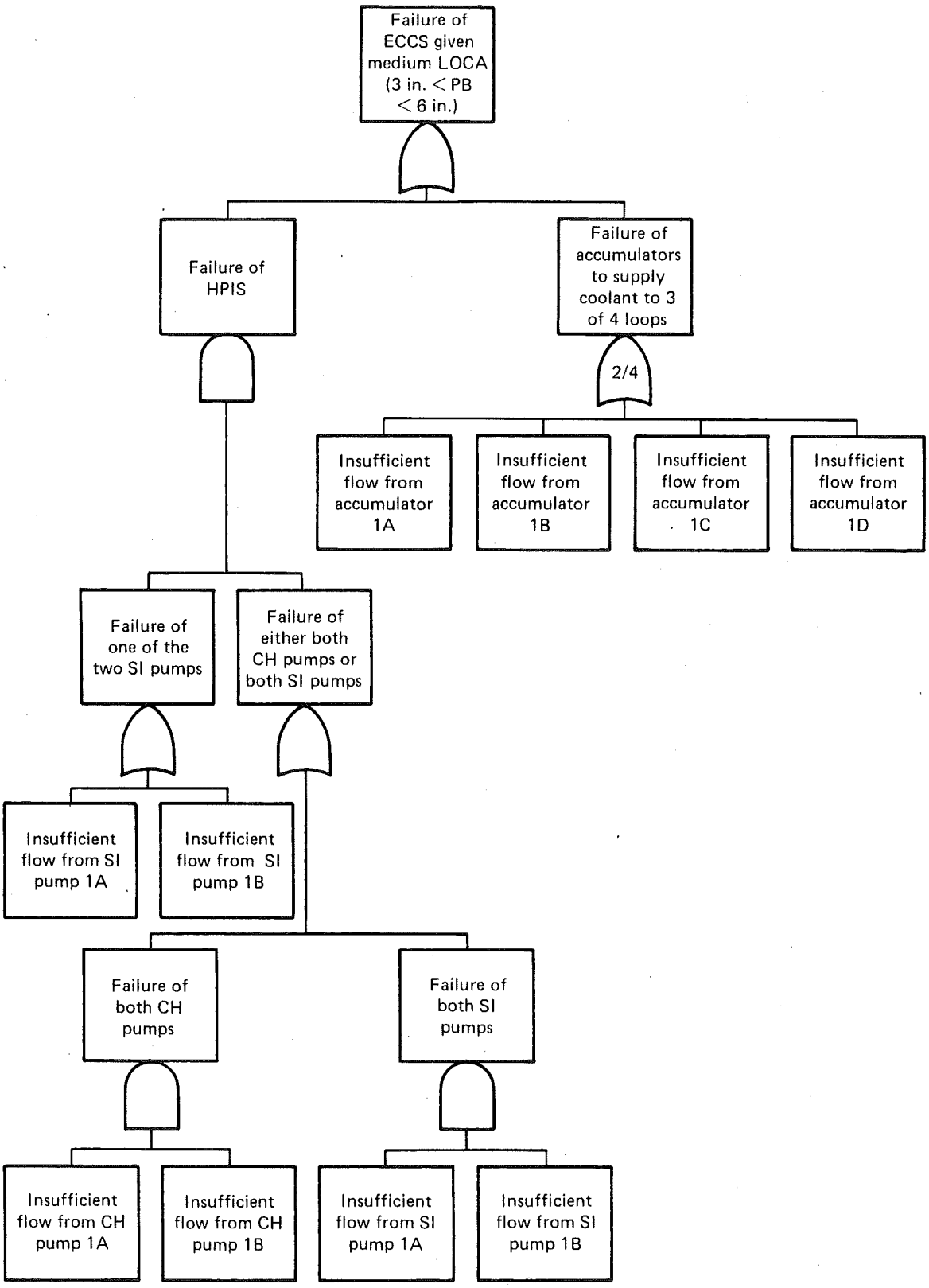


Figure D.3. Failure of ECCS given medium LOCA (injection mode).

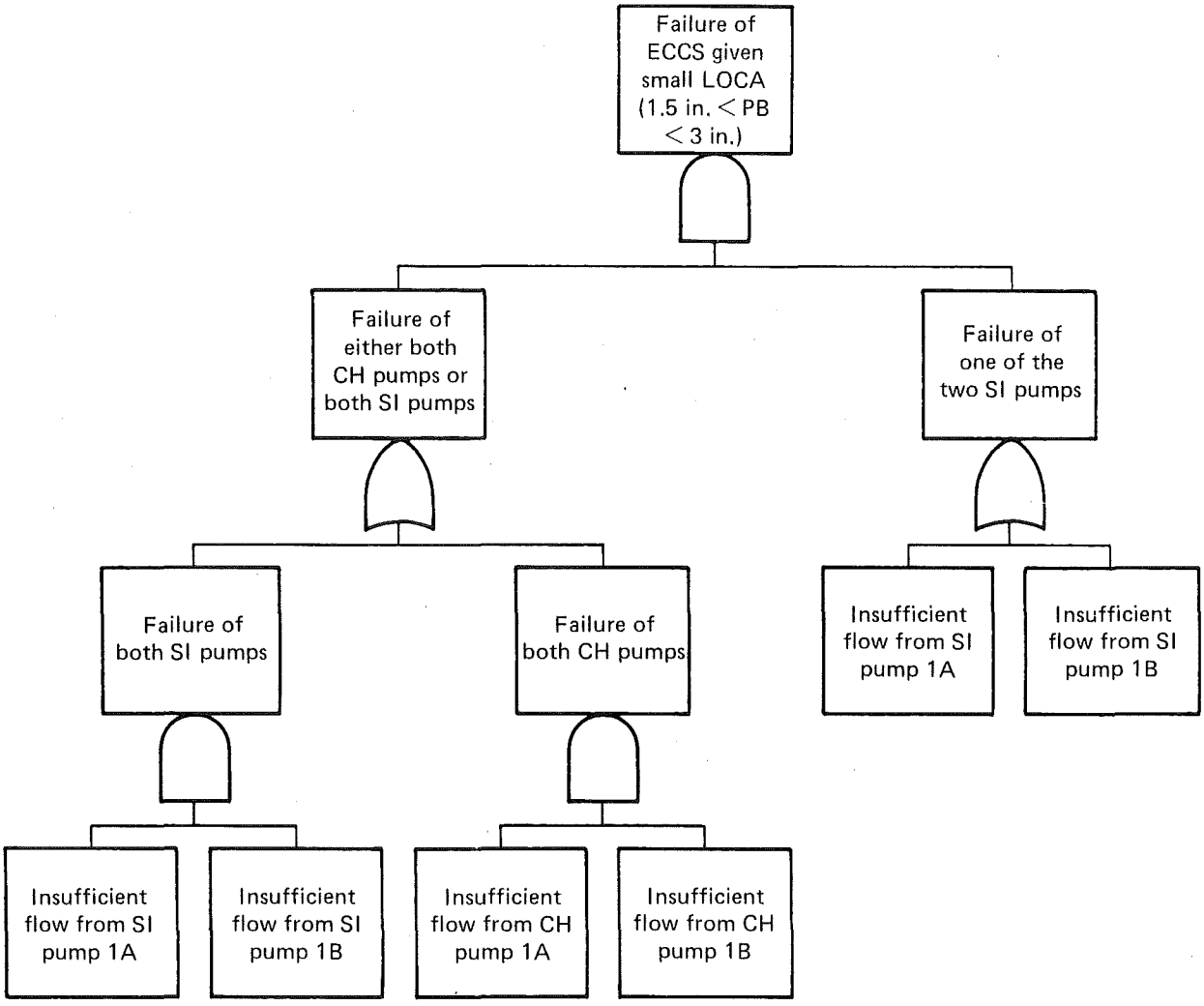


Figure D.4. Failure of ECCS given small LOCA (injection mode).

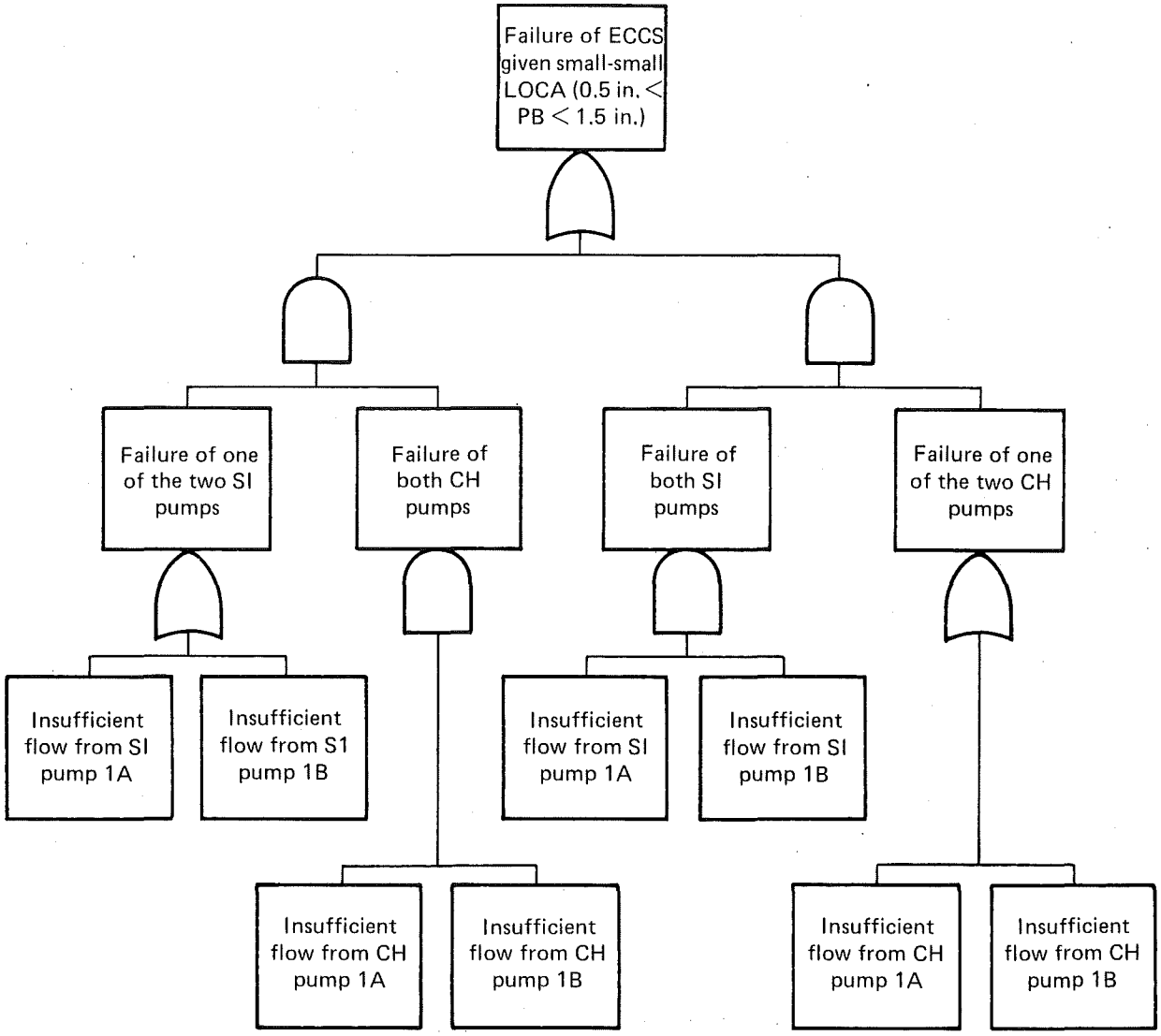


Figure D.5. Failure of ECCS given small-small LOCA (injection mode).

SECTION D.3: AUXILIARY FEEDWATER SYSTEM

We now consider the response of the Auxiliary Feedwater System (AFWS) to a seismically initiated nuclear power plant accident. The event tree analysis discussed previously identified the AFWS as an important system in the event of a small-small LOCA or a transient-initiated accident. Such an accident requires removal of the decay heat from the core by the secondary side of the Nuclear Steam Supply System (NSSS). In order for the secondary side to successfully remove the heat, the steam generators must be adequately cooled by the associated active systems designed for that purpose. Both the AFWS and the Power Conversion System (PCS) can deliver cooling water to the steam generators. In the following pages we describe the analysis of the AFWS in light of the above considerations.

D.3.1 AFWS SYSTEM DESCRIPTION

If the PCS is not available, the AFWS is required to provide adequate coolant to the steam generators. The design of the AFWS specifies that one of the three auxiliary feedwater pumps delivers water to two of the four steam generators at or below the pressure of the secondary steam relief safety valve set points. The system is composed of:

- Five secondary steam relief safety valves and one power-operated relief valve for each steam generator, any one of which will sufficiently depressurize the steam generator.
- Two motor-driven pumps requiring power from the 4160 KV emergency AC buses.
- One turbine-driven pump at twice the required rated capacity, requiring steam from either the main steam line A or D.
- Two headers connected by normally locked-closed manual isolation valves, each of which can deliver to all four steam generators through normally open valves.
- Eight normally open, air-operated throttling valves requiring instrument air, but failing open.
- One connection from each of the two headers to each main feedwater line leading to each of the steam generators.

- The preferred source of cooling water is from the secondary condensate storage tank which is not seismically qualified. It is located outside the auxiliary building.
- A secondary source from the service water system which is automatically or manually activated on low pump suction pressure.
- One supply header for each pump, all interconnected by normally open AC motor-operated valves.
- Associated check valves on the pump supply headers and the headers to the main feedwater line.
- Normally open manual valves for isolation of each pump for maintenance.
- Miniflow test lines from each pump to the secondary condensate storage tanks.

The equipment listed above is designed to Seismic Class I design codes, except for the secondary condensate storage tank and its supply header. The pumps, the discharge header piping up to the containment penetration, the supply header piping from the service water system interface, and the supply header piping from the secondary condensate storage tank header interface are all located inside the auxiliary building. The main feedwater header, the steam generators, and the interconnecting AFWS piping are located inside the containment. Additionally, the service water system and condensate system involve piping that is located on or under the turbine building, and also outside of it. (The service water system starts at the crib house.)

When the auxiliary feedwater system is needed, it must operate to remove decay heat before boil-off of the primary system inventory causes sufficient uncovering of the core to result in an irreversible melting of the fuel rods. This time period is from 1 to 1-1/2 hours [based on calculations referred to in Appendix I, page 61, of the Reactor Safety Study (RSS)]. This includes 1/2 hour until the U-tube steam generators have boiled dry. After this time period, additional stresses are placed on the steam generator when it is refilled; however, this effect has been ignored in terms of causing further structural failures in the secondary system or primary/secondary interface.

Certain transient event initiators could result in simultaneous degradation of the AFWS operability. A main feedwater line rupture between the check valve inside the containment and the connection to the steam generator would disable one steam generator and would require isolation by the operator to avoid AFWS flow out of the rupture. Additionally, a loss of offsite power would mean that diesel power from one of the diesel generators

would have to be available to supply electric power to run the AC motor-driven pumps and to provide lubrication for the steam turbine-driven pump. Finally, a break in main steam lines A and/or D would eliminate or reduce redundancy in the steam supply to the turbine-driven AFWS pump. Steam generator tube ruptures also result in the loss of the associated steam generator for use in the cooldown process because the affected steam generator must be isolated to limit radiation releases out of the secondary steam-relief valves. Steam generator tube ruptures place additional burden on the operators, a factor which is discussed in this section.

When an accident occurs which requires heat transfer from the primary system to the secondary system, the heat transfer must take place until the residual heat removal system can cool the reactor from hot shutdown to cold shutdown. The length of time the heat transfer takes affects the likelihood of the pump's failure to run; the repairability of components; the adequacy of the secondary condensate storage tank cooling inventory; and the failure and repair of interfacing systems, such as the service water system and the emergency electric power system. The secondary condensate storage tank has an alarm at the 170,000 gallon level (its capacity is 500,000 gallons). This would supply adequate coolant inventory for between 8 to 24 hours, assuming the nonseismic tank and header survived the initiating earthquake.

The AFWS naturally interfaces with the instrumentation and control system. The motor-driven pumps are activated by the following signals:

- Low water level on any steam generator.
- Safety injection control signal.
- Loss of offsite AC electric power.

The steam turbine-driven pump is activated by either of two signals--low water level on any two steam generators or complete loss of AC electric power (offsite AC plus emergency AC). In addition, the cooling-water supply from the service water system is activated automatically on low suction pressure to the pumps. Manual activation of the pumps and valves is possible if automatic signals do not initiate operation of the system.

The operators interface with the AFWS system by controlling the flow of coolant to the secondary side. The control is achieved by air-operated throttling valves in each of the two header legs to each steam generator.

Backup-control is provided by AC motor-operated valves. The operators must allow enough coolant to the steam generators to avoid boil-off of the primary coolant. However, they must not cool the steam generators too rapidly. Too rapid a cooldown can result in additional structural effects on the primary system. To determine these effects, the operator depends on the instrumentation associated with the steam generator water level and system flow indicators.

Further, if line breaks occur as a result of the earthquake initiator, the operator must isolate them and align the correct coolant flow path to the steam generators and/or the pumps and/or water supplies. Pump flow indicators and the pump suction line low-pressure annunciator also provide information to the operator.

Finally, a steam generator tube rupture accident, which is similar in most respects to a small-small LOCA, requires operator identification. It differs from the small-small LOCA in that radiation from the primary coolant is leaked into the secondary side and out the secondary steam relief valves. This results in the lighting up of a secondary side radiation-level annunciator. From this instrumentation, as well as the steam generator water level instrumentation, the operator must then isolate the affected steam generator to prevent it from releasing too much radiation into the atmosphere. This process is not trivial: according to the FSAR, it requires turning off the high pressure injection pumps (charging pumps) within a certain time period. Given the new time limitations on turning off the high pressure injection pumps resulting from the Three Mile Island accident and the difficulty in identifying the affected steam generator, it is possible that the water level in the steam generator can go high enough to fill the main steam line associated with that steam generator. This would result in a quenching of the steam flow from that steam generator.

In addition, if the steam generator water level instrumentation is lost, the operator is likely to err in the direction of overfilling the steam generator. Again, the result could be quenched steam flow in one or more steam generators. If the quenched steam flow occurs in either main steam line A or D, the redundancy of the steam supply to the steam turbine pump is compromised.

In an analysis concerning randomly initiated events, the operator-instrumentation interface can be ignored because the probability of instrumentation failure is low. However, in an earthquake-initiated event, the simultaneous occurrence of an accident initiator and instrumentation failures cannot be ruled out. In this situation, the operator response would be based on severely limited information and would therefore be less likely to succeed. The likelihood of the operator failing to correctly complete the required action is dependent on the state of the crucial instrumentation. For this reason, whenever operator action is required, the piece or pieces of instrumentation crucial to that action are identified. This identification made possible a better assessment of the instrumentation response to a seismic event.

Finally, the maintenance and test procedures for the AFWS affect the system availability. According to the Zion technical specifications, up to two of the three auxiliary feedwater pumps can be simultaneously out of service. The resulting degradation of system availability is modeled by the use of a three-component dependency model, which had been developed previously by SAI. In the SAI model, the probability is zero of Pump 1C being in maintenance when Pumps 1A and 1B are in maintenance. The probability of any other combination of maintained pumps being out for maintenance at the same time would be taken from Zion data on limiting conditions for operation (LCOs). This information could also be obtained from another data source, such as the RSS. The AFWS is tested on a monthly basis.

In this section we have described the design basis and the framework under which the AFWS was examined. An earthquake-initiated event is unique in that it affects every component in the plant simultaneously. For this reason, a thorough analysis is required of every component and every interface of the AFWS. The continuing examination of other important safety systems may bring even more information to light. Therefore, a complete review of this analysis will be made on a continuing basis.

The following section describes the fault tree analysis process. It includes more details and a complete outline of the assumptions made in developing the tree.

D.3.2 AFWS FAULT TREE MODEL

The fault tree analysis process incorporates into a calculational model the information described in the preceding section. The result is a calculational tool applicable to all ranges of earthquake-initiated effects. In this analysis the AFWS fault tree was developed as part of the input to the event-tree element representing heat removal to the environment. The top event of this fault tree was "insufficient cooling of the steam generators." To find all the possible failure modes of the system or top event, the flow of cooling water was traced from each steam generator all the way back to the cooling-water supply. In analyzing the system, we employed the system diagram as a map and a topological analysis (Fig. D.6). The flow of cooling water to the steam generators was traced to its input header, then to the headers of the motor- and turbine-driven pumps, from there to the pumps, then to the supply headers, and so on. As each component along the flow path is encountered, a complete review is made of its basic failure modes, its interfaces, and its location. The advantage in this approach is the increased assurance that the model is complete. Also, more failure modes may be discovered.

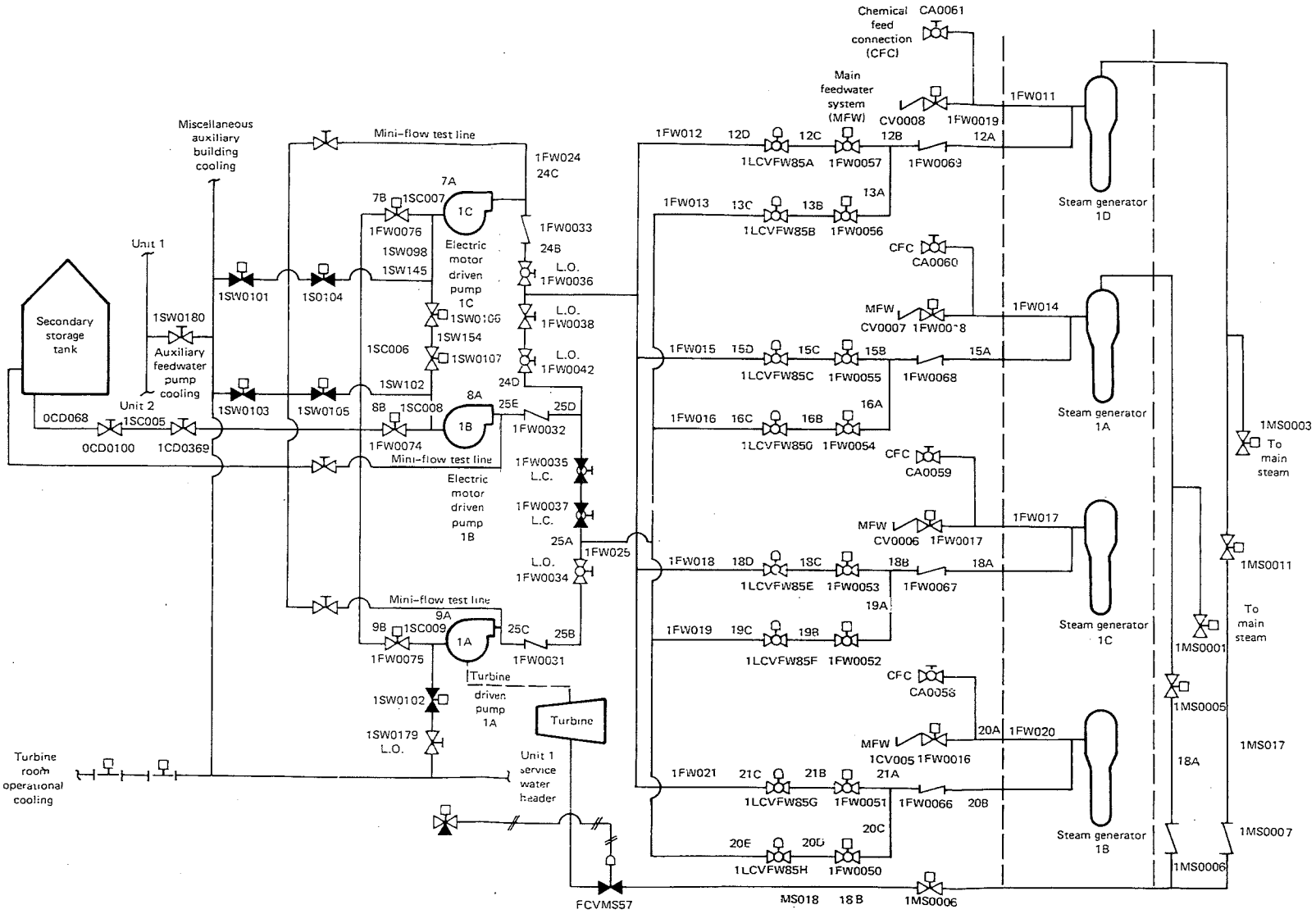


Figure D.6. Description of AFWS.

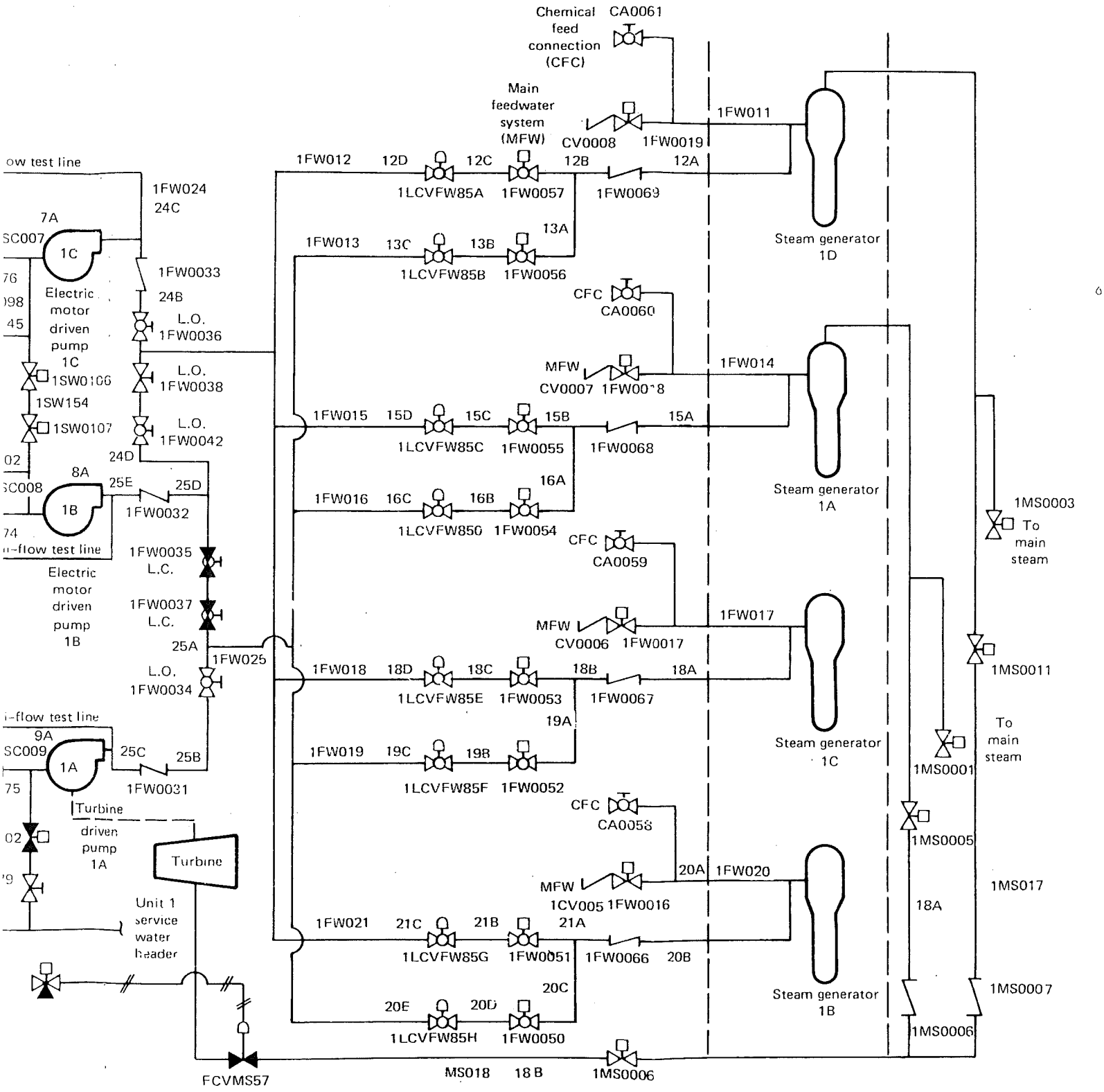
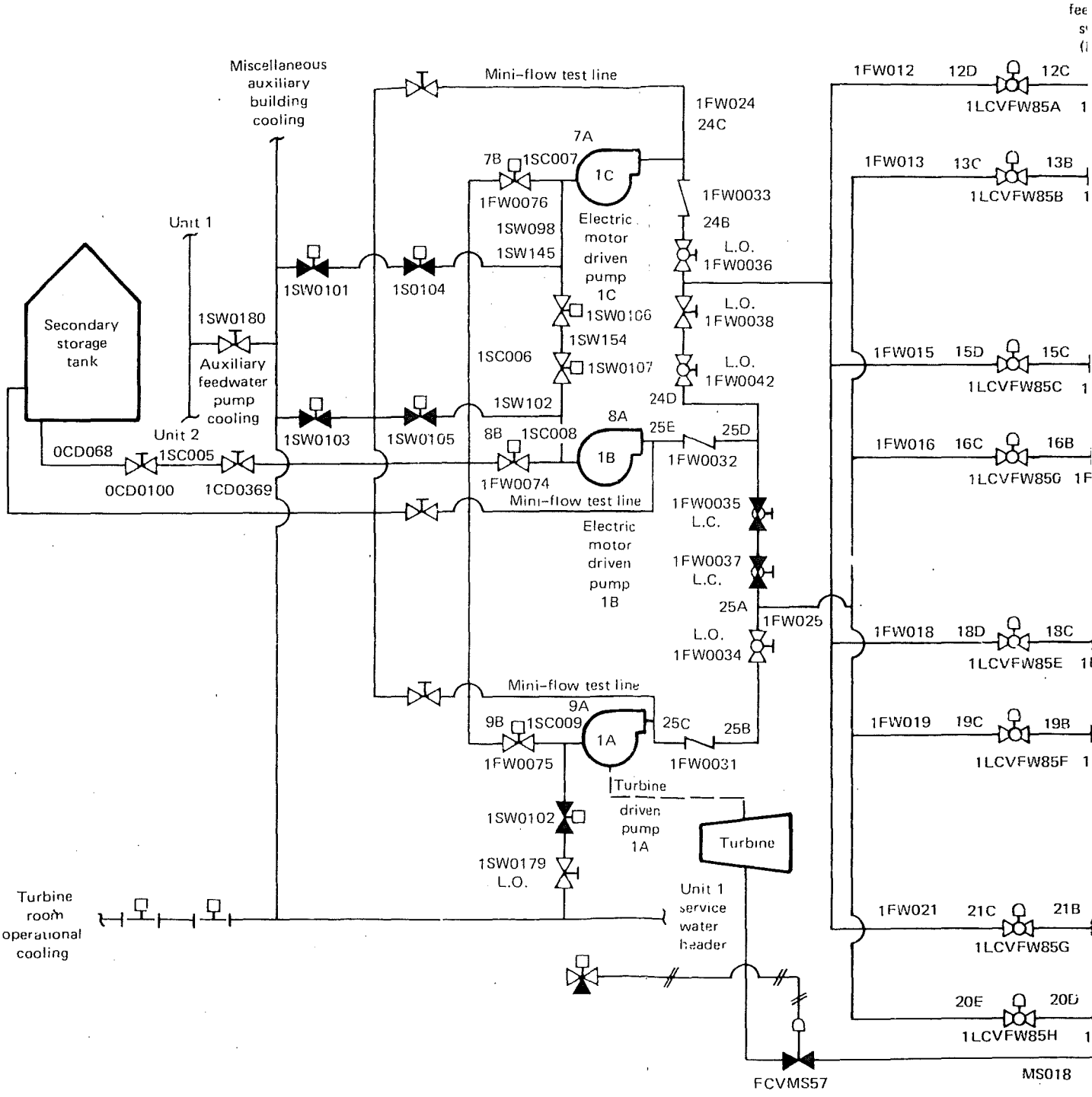


Figure D.6. Description of AFWS.


Miscellaneous auxiliary building cooling
Mini-flow test line
1FW024
24C
7A
7B
1SC007
1C
1FW0076
1FW0033
24B
1SW098
1SW145
Electric motor driven pump 1C
L.O. 1FW0036
Unit 1
1SW0101
1SO104
1SW0180
Secondary storage tank
Auxiliary feedwater pump cooling
1SW0106
L.O. 1FW0038
1SW154
1SC006
1SW0107
L.O. 1FW0042
24D
1SW102
8A
Unit 2
1SW0103
1SW0105
8B
1SC008
25E
25D
1B
1FW0032
0CD068
1SC005
0CD0100
1CD0369
1FW0074
Mini-flow test line
1FW0035 L.C.
Electric motor driven pump 1B
1FW0037 L.C.
25A
1FW025
L.O. 1FW0034
Mini-flow test line
9A
9B
1SC009
25C
25B
1A
1FW0075
1FW0031
Turbine driven pump 1A
Turbine
1SW0102
1SW0179 L.O.
Turbine room operational cooling
Unit 1 service water header
FCVMS57
MS018
1FW012
12D
12C
1LCVFW85A
1FW013
13C
13B
1LCVFW85B
1FW015
15D
15C
1LCVFW85C
1FW016
16C
16B
1LCVFW85G
1FW018
18D
18C
1LCVFW85E
1FW019
19C
19B
1LCVFW85F
1FW021
21C
21B
1LCVFW85G
20E
20D
1LCVFW85H

SECTION D.4: SERVICE WATER SYSTEM

In this section we consider the response of the service water system (SWS) and its associated safety related functions to an earthquake-initiated LOCA or a transient event. During the course of the event tree analysis, it became clear that since the service water system interfaced with many of the important systems, it should be classified as a critical system for SSMRP analysis. We therefore include a description of the system and the definition of its design basis. We also discuss the service water system relationship with possible transient initiators. In addition, we discuss the modeling of the system with respect to normal and emergency operation valving configurations, and also with respect to the requirements of Zion Unit 2 (Zion Unit 1 is the object of the SSMRP analysis). Finally, the fault tree analysis of the service water system is presented and broken down into each of its important functions. The fault tree analysis includes a common-cause failure review, an instrumentation and control and operator interface review, and identification of the important assumptions made in the modeling process.

D.4.1 SWS SYSTEM DESCRIPTION

The function of the service water system is to provide the cooling water necessary for all plant equipment. The service water system differs from the other important plant systems in two respects: it is interconnected with Zion Unit 2, and it is required for both normal and emergency operation. The design requirements for both LOCA and transient-initiated events are that one out of three pumps per unit must be operational. (In normal operation, two out of three service water pumps per unit are required.) It has been assumed that the one-out-of-three requirement will satisfy all emergency requirements consistent with the SSMRP systems analysis task only if the system can be brought from the normal configuration to emergency configuration. In addition, the water delivered from the crib house on Lake Michigan by the pump sets of both Unit 1 and Unit 2 must reach the equipment it is designed to service.

The following equipment cooling functions were analyzed:

- Containment fan cooling system fan motors and heat exchangers.
- Component cooling-water heat exchangers.
- Diesel-generator-cooling heat exchangers.
- Auxiliary feedwater pump cooling.

The following emergency cooling functions were assumed to be less important to the systems analysis task:

- Auxiliary building HVAC.
- Emergency pump room coolers: RHR, SIS, etc.
- Penetration pressurizers for the containment.
- Computer room and control room HVAC.

The following assumptions were made: the HVAC and pump room coolers are not crucial for bringing the plant to hot shutdown, the penetration pressurizers do not have a critical effect on containment leakage paths, and equipment could run without room-cooling under emergency conditions. This may be modeled more accurately if one assumes that the equipment failure rates would be dependent on the temperature in the room.

In addition to its equipment cooling function, the service water system can serve as a water supply for the auxiliary feedwater system and the fire water system.

The service water system is designed to Seismic Category 1, with the exception of the return piping from the safety related equipment. Because the service water system is required for normal operation, the loss of all or part of the system capabilities could result in a transient accident. This system is vital: the loss of service water required for emergency operations would result in a core melt. Therefore, a transient initiated by a pipe rupture in the common pipe between Unit 1 and Unit 2, and failure to isolate it, would result in the loss of both units. Also, transients caused by the loss of a service water pump could result in a degraded service water system, and normal operation of this system is required to protect the plant. Because of this importance, the interfaces should be properly accounted for in the list of failures causing a transient with resulting loss of the power conversion system because related equipment is cooled by the operational mode of the service water system. These types of failures could be important elements in the most likely cut sets of total plant failure because they are common to both the initiator and the emergency safeguards.

A fault tree model of the service water system must include consideration of the system's role in Unit 2 emergency requirements and in changing from normal operational status to emergency status. The SWS is a system which provides for both Zion units; however, it is generally considered as two independent systems with crossties, each with the capacity to provide for the emergency requirements of both units simultaneously. Because a correct model must consider the effects of this redundant capacity, it is conceivable that a particular unit's configuration of three service water pumps could provide the pumping flow for both Unit 1 and Unit 2 accident needs. The system also includes a redundant set of electric motor-operated isolation valves, which can be closed automatically or manually, thereby cutting off the water flow to the parts of the system which provide for normal plant operation. This reduces the pumping requirements from the two out of three per plant required for the normal operation system configuration to the one out of three per plant required for the emergency operation system configuration. The requirement on one unit's service water pumps for pumping to the other unit (as a result of that unit's part of the SWS failing to operate in an emergency) would be equivalent to an extra pump load. The requirement on that unit's service water pumps, if the isolation valves fail to close off the water flow to normal operational parts of the system, would also be equivalent to an extra pump load.

- Pump A, B, or C fails to provide flow to the system (failure of a positive flow).
- The other unit requires flow for its cooling requirements (existence of a negative flow).
- One of two isolation valves fails to close and isolate operational equipment (existence of a negative flow).

The model described above will be found in the fault tree for main service water headers for Unit 1 and Unit 2 (SWA and SWB event names, respectively). A system description of the service water system would also normally consider the timing requirements of the system, the instrumentation and control system, and operator and other system interfaces. Because the service water system has many important functions, we felt it best to discuss these in the fault tree analysis section, which follows. Each function is considered separately, and the above requirements are discussed for each function. In

addition, the next section contains a description of the assumptions made in the analysis, a review of common-cause failure, and an assessment of the failure modes of each function and the conclusions drawn from those results.

D.4.2 SWS FAULT TREE MODEL

The fault tree analysis process incorporates the information contained in the system description into a calculational model. The result is a tool, expressed in Boolean logic, applicable to all ranges of earthquake-initiated effects. Normally, a fault tree is defined by its top event. However, the service water system has many top events and safety-related functions, so the analysis is divided into five sections, each of which describes a separate function of the service water system. The five sections are:

- Main service water headers and pumps for Unit 1 and Unit 2 (Fig. D.7).
- Cooling for diesel generators 0A, 1A, and 1B (Fig. D.8).
- Cooling for the containment fan coolers and motors 1A through 1E (Fig. D.9).
- Cooling for AFWS pumps 1A, 1B, and 1C (Fig. D.10).
- Cooling for the component cooling water heat exchangers for Unit 1, Unit 2, and the shared heat exchanger.

These sections contain the description of the fault tree submodels which were input into other fault trees developed as part of the SSMRP systems analysis. Each of these submodels includes all the failures resulting from the system bringing cooling water from Lake Michigan to the equipment in question.

One very important function of the service water system is to supply water to the AFWS. Since the AFWS draws off the main headers directly through valves which are normally closed, automatically activated, and electric motor-operated, the fault tree model input to the AFWS is that of the main headers. The failures associated with the motor-operated valves are treated in the AFWS fault-tree model. Therefore, we judged the five functions described below sufficient to model all the safety related functions of the service water system.

D.4.2.1 Main Service Water Headers

Both Unit 1 and Unit 2 have 48-inch-diameter main water-headers supplied by three electrically operated centrifugal pumps. The pumps draw suction from the crib house forebay. Each header passes under the turbine building to the auxiliary building. At the auxiliary building, further piping and electrically operated isolation valves provide the water for each required safety function. The main headers, up to the piping for each safety function, are labeled in the fault tree as SWA for Unit 1 and SWB for Unit 2 (Fig. D.7).

Each main header is fed by two smaller lines. Each of these lines contains an electrically operated strainer with sufficient flow capacity for the main header. It is assumed that one of the strainers could be in maintenance. The strainers can be isolated by manual valves for maintenance or in case of rupture. It has been assumed that drain system failure would not impact on emergency operation. It has also been assumed that electric power will not be required: this assumption is important since both Unit 1 strainers are powered from the same MCC 1392, in Division 19.

For each unit, two strainers lead to a common pipe fed by the three service water pumps for that unit. The service water pumps for Unit 1--1A, 1B, and 1C--are powered by Divisions 17, 18, and 19, respectively. Service-water pumps 2A, 2B and 2C are powered by Divisions 27, 28, and 29. It should be noted that Division 17 and Division 27 compete for the same diesel backup. There is a lubrication system common to both units. Immediate lubrication requirements are met by an individual 30-gallon tank for each pump. It was assumed that the common elements of the lubrication system were needed only for long-term operation. It was further assumed that the lubrication system would be repaired and therefore would not have a significant impact on system unavailability. Because the water supply is cold water from Lake Michigan, the pumps do not require cooling. In fact, each pump has a heater. It was assumed that heater failure would not have a significant effect on pump performance.

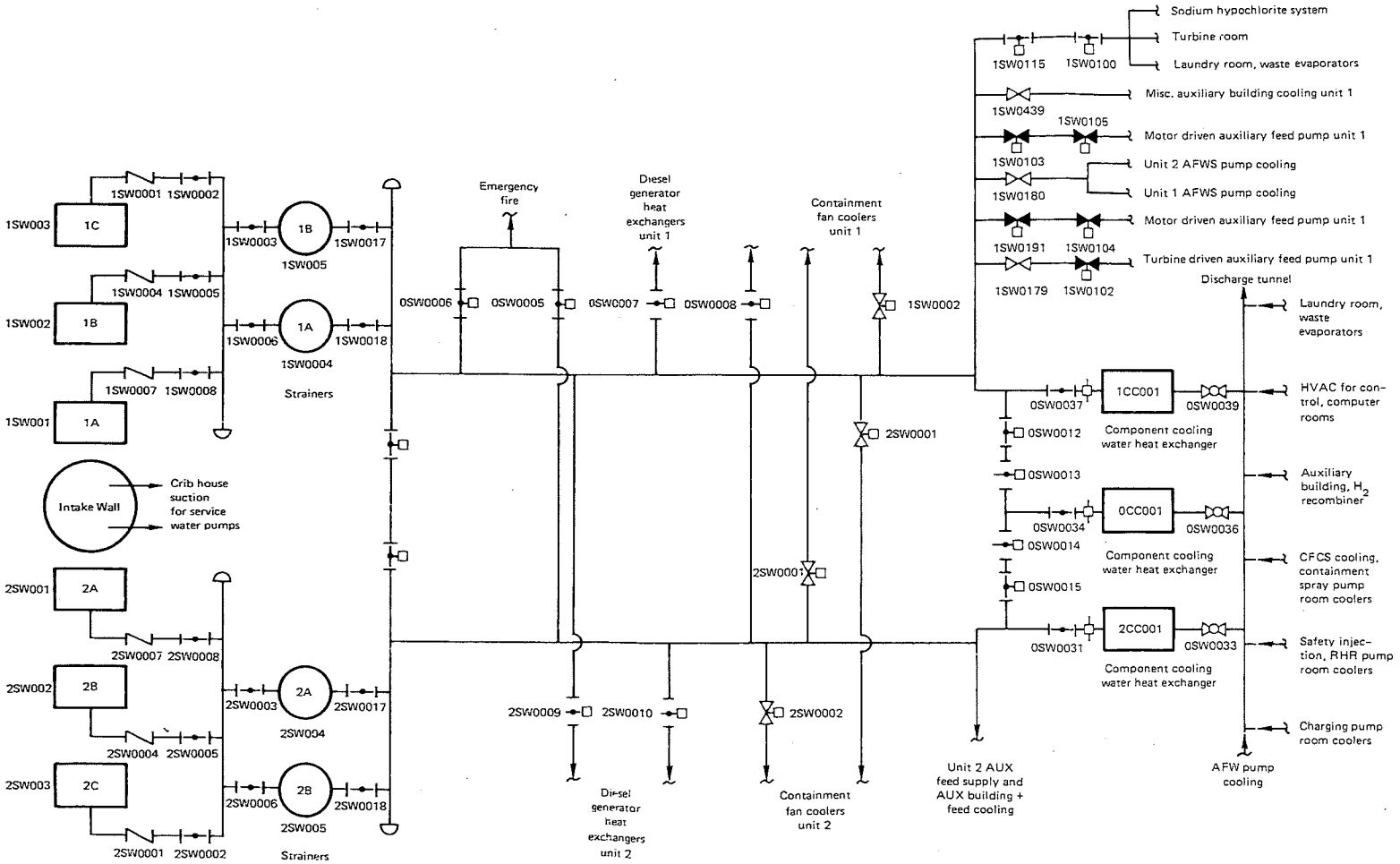


Figure D.7. Service water pumps and supply.

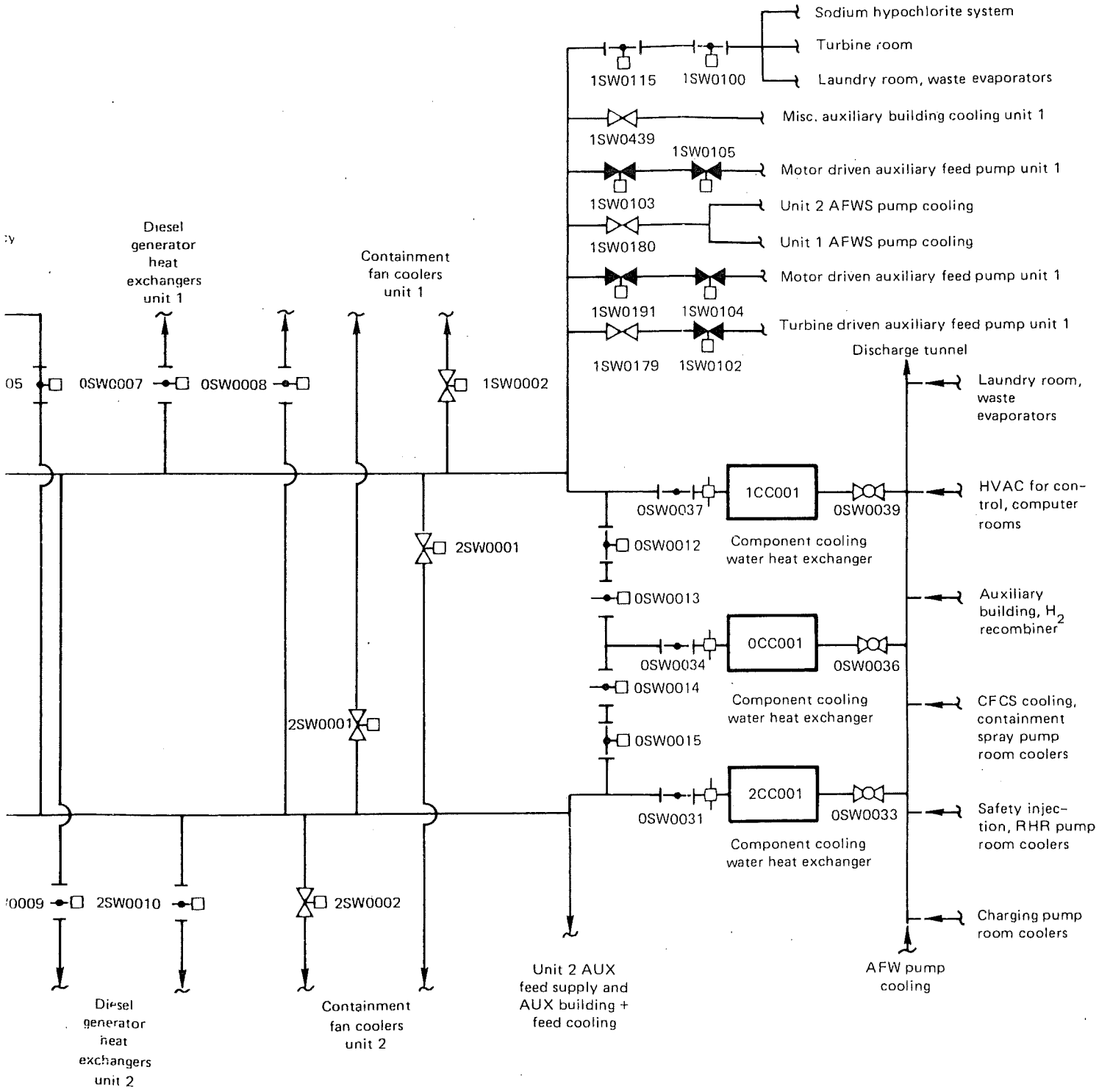
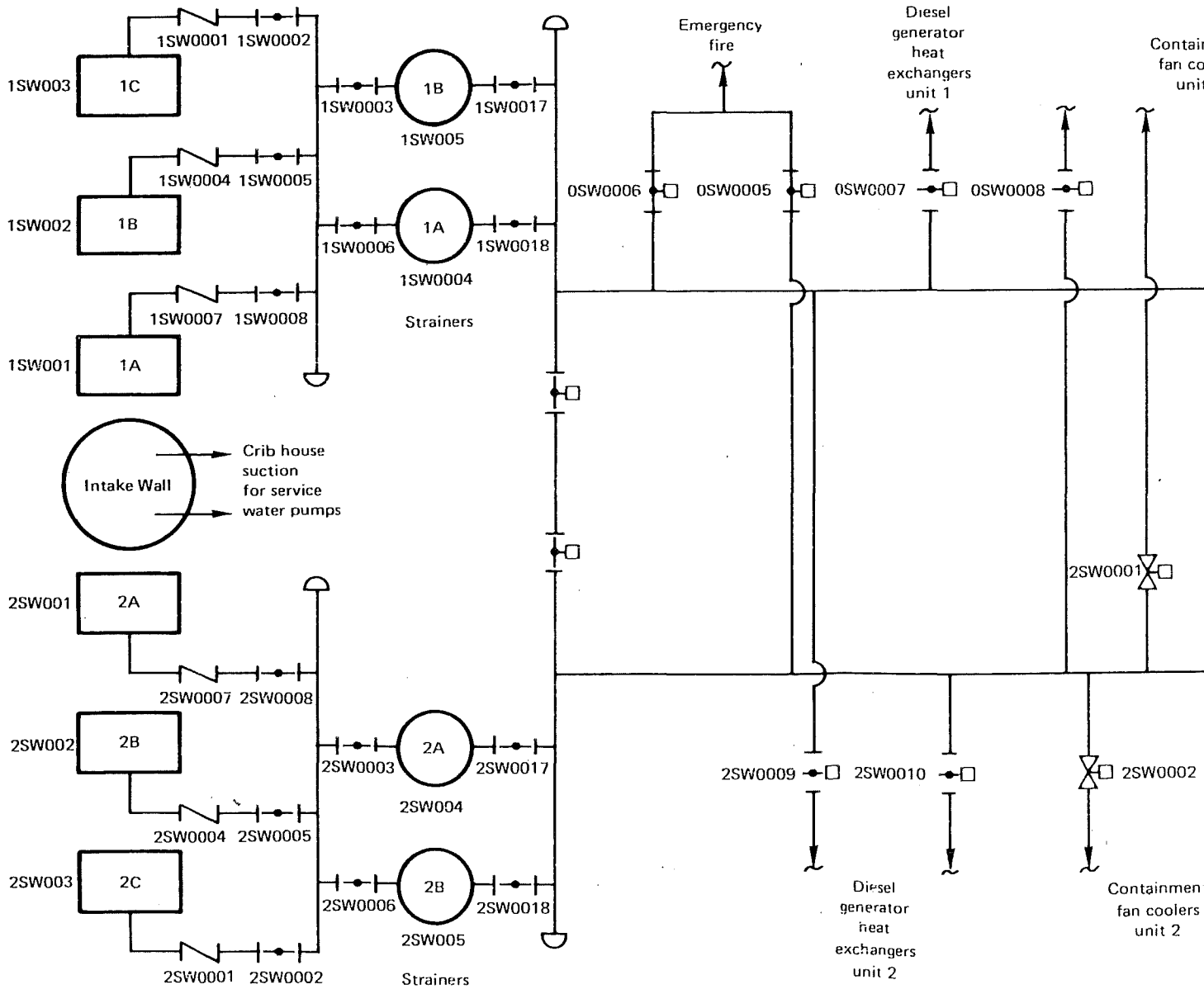


Figure D.7. Service water pumps and supply.


1SW0001 1SW0002
1SW003
1C
1B
1SW0003
1SW0017
1SW005
1SW0004 1SW0005
1SW002
1B
1A
1SW0006
1SW0018
1SW0004
1SW0007 1SW0008
Strainers
1SW001
1A
Intake Wall
Crib house suction for service water pumps
2SW001
2A
2SW0007 2SW0008
2SW002
2B
2SW0003
2A
2SW0017
2SW004
2SW0004 2SW0005
2SW003
2C
2SW0006
2B
2SW0018
2SW005
2SW0001 2SW0002
Strainers
Emergency fire
Diesel generator heat exchangers unit 1
0SW0006
0SW0005
0SW0007
0SW0008
2SW0001
2SW0009
2SW0010
2SW0002
Diesel generator heat exchangers unit 2
Containmen
fan coolers
unit 2

Given that the service water system is normally in operation, two of the three pumps will already be operating, with the third in standby. Consequently, only the standby pump (assumed for simplicity to be Pump A) is required to start if it is needed. The two failure modes for Pump A are failure to start and failure to receive either an automatic or manual signal to start. It has also been assumed that one of the three pumps per unit can be in maintenance. Since, if this is true, the standby pump will be operating, the "failure-to-start" failure modes are made mutually exclusive from any pump in maintenance. Each of the main service water headers contains flow indicators. Additionally, each pump has a lubrication indicator. This is the only SWS instrumentation in the control room discernable in the P&IDs. Therefore, any ruptures or pump failures or other actions requiring operator intervention are modeled to be dependent on the status of the flow indicators in Unit 1. There are also local instrument panels in the control room with further information; however, it was judged that these would be of no value to the control-room operator.

The timing requirements of the main service water system are dependent on the timing of the most limiting function. However, since repair has not generally been considered, this time-dependence is not very important. It has been assumed that no single function's timing requirements would preclude time for operator intervention.

The failure modes of the main service water headers will now be described. Each header will fail if there is a rupture in the 8-inch-diameter pipe or if ruptures occur in the pipe common to all these pumps. These single events will result in a failure of SWA or SWB. Since the main pipes are located in close proximity and in similarly structured locations, their rupture failures will be coupled events in terms of seismic response. Therefore, this event is the most critical, although not necessarily the most likely, failure of the entire two-unit system.

Each main header will also have associated with it a number of double events leading to failure. These include strainer rupture coupled with failure of the operator to isolate, and rupture in the other header coupled with failure of the operator to isolate. Additionally, simultaneous strainer failures, or a strainer in maintenance and failure of the other strainer, will be doubled, leading to failure of SWA or SWB, depending on the particular failure. Since generally either SWA or SWB are sufficient to provide water for each function, the failure of both is the most important top event. Since

a rupture in either header requires isolation of the other header, this failure would also be an entire system failure. Therefore, this is the most important double event leading to the entire service water system failure.

Any other combinations of events leading to complete system failure will be of significantly higher order. Individual main service water headers can have triple events leading to failure, as defined by the three out of five pumping model described earlier. However, to fail, both headers would require the simultaneous occurrence of at least a quadruple event--triple for one header and a single for the other. Given the extremely large combination of such events, they will not be treated specifically. Also, as the service water system has been shown to be relatively immune to common-cause failures, these very high order failures are likely to be the next most important failures, other than ruptures in the main headers.

In conclusion, if the main service water headers fail to rupture in the initiating earthquake, it would then require more than two failures for complete failure of the system. It should be noted, however, that movement of the crib house relative to the turbine building could be a very important event, resulting in simultaneous rupture of the service water headers.

In the following subsections, each of the four individual cooling functions will be addressed. Each of these will require the main headers to provide flow to their piping configurations; each will therefore contain some common and some unique failures.

D.4.2.2 Diesel Generator Cooling

The main service water headers are intertied by a pipe with two MOVs operable from the control room. Tracing the header piping, the next piping system encountered is the fire-water supply system. Following the fire-water system, each header is intersected by two pipes which provide cooling water for each unit's diesel generators. In that way, cooling water can be supplied to all diesel generators from either unit. Normally closed electric motor-operated isolation valves receive a signal to open, which provides water to a piping loop that feeds diesel generators 1A, 1B, and the swing diesel, 0A. The normal loop valving configuration sends Unit 2 service water to the swing diesel and Unit 1 service water to the Unit 1 diesels (Fig. D.8). If either water supply is unavailable, the operator can open an isolation valve

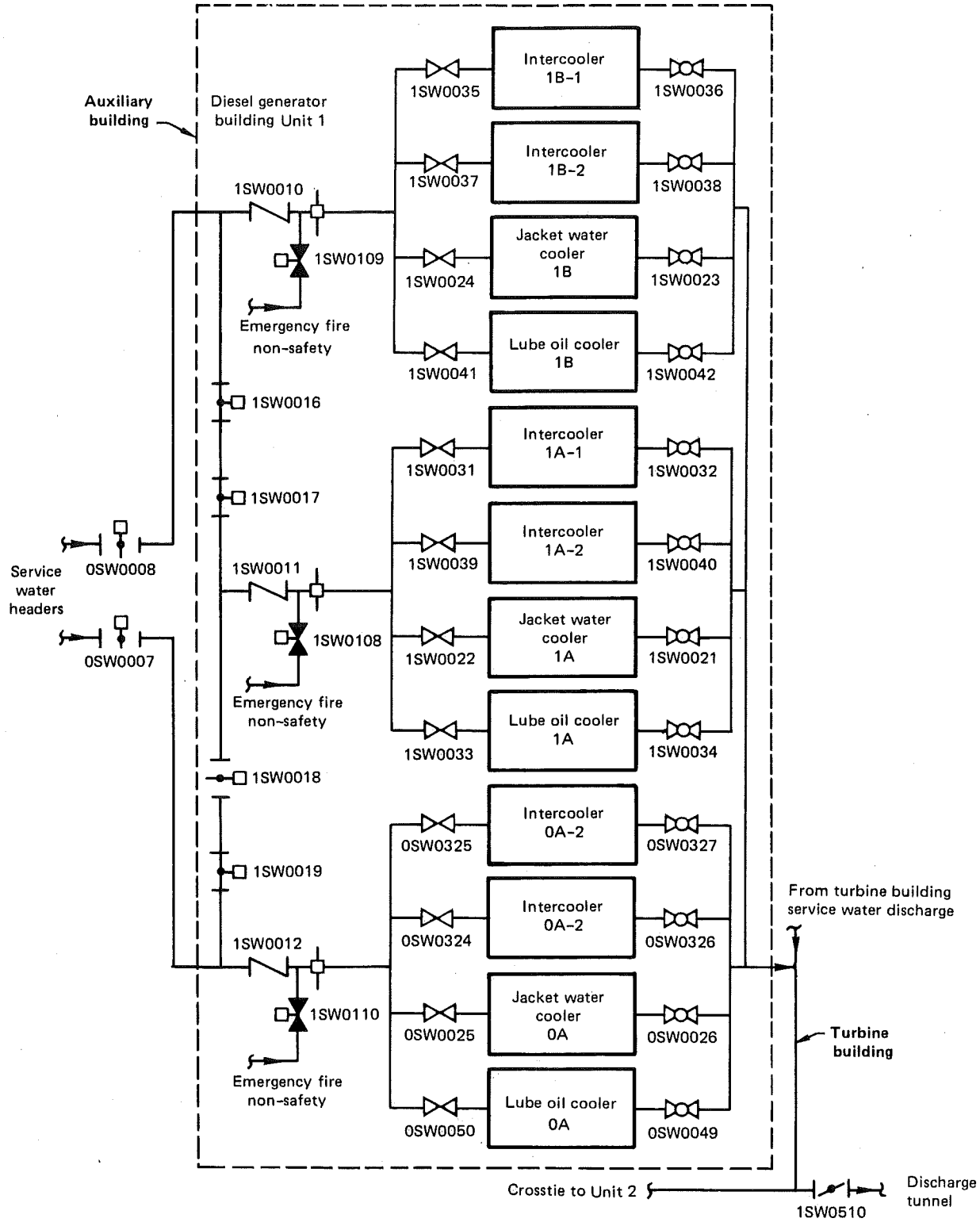


Figure D.8. Diesel generator cooling portion of the SWS.

from the control room and cool each diesel generator from either unit. This loop feeds three cooling arrays of four heat exchangers each. Each diesel has two intercoolers--one jacket water cooler and one lube oil cooler--both of which have been assumed to be required for successful diesel operation. Each heat exchanger is isolated by two isolation valves. These cooling arrays also can each be fed by a fire-water system connection. This connection occurs through an operator-controlled motor-operated valve. It should be noted that this connection through the fire-water system is not a Seismic Class I design. Each cooling array receives its water from the main loop through a check valve and an orifice. The placement of a check valve between the main water and the fire-water connections, and the normally closed isolation valve at the fire-water connection, effectively isolate ruptures in one water supply from the other. However, both water supplies are eventually fed by the main service water headers.

Since the service water system connection to the diesel generators is not normally at operational status, the manual- and motor-operated valves could be left in the wrong positions after maintenance or test. Each diesel generator is tested monthly, and the successful operation of the service water system is a part of that test. Nevertheless, misalignment of the system is still a possible failure, if not corrected by the operator. Maintenance of the components themselves is not of concern because it is assumed to take place simultaneously with diesel maintenance.

The diesel generators will trip during test for failure of the service water to provide adequate cooling. This trip is overridden for emergency conditions, when the diesel generators will operate initially with service water system failure. For this reason, loss of service water to the diesel generators is annunciated on the control room board. There are also local indicators, including flow orifices in the diesel generator building rooms.

Identification of the loss of service water problem is based on the control-room-annunciated overtemperature indicators; consequently, human error failure probabilities are dependent on the status of each diesel generator's indicator. Because the diesel generators can run without initial service water cooling, there exists a time dependence on the mission of this function. We conservatively assumed that the diesel generators could be run for one-half hour before failure was likely to occur. Therefore, human action to correctly identify, analyze, and repair or realign the system must take place within one-half hour.

The failure modes of the diesel generator cooling are all those of the main service water headers, plus those specific to the system described in this subsection. Those failures would include no single-failure events. However, there would be single failures of the individual cooling arrays caused by rupture of the valves and heat exchangers or failure of the valves to remain open. Rupture of check valves is particularly important because it requires operator-isolation of the failed cooling array. There are no double failures in the whole system; doubles for individual cooling arrays result only from the aforementioned check valve ruptures and operator failure to isolate. However, there are a number of triple events leading to whole-system failure. One type is failure in each diesel-cooling array. The other type is failure of each of these cooling-water supply connections: Unit 1 main service water, Unit 2 main service water, and the fire-water system. Numerous permutations of triple-event failures can be found; however, all have the characteristics of one or the other of the two types just described. Higher order cut sets have not been found and are not considered crucial to the analysis of this particular function of the service water system.

D.4.2.3 Cooling Function of the Containment Fan Coolers

After the diesel generator piping, the next piping interface with the main service water headers is the piping to the containment fan-cooling system (CFCS)(Fig. D.9). Each fan assembly requires cooling of both its heat exchangers and its electric motor. The topological arrangement of the system is similar to the diesel cooling function. A loop fed by both main service water headers delivers water to the cooling array for each fan. In this arrangement, parts of the cooling arrays of Fans 1A and 1B, and Fans 1D and 1E, are interconnected. Consequently, failures can result in simultaneous failure of two fans (three out of five fans are required for CFCS success). The Unit 2 main service water header is normally aligned to Fans 1C, 1D, 1E, and the Unit 1 main service water header. Electric motor-operated valves give the operator the capability to adjust this alignment, depending on the availability of each service water supply header. In addition, the heat exchangers and water coolers in each fan cooling array are isolated by manual isolation valves. If required for containment isolation because of system leaks or other effects, electric motor-operated valves are located outside of the containment on the discharge lines. Therefore, with one exception, only

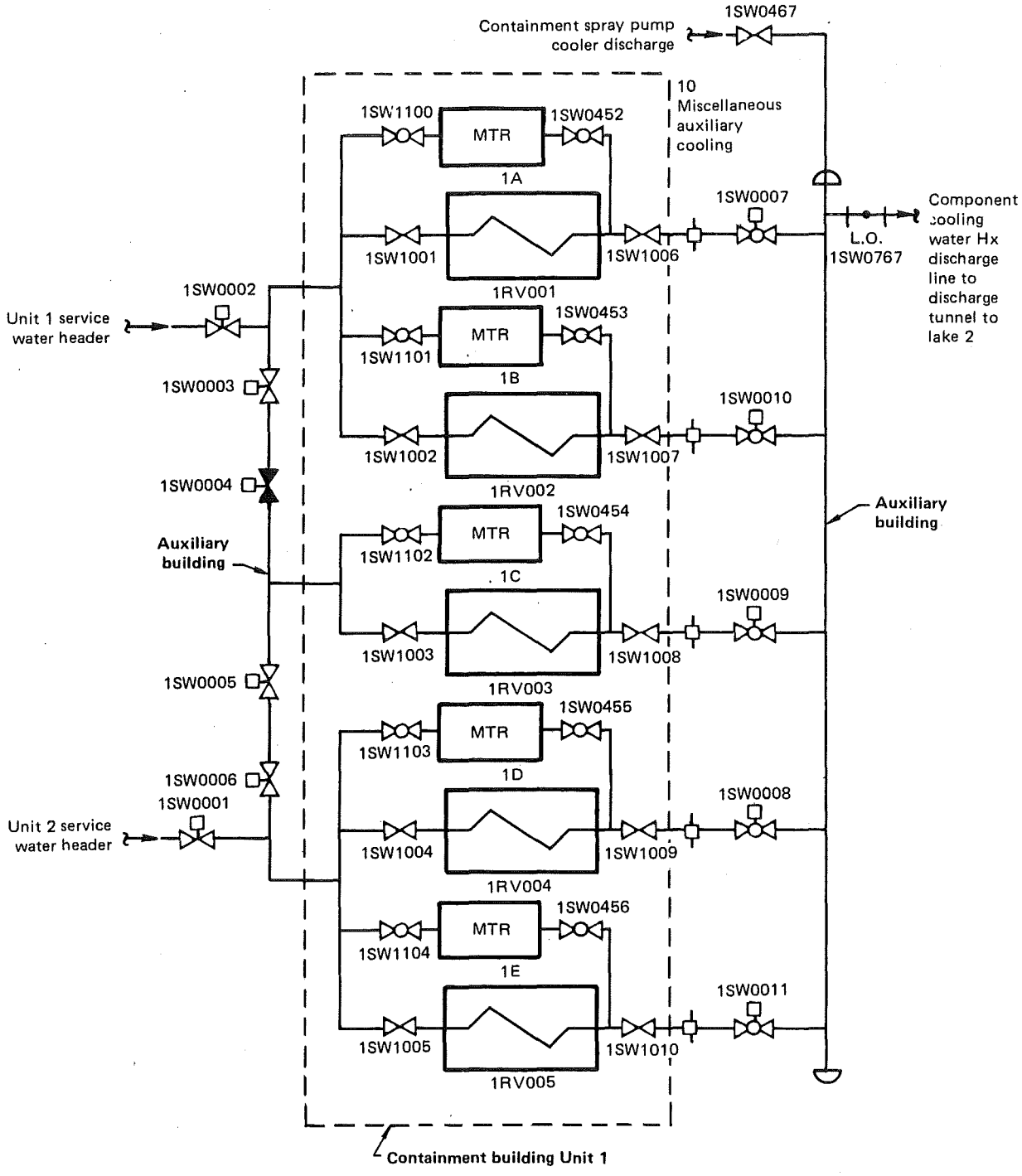


Figure D.9. Containment fan coolers portion of the SWS.

passive failures can result in system failure or individual fan failures. The exception is a failure of the main service water header. Maintenance-related failures are assumed to be part of the CFCS analysis. The passive nature of failures in this system make it a rather uninteresting system. Human interface is limited to response to passive failures through realignment or isolation of the system. This information is dependent on indicators for the fan coolers. The CFCS is desirable immediately upon initiation of the accident. Given the nature of dominant system failure modes, it is likely to have little impact on the final fault tree effort. We assume that because the fans dissipate heat continuously, CFCS failure due to service water failure would be identified promptly and corrected from the control room. Since the fans are located inside the containment, local intervention would be impossible.

The failure modes of the entire CFCS cooling function are primarily doubles--the failure of redundant supply systems and the passive failures of three of the five fan cooling units. Additional passive failures will result in the loss of one or more fan cooling units. The permutations of all the above mentioned failures will result in many doubles and triples for the CFCS as a whole, and many singles for each fan cooling unit.

D.4.2.4 Auxiliary Feedwater System Pump Cooling

Each of the three auxiliary feedwater pumps require service water-system cooling. These are the next piping interfaces encountered along the main service water header (Fig. D.10). Both units again have connections to the pump cooling arrays. Each electrical AFWS pump (1B, 1C) requires the operation of only pump room coolers. The turbine-driven pump requires a pump room cooler, and it also requires cooling to the turbine itself and the turbine governor. Solenoid-operated valves open to permit flow to the coolers. Manual isolation valves are also available for isolating the coolers and the water supplies from the main service water header. The solenoid-operated valves receive signals to open from the pump controller mechanism.

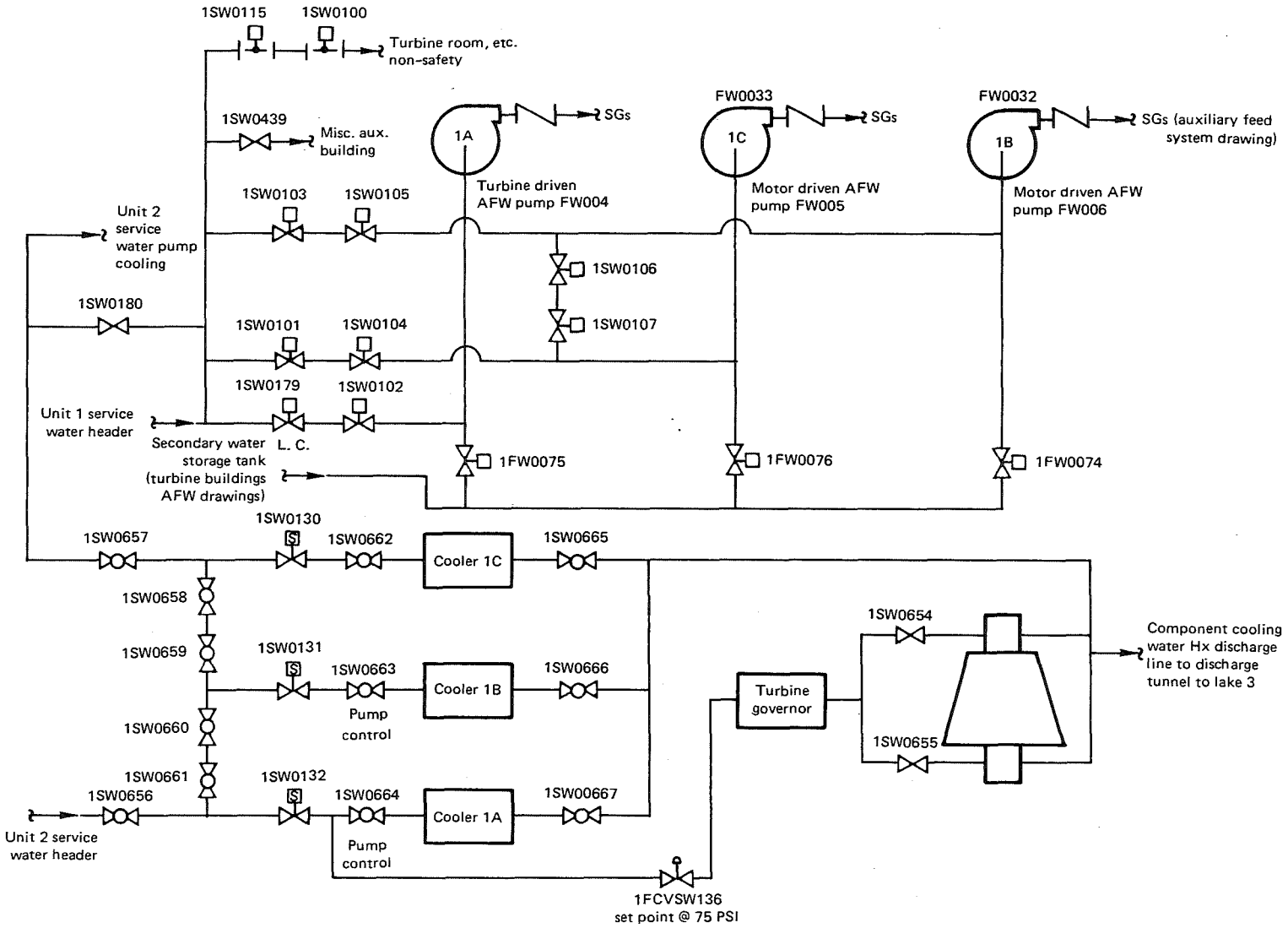


Figure D.10. Auxiliary feedwater supply and cooling portion of the SWS.

Because the system is not normally in operation, some valves could be in the wrong positions. These can be corrected by the operator. Manual override is also available for the solenoid-operated valves. As defined in the AFWS analysis, the auxiliary feedwater system must be activated within 1 to 1-1/2 hours. This will allow sufficient time for an operator to locate the pumps and correctly align a workable cooling-water-valving configuration. The pump temperature indicator would be the main instrumentation interface for the control room operator.

The failure modes for the AFWS pump cooling function will revolve around doubles--resulting in both main service water headers failing to deliver water--and in triples, which are associated with simultaneous single failures of each individual pump cooling function.

D.4.2.5 Cooling of the Component Cooling-Water System (CCWS)

The CCWS has three heat exchangers, any two of which are required as a heat sink for that system and the ultimate heat sink for the rest of the equipment cooling functions. These heat exchangers are located near the end of the main service water headers. A set of motor-operated isolation valves enable the operator to align either main service water header to each CCWS heat exchanger from the control room. Manual isolation valves are also found in the system. Operator intervention is minimal, and automatic control is nonexistent, with the result that all system failures are related to passive failures, with the exception of the active failures associated with each main header. Since equipment cooling is the desired, long-term function, immediate success of the system is not required. Requirements similar to those of the diesel generators were assumed. The failure modes of this system are relatively simple: two active failures resulting in each main header failing, and two passive failures or one passive failure and one operator-failure to isolate.

SECTION D.5: ELECTRICAL POWER

In this section, we consider the response of electric power to a seismically initiated nuclear power plant accident. The event tree analysis, discussed previously, did not identify electric power (EP) as a specific system on the event trees. However, nearly every system that would be considered an accident-mitigating system requires electric power.

D.5.1 EP SYSTEM DESCRIPTION

Unit 1 of the Zion plant has three major electrical divisions--17, 18, and 19. The system design satisfies the single-failure criteria in that any one of the three divisions, including its control power, can be lost and the system will still have enough safety features operating to safely control the plant in any operational mode.

A division consists of a 4160 VAC engineered safety feature bus, a 480 V engineered safety feature bus, a 480 VAC motor control center, a 120 VAC instrumentation bus, and a 125 VDC control bus. Each division can be fed from a 4160 VAC bus supplied by the system auxiliary transformer. In Unit 1, Divisions 18 and 19 have a diesel generator dedicated to supplying them power in the event of offsite power loss. Division 17 has a swing diesel attached to it. The swing diesel can feed either Division 17 for Unit 1 or the equivalent division for Unit 2--it swings to the division first requiring power. Single-line diagrams for the three divisions are shown on Figs. D.11 through D.13. These diagrams show the interrelationships of the buses and motor control centers (MCC) within a division.

D.5.2 EP FAULT TREE MODEL

A fault tree model was developed for Divisions 17, 18, and 19. The tree top for the three divisions is "Insufficient power on the 120 VAC bus" unique to the division. These three fault tree models conclude with failure of the appropriate diesel. These fault trees are actually contained within the division trees, at least for the MCCs that are tied directly to the inverters.

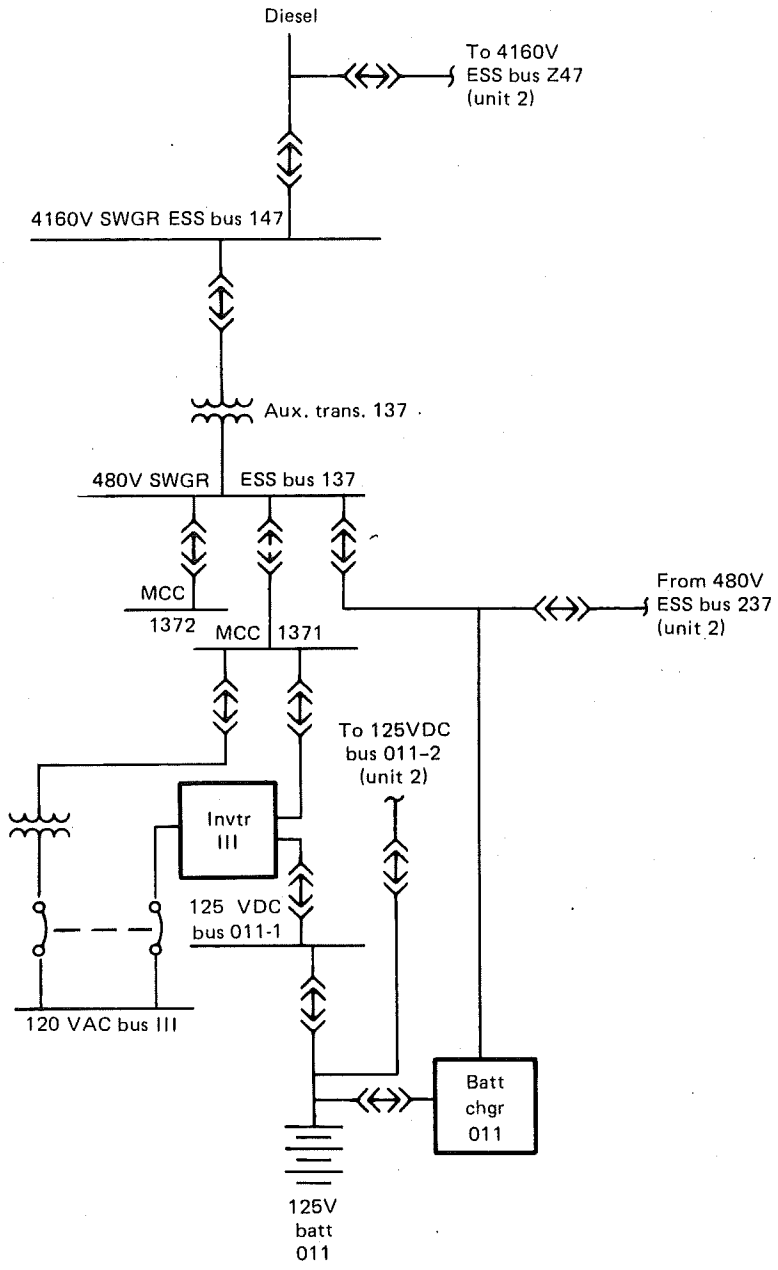


Figure D.11. Electrical power - Division 17.

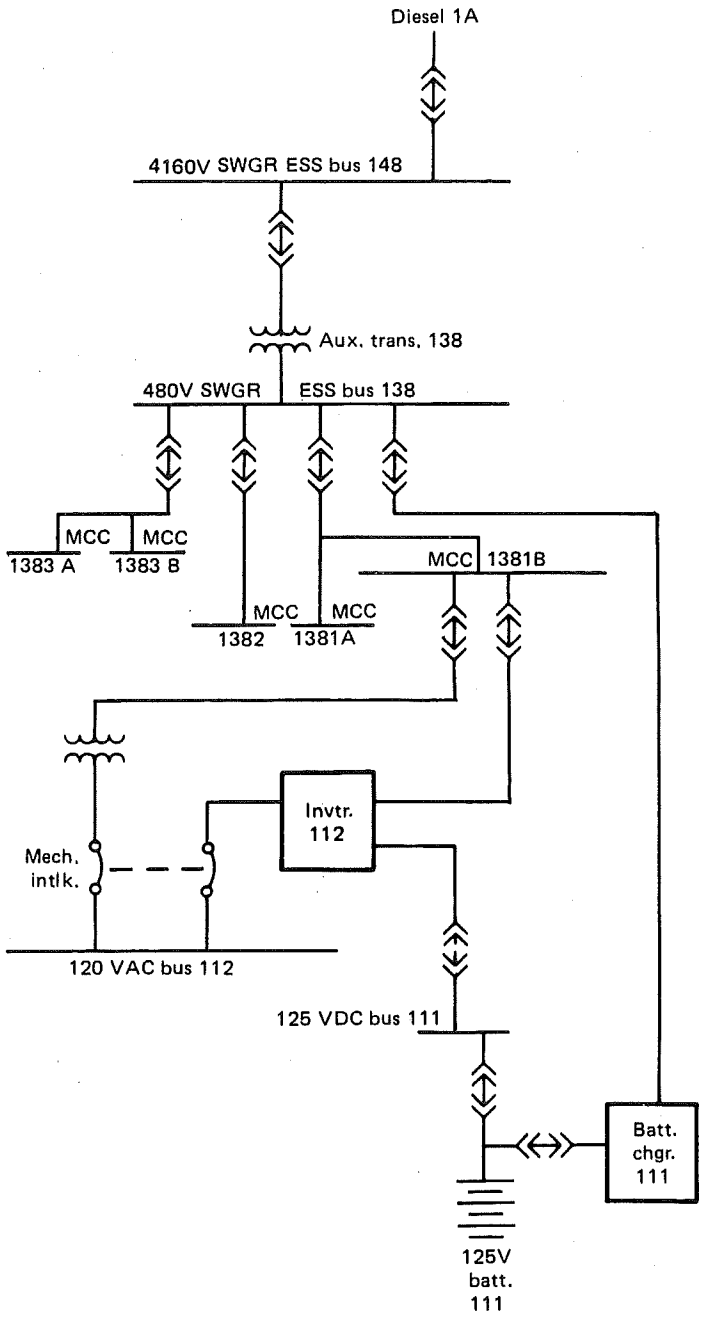


Figure D.12. Electrical power - Division 18.

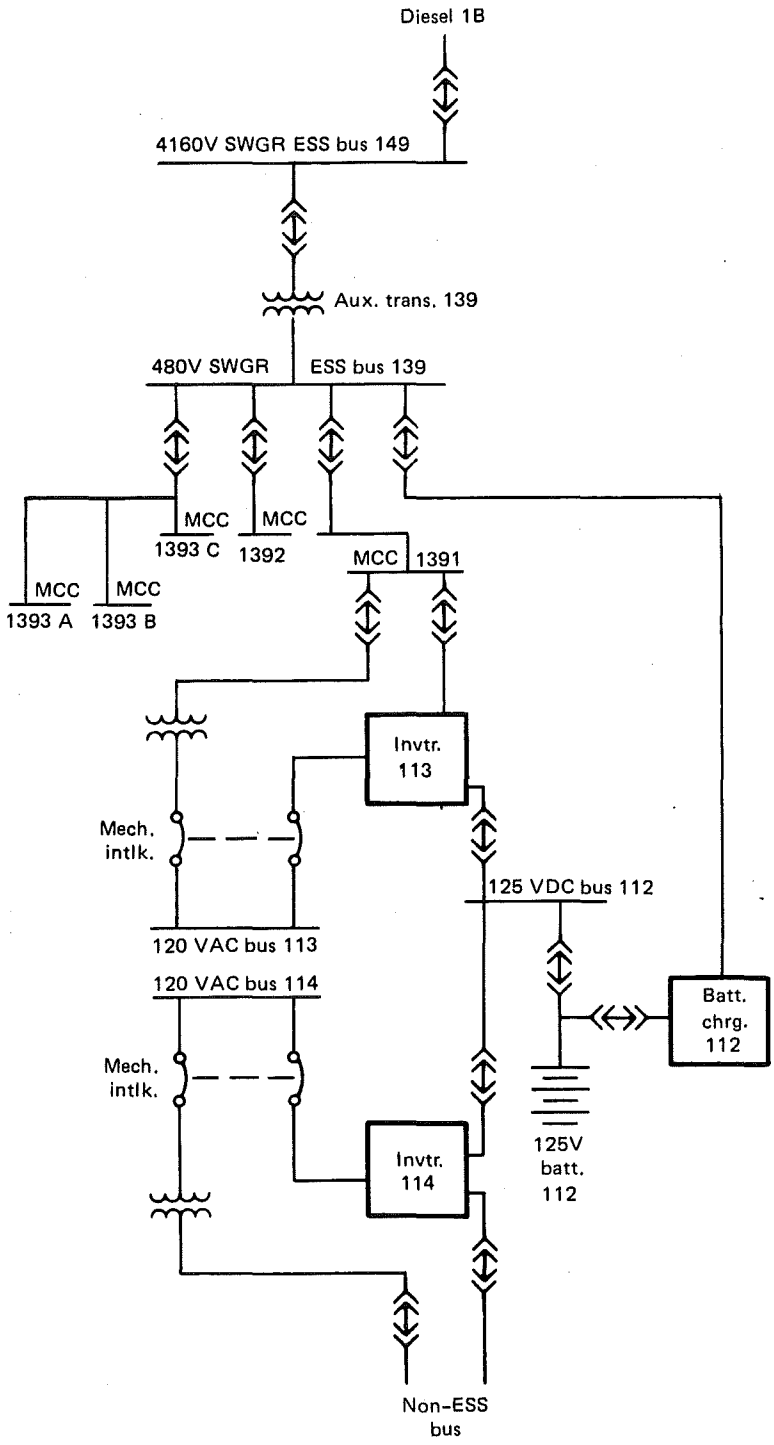


Figure D.13. Electrical power - Division 19.

The undesired event for the top fault trees of the emergency power system is "insufficient power." This term means any state of the emergency power system that inhibits adequate engineered safety feature system operability subsequent to a seismic event. The undesired event for the MCCs is also designated "insufficient power." For the MCC fault trees, insufficient power means any failure that prevents the affected MCC or bus from distributing power to its engineered safety feature loads.

It is assumed in this analysis that all emergency buses are available immediately prior to the seismic event. This assumption is based on the technical specifications, which require that the reactor be shut down if an emergency bus is not available. No credit is given for any operator action which may compensate for a failure.

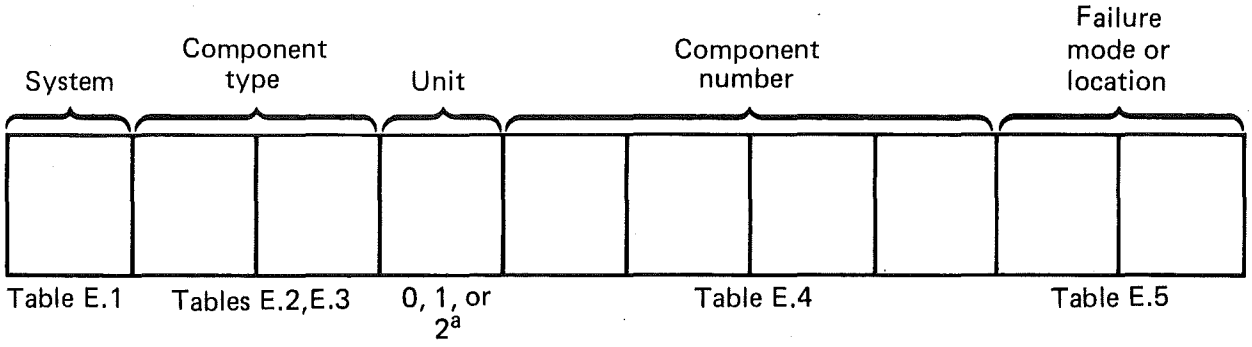
APPENDIX E

BASIC EVENT CODE

ILLUSTRATIONS

TABLES

This Appendix contains figures and tables which describe the ten-digit basic event code (Fig. E.1) used to identify basic events in all the fault trees and accident sequences. There are a few basic event names that do not fit the code.



[a]Taken directly from P&IDs. First character of Zion codes indicate Unit 1 (1), Unit 2 (2), or shared (0).

Figure E.1. Ten-digit basic event naming scheme.

Table E.1. Basic event system codes.[a]

Code 1st character	System name	Zion codes (for ref.)	
A	Auxiliary building equipment		AD
B	Auxiliary power - electrical		AP
C	Area radiation monitoring		AR
D	Auxiliary steam		AX
E	Component cooling		CC
F	Condensate and condensate booster		CD
G	Containment spray		CS
H	Battery and distribution		DC
I	Diesel generator		DG
J	Diesel fuel oil		DO
K	Reactor coolant system		DT
L	Fire protection and screen wash		FP
M	Steam generator feedwater (inc. aux. feed)	(HM,HDC,FS)	FW
N	Instrument air		IA
O	Instrumentation power - electrical		IP
P	Essential lighting		LS
Q	Main steam	(HR,DD)	MS
R	Main power - electrical		MP
S	Neutron monitoring		NR
T	N_2 system		NT
U	Process rad monitoring		PR
V	Primary water		PW
W	Pressurizer and miscellaneous piping in reactor building		PM
X	Reactor coolant	(SS)	RC
Y	Reactor building equipment		RD
Z	Residual heat removal system		RH

Table E.1. (Continued)

Code 1st character	System name	Zion codes (for ref.)
1	Reactor protection	(RM,CR,CB,AN) RP
2	Reactor containment ventilation	RV
3	Other HVAC	AV,CV,OV,PV,SV,TV
4	Service air	SA
5	Condensate storage	SC
6	Safety injection	SI
7	Service water	SW
8	Chemical and volume control	VC
9	Other	
0	Not applicable	

[a]Zion Codes without parentheses indicate direct correspondence between system codes. Codes with parentheses indicate systems which should be combined into the indicated system.

Table E.2. Basic event component-type codes: major groupings.

Code 2nd, 3rd characters	Description
AC	Accumulators
AD	Air dryers
AN	Annunciator modules
BA	Batteries
BC	Battery chargers
BL	Blowers
C-[a]	Circuit closers/interrupters
CR	Control rods
CV	Control rod drive mechanisms
DE	Demineralizers
EC	Electrical conductors (includes buses)
EH	Electrical heaters
EN	Engines, internal combustion
FE	Fuel elements
FI	Filters
G-[a]	Generators
H-[a]	Heat exchangers
I-[a]	Instrumentation and controls
MF	Mechanical function units (includes governors, gear boxes, etc.)
M-[a]	Motors
N-[a]	Penetrations, primary containment
O-[a]	Pipes, fittings
P-[a]	Pumps
RR	Recombiners
R-[a]	Relays
S-[a]	Shock suppressors and supports

Table E.2. (Continued)

Code 2nd, 3rd characters	Description
TA	Tanks (unpressurized)
TR	Transformers
TU	Turbines
V-[a]	Valves
W-[a]	Valve operators
XX	Other
Y-[a]	Vessels, pressure
ZZ	No applicable component

[a]These codes are broken down further in Table E.3.

Table E.3. Basic event component-type codes: subgroupings.

Code 2nd, 3rd characters	Description
C-	Circuit closers/interrupters
CA	Circuit breaker
CB	Contactor
CC	Controller
CD	Starter
CE	Switch (other than sensor)
CF	Switchgear
CX	Other
G-	Generators
GA	Alternator
GB	Converter
GC	Dynamotor
GD	Generator
GE	Amplidyne
GF	Inverter
GX	Other
H-	Heat exchangers
HA	Steam generator
HB	Steam generator tubes
HC	HVAC heat removal equipment
HD	Low pressure heater
HE	Gland condenser
HF	Cooler
HX	Other

Table E.3. (Continued)

Code 2nd, 3rd characters	Description
I-	Instrumentation and controls
IC	Controller
ID	Sensor/detector/element - pressure
IE	Sensor/detector/element - temperature
IF	Sensor/detector/element - flow
IG	Sensor/detector/element - level
IH	Sensor/detector/element - radiation
II	Indicator
IQ	Integrator (totalizer)
IP	Power supply
IR	Recorder
IT	Transmitter
IU	Computation module
IX	Other
M-	Motors
MA	AC
MD	DC
MX	Other
N-	Penetrations, primary containment
NA	Personnel access
NB	Fuel handling
NC	Equipment access
ND	Electrical
NE	Instrument line
NF	Process piping
NX	Other

Table E.3. (Continued)

Code 2nd, 3rd characters	Description
O-	Pipes, fitting
OA	<1"
OB	≥1", <2"
OC	≥2", <3"
OD	≥3", <4"
OE	≥4", <6"
OF	≥6", <8"
OG	≥8", <10"
OH	≥10", <12"
OI	≥12", <16"
OJ	≥16", <24"
OK	≥24", <36"
OL	≥36"
OM	Orifice
OO	Strainer
OX	Other
P-	Pumps
PA	Axial
PB	Centrifugal
PC	Diaphragm
PD	Gear
PE	Reciprocating
PF	Radial
PG	Rotary
PH	Vane type
PJ	Electromagnetic
PK	Jet
PL	Positive displacement
PX	Other

Table E.3. (Continued)

Code 2nd, 3rd characters	Description
R-	Relays
RA	Control, general purpose
RB	Control, sealed
RC	Miniature
RD	Switchgear, protective
RE	Switchgear, protective, slow acting
RF	Switchgear, auxiliary
RG	Mercury wetted
RH	Time delay, pneumatic
RJ	Time delay, solid state
RK	Reed
RL	Telephone
RM	Event sequencer, timer, or time-sequence controller
RS	Solid state (SCRs)
RX	Other
S-	Shock suppressors and supports
SA	Hangers
SB	Supports
SC	Spring loaded sway brace/stabilizers
SD	Snubbers
SX	Other

Table E.3. (Continued)

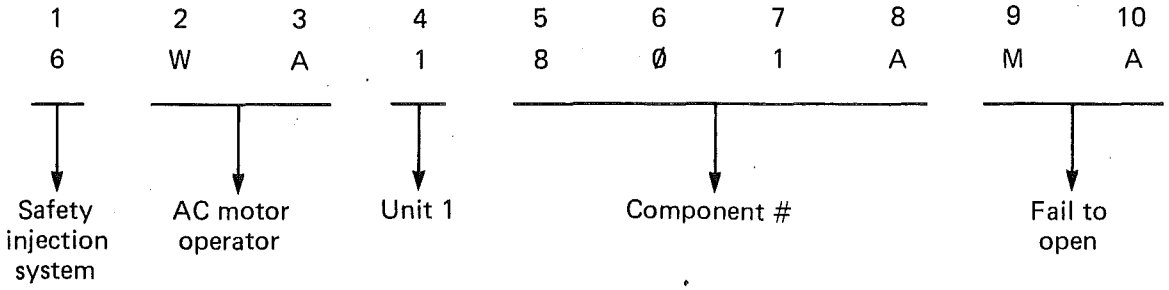
Code 2nd, 3rd characters	Description
V-	Valves
VA	1-way flow (check)
VB	Pressure relief (power operated)
VC	Vacuum relief
VD	Shutoff, isolation, stop
VE	3-way
VF	4-way
VG	Flow control
VH	Pressure control
VJ	Level control
VL	Vent
VN	Sample
VP	Drain
VQ	Bypass
VX	Other
VY	Safety relief-valve
W-	Valve operators
WA	Electric motor - AC
WB	Electric motor - DC
WC	Hydraulic
WD	Pneumatic, diaphragm, cylinder
WE	Solenoid - AC
WF	Solenoid - DC
WG	Float
WH	Explosive, squib
WJ	Mechanical (differential pressure to open, spring-force to close)
WK	Manual only
WX	Other

Table E.3. (Continued)

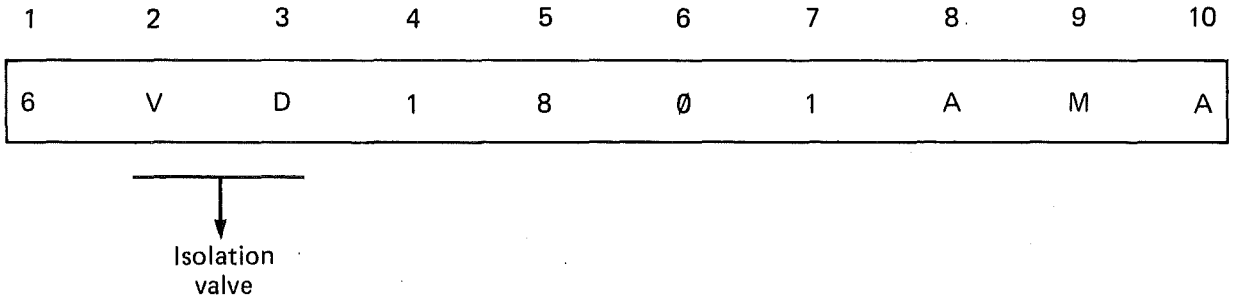
Code 2nd, 3rd characters	Description
Y-	Vessels, pressure
YA	Reactor vessel
YB	Pressurizer vessel
YD	Containment/drywell
YE	Pressure suppression
YX	Other

Table E.4. Component numbers: representative examples.[a]

1. Valve 1MOVI88O1A fails to open on signal – failure of valve operator



2. Same valve – fails to open on signal – stem binding (failure of valve itself)



[a]There is only one difference between Example 1 and Example 2: in Example 1 the valve operator failed, while in Example 2, the valve itself failed.

Table E.5. Failure mode or location (9th and 10th characters).

Random component failures

MA	Fails to open/de-energize/disengage
MB	Fails to close/energize/engage
MC	Open/de-energized/disengaged
MD	Closed/energized/engaged/fails to remain open
ME	Fail to start
MF	Fail to stop
MG	Fail to run/operate (instrumentation)
MH	Set-point drift (too high)
MI	Set-point drift (too low)
MJ	Short circuit/leak/rupture
MK	Open circuit/blockage/implode
ML	Overload (overpressure/overcurrent/overvoltage/etc.)
MM	Underload (underpressure/undercurrent/undervoltage/etc.)
MN	No signal/input
MO	Erroneous signal/input
MP	Lack of availability
MQ	Support failure

Operator/maintenance related component failures

OA	Operator fails to open/de-energize/disengage
OB	Operator fails to close/energize/engage
OC	Inadvertently opened/de-energized/disengaged by operator
OD	Inadvertently closed/energized/engaged by operator
OE	Operator fails to start
OF	Operator fails to stop
OG	Operator fails to leave running
OH	Calibration error (set too high)
OI	Calibration error (set too low)
OJ	Maintenance error leads to short circuit/leak/rupture
OK	Maintenance error leads to open circuit/blockage/implosion

Table E.5. (Continued)

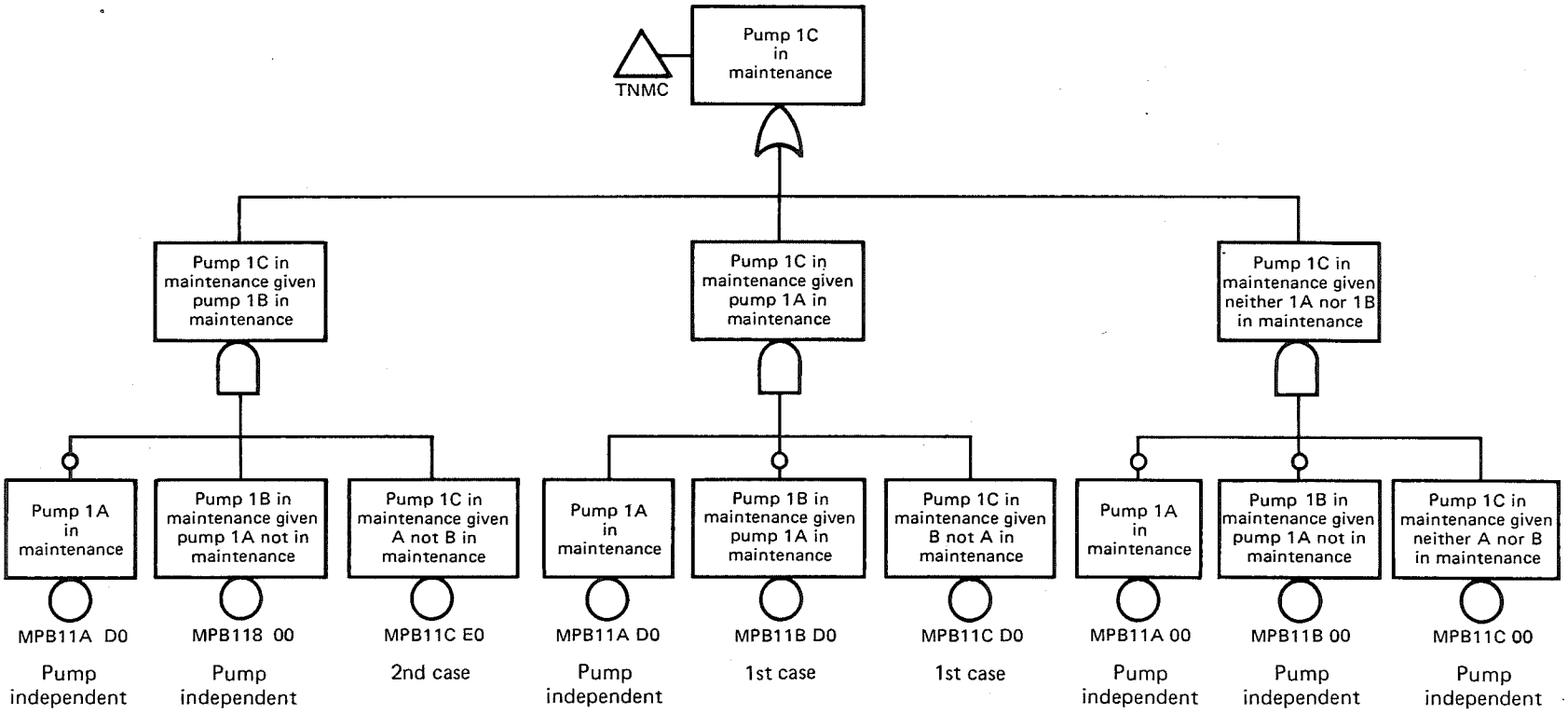
Operator/maintenance related component failures (cont'd)

OL	Left open/de-energized/disengaged[a]
OM	Left closed/energized/engaged[a]
ON	Out of service - test
OO	Out of service - maintenance
OP	Same as OA except instrumentation not fully operational
OQ	Same as OB except instrumentation not fully operational
OR	Same as OE except instrumentation not fully operational
OS	Same as OF except instrumentation not fully operational
OT	Same as OG except instrumentation not fully operational
OW	Same as OA except this concerns a locked component
OX	Same as OP except this concerns a locked component

Dependent Events Involving Component Failures[b]

D	1st order dependent event
E	2nd order dependent event
F	3rd order dependent event
G	4th order dependent event
etc.	Nth order dependent event

[a]Applies if erroneously left in this position after test/maintenance.
[b]See diagram in Fig. E.2.



00 1 pump in maintenance (independent)

D0 1 pump in maintenance (dependent on another in maintenance, 1st case)

E0 1 pump in maintenance (dependent on another in maintenance, 2nd case)

Figure E.2. Dependent events sample.

APPENDIX F

SUPPORTING SYSTEMS ANALYSIS STUDIES

CONTENTS

ILLUSTRATIONS

SECTION F.1: INTRODUCTION TO SEISMIC SAFETY MARGINS RESEARCH PROGRAM (SSMRP) SYSTEMS ANALYSIS STUDIES

The supporting studies described below develop SEISIM theory, investigate alternatives to SEISIM, and develop refinements that may be incorporated in SEISIM in Phase II.

The first supporting study lays the theoretical foundations for SEISIM, derives the fragility function estimator used to process subjective percentiles, and refines simulation alternatives to SEISIM. ("Probability Computation Methods," unpublished draft report, George, 1981).

The second study discusses alternative sensitivity analyses. ("Sensitivity Techniques," unpublished draft report, George, 1982). It defines the importance measures programmed in SEISIM and the derivative sensitivity measures planned for SEISIM in Phase II.

The third study (Moeini, et al., 1980) examines Licensee Event Reports (LERs) and design errors. Two types of component design errors are hypothesized. The first kind of error is discovered by design review and analysis, the second by test. The ratio of the frequencies of the two kinds of errors is estimated.

The fourth study (Wolff, 1981) applies three variance reduction methods to simulation of multiple component failure probabilities. The methods are stratified sampling, conditional Monte Carlo, and principal component analysis. The use of these methods reduces variance by an order of magnitude. The computer program MULTI written to demonstrate the methods is used to validate SEISIM.

SECTION F.2: PROBABILITY COMPUTATION METHODS

The first study, which deals with probability computation methods, derives the SSMRP reliability computation method, the probability methods for processing fragility inputs, and ways to make computations efficient. The study also describes simulation errors that will make the reliability computation incorrect or inefficient, and then describes the correct methods.

Multivariate interference analysis is the SSMRP reliability computation method. This method represents dependence among component responses and strengths (George and Wells, 1981). Multivariate interference analysis has never been applied to mechanical system reliability analysis until now. Van Marcke (1973) and Rackwitz and Kryzkacz (1978) independently applied the same analysis to components which can fail in several, dependent modes. George (1978) used this method in computing electrical loss of load probability.

Fragility functions (the distribution functions of strengths at failure) are estimated for the reliability computation. The sample is a set of subjective percentiles, not a random sample. Therefore, new estimation methods are required. Two methods are proposed: maximum uncertainty and least squares. The latter is used in SSMRP.

The omission of inherent randomness in the simulation of uncertainty causes an error called dissimulation. We describe two methods for simulating inherent randomness and uncertainty due to lack of knowledge: the expected value method and a bounding method.

The study proposes marginal analysis for allocating run time and numbers of runs among subroutines of simulation programs, describes simulation variance reducing methods, and gives a test for verifying variance reduction.

SECTION F.3: SENSITIVITY ANALYSES

Two problems of sensitivity analysis are addressed. The first is finding the sensitivity of outputs to changes in significant input parameters. These output sensitivities are computed by SEISIM as slopes of chords or derivatives. The second problem is finding important components. Dominance analysis helps in dealing with this problem. Dominance analysis is another type of sensitivity computation performed by SEISIM. The objective is to find the components, accident sequences, etc., that most influence the probability of radioactive release. This tool is particularly useful in focusing the model and making sure that insignificant elements are eliminated.

F.3.1 DEFINITION OF SENSITIVITY ANALYSES

Sensitivity analyses tell how probability outputs from SEISIM change as inputs change. Typical inputs are primary input variables and parameters of cdf's. Typical outputs are event probabilities.

Sensitivity analyses can be local, global, or intermediate. Local sensitivity analyses illustrate the effect on outputs of small changes in inputs. In Fig. F.1 the derivative measures the change in z as x and y change in the neighborhood of nominal values x_o and y_o. Derivatives are local sensitivity measures of outputs that are continuous functions of inputs. Global sensitivity analyses tell the extremes of the outputs and the inputs for which they occur. In Fig. F.2 the global sensitivity tells the largest value of z, which is designated z*. The value z* occurs when the inputs x* and y* (as shown in Fig. F.2) are used as inputs. Response surface analysis, bounds, and model optimization help establish extremes. In Fig. F.3 the slope of a chord tells the effect on z of changing from (x_o, y_o) to (x_1, y_1). Intermediate sensitivity analyses tell the amount of output change for discrete changes in inputs. Intermediate sensitivity analyses can be done by rerunning SEISIM with different inputs. Slopes of chords measure intermediate sensitivities.

There are three classes of sensitivity analyses, each with a different use. Analyses of local sensitivity measures help indicate where money and effort should be spent to change inputs, assuming the nominal inputs are true and that only small changes in inputs are contemplated. Global sensitivity analyses establish the worst output that could occur within the domain of

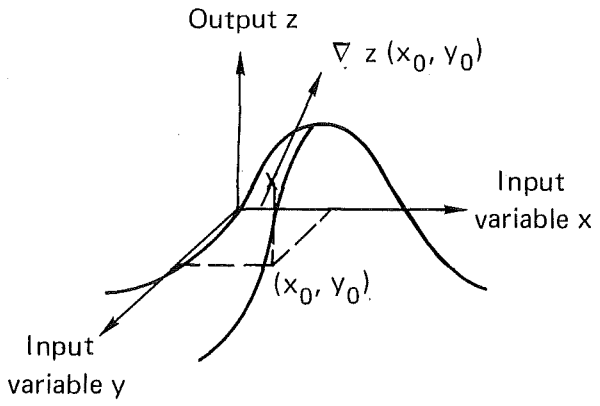


Figure F.1. Sensitivity measure using derivatives.

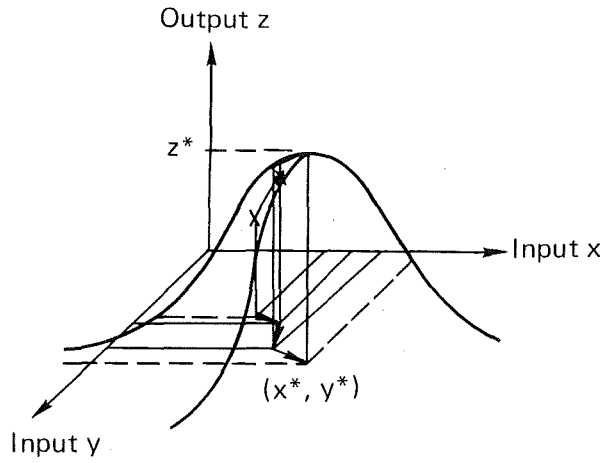


Figure F.2. Global sensitivity measure.

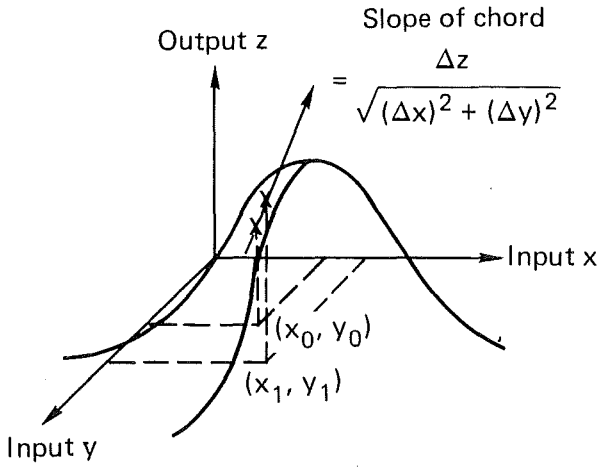


Figure F.3. Sensitivity measure using slope of a chord.

feasible inputs. Intermediate sensitivity analyses are "what if" analyses: What if the true input was not what we put in? How much would output change? These analyses are worthwhile if money and effort could change inputs more than a small amount, or if there are alternative credible inputs. For instance, it is of interest to see how much change there will be in probabilities when we remove the increment in fragility variance due to disagreements among experts. The change measures the sensitivity to modeling uncertainty.

F.3.2 PURPOSE OF SENSITIVITY ANALYSES

Sensitivity analyses in the Seismic Safety Margins Research Program (SSMRP) help satisfy these needs:

1. Establish credibility of the results (model),
2. Estimate the worst that could happen to a reactor in an earthquake, (global),
3. Identify systems, components, or parameters important to reactor safety (local or intermediate), and
4. Determine how to allocate resources to reduce uncertainty and failure probability in reactor safety (local or intermediate).

These needs determine the sensitivity analyses in SSMRP.

Modeling and local sensitivity analyses indicate how outputs change as inputs change. If the model and changes are plausible, credibility is improved. Global sensitivity analyses can estimate limits on probabilities of reactor accidents. If the model is accurate, the estimates are useful for establishing worst cases.

If we estimate the rate of change of output with respect to changes in input, and if we then estimate marginal costs of changing inputs, we can rationally recommend where to spend money to change output. This will help allocate resources to reduce uncertainty and to reduce the probability of radioactive release due to an earthquake.

F.3.3 ALLOCATION OF RESOURCES TO REDUCE UNCERTAINTY IN OUTPUT

One SSMRP objective is to allocate resources to reduce uncertainty in release probabilities. The method suggested here is called marginal analysis. It requires sensitivity analyses and estimates of the marginal change in inputs per unit of resource spent. By changing inputs, marginal analysis can allocate resources to reduce release probability.

The following information is required for marginal analysis:

1. The marginal rates of change of release probability per unit change of inputs (from sensitivity analyses),
2. Simultaneous confidence intervals on release probabilities,
3. Budget or resources to be allocated to reducing uncertainty in inputs (from NRC), and
4. Marginal rates of change in inputs per unit resource allocated to reducing uncertainty (subjective opinion).

An example follows which will illustrate how to allocate a budget of B dollars among components of a safety system. An estimate of the release probability, P_R, is a function of component failure probabilties $P(B_j)$, $j = 1, 2, \ldots, k$. The amount of money to be spent on component j is denoted X_j. The amount spent determines both an estimate $P(B_j)$ and the confidence interval on P_R.

The objective is to minimize the length of the confidence interval on P_R subject to the budget constraint.

$$\sum_{j=1}^{k} X_j < B \quad .$$

The following example illustrates a solution to the resource allocation problem. For a large sample of size N, a confidence interval on P_R is

$$\hat{P}_R \pm \sqrt{\hat{P}_R (1 - \hat{P}_R)/n} \; z_{\alpha/2}$$

where $z_{\alpha/2}$ is a value of the standard normal random variable and $\hat{P}_R$ is an estimate of P_R based on a sample of size n. The objective function is

$$\min_{X_1,\ldots,X_k} \; 2\sqrt{\hat{P}_R (1 - \hat{P}_R)/n} \; z_{\alpha/2} \quad .$$

Form the Lagrangian

$$L = 2\sqrt{\hat{P}_R\,(1 - \hat{P}_R)/n}\; z_{\alpha/2} - \lambda\,(\sum_{j=1}^{k} X_j - B) \quad .$$

Use calculus to minimize L with respect to X_j. The condition

$$\frac{\delta L}{\delta X_j} = 0$$

for all j is necessary for an optimal allocation. This is equivalent to

$$\frac{\delta \sqrt{2\ \hat{P}_R\,(1 - \hat{P}_R)/n}\; z_{\alpha/2}}{\delta\, X_j} = +\ \lambda$$

for all j.

The interpretation of this condition is as follows. The derivative is the rate of change of the confidence interval width as money is spent on component j. Marginal analysis says spend dollars on component j until the rate of change of the confidence interval width per dollar is the same as the rate of change per dollar spent on all other components.

The connection between confidence interval width and component sensitivity is as follows. By the chain rule,

$$\frac{\delta\sqrt{\hat{P}_R\,(1 - \hat{P}_R)/n}}{\delta X_j} = \frac{\delta\sqrt{\hat{P}_R\,(1 - \hat{P}_R)/n}}{\delta P(B_j)} \qquad \frac{\delta P(B_j)}{\delta X_j} \quad .$$

The first term is the rate of change of the confidence interval width as the component failure probability changes. It comes from sensitivity analysis. The second term is based on subjective opinion about the marginal change in component failure probability per dollar spent.

The first term can be computed from the sensitivity of P_R to component failure probability as follows:

$$\frac{\delta}{\delta P(B_j)} \left[2\sqrt{\hat{P}_R\,(1 - \hat{P}_R)/n}\right] z_{\alpha/2}$$

$$= \frac{z_{\alpha/2}\sqrt{(1 - 2\hat{P}_R)/n}}{\hat{P}_R\,(1 - \hat{P}_R)/n} \cdot \frac{\delta\hat{P}_R}{\delta P(B_j)} \quad .$$

A subjective opinion about $\delta P(B_j)/\delta X_j$ can be obtained as follows. The component failure probability is

$$P(B_j) = P[\text{Response} > \text{Strength}] = 1 - \Phi\left(-\frac{\mu_R - \mu_S}{\sqrt{\sigma_R^2 + \sigma_S^2}}\right).$$

Suppose money can be spent to reduce either the variance of response σ_R^2 or the variance of strength σ_S^2, measures of uncertainty in response and strength. The money should be spent to get the most benefit for the dollar; that is, spend so that

$$\frac{\delta P(B_j)}{\delta X_j} = \max\left\{\frac{\delta P(B_j)}{\delta \sigma_R^2} \cdot \frac{\delta \sigma_R^2}{\delta X_j}, \frac{\delta P(B_j)}{\delta \sigma_S^2} \cdot \frac{\delta \sigma_S^2}{\delta X_j}\right\}.$$

Formulas for $\delta P(B_j)/\delta \sigma^2$ are in George and Wells, 1980. The decision maker must estimate $\delta \sigma^2/\delta X_j$. Because $\delta P(B_j)/\delta \sigma^2$ is negative, the minimum of absolute values of the two products should be chosen. The marginal change in probability, $\delta P(B_j)/\delta \sigma_R^2$, results from better stress analysis. The marginal change, $\delta P(B_j)/\delta \sigma_S^2$, comes from fragility test data.

F.3.4 SENSITIVITY ANALYSES TECHNIQUES

Several aids to sensitivity analyses are already in SEISIM. Subroutines DSEQ and DCAG rank components. Subroutine DPRI (incomplete) ranks primary input variables. Subroutine DERIV computes slopes of chords and derivatives. Some modeling can be done within SEISIM by the multivariate linear regression program in DPRI and by the reruns required by subroutine DERIV. Some modeling can be done by applying regression to combined SEISIM outputs.

The modeling will be done in stages. The first stage eliminates input variables which do not significantly affect outputs. The second stage models output as a function of the remaining variables. The third stage computes the required sensitivity measures from the model. The last stage estimates confidence intervals on sensitivity measures. Stages will be repeated as new input variables are introduced or as different subsets of the input variable domain are explored. Different input variables may be included in Stage 2 in different subsets of the input variable domain.

The Stage 1 preliminary screening will be done by rank regression or multivariate linear regression. Rank regression is appropriate when output is monotonic in input and requires no other model assumptions. Multivariate linear regression will be modified to print residuals and partial correlations. The residuals and partial correlations indicate strength and the nature of relations. The nature of relations between output and input variables suggests transformations which yield linear relations. These transformations may fit output better with fewer variables than if multivariate linear regression was used without any transformations. Ridge regression may be used after screening and transformation to locate extrema.

Fractional factorial, Box-Hunter response surface, Latin hypercube, or min D designs will be used in the first two stages. Latin hypercube design is optimal for rank regression. Min D designs are robust and can handle the problem of choosing additional observations when some runs have already been made, as in the second stage.

SECTION F.4: DESIGN ERRORS AND THEIR EFFECTS ON FRAGILITY FUNCTIONS

Design errors could cause nuclear power plant components to have fragility functions different from those initially estimated. If we know the reduction of strength due to design error and the frequency of design error occurrence, we can modify our estimates of the fragility functions to obtain a less biased estimate of radioactive release probability.

The design error study (Moeini et al., 1980) provides some of the information necessary to modify fragility functions. Examination of Licensee Event Reports (LERs) and other reported design errors show that design errors have three effects on fragility functions, and these effects depend on the way in which the error is discovered. One method of discovery is by review and analysis. Errors discovered this way would shift the upper tail of the fragility function to the left. This increases the probability of component failure under high load. The other method of discovery is by test. This either shifts the whole fragility function to the left or shifts the lower tail to the left (Fig. F.4).

If we knew how much to shift the fragility functions and how frequently each type of error and effect occurred, we could modify fragility input by putting in a mixture of distributions for fragility functions; the nominal, error-free function; and the others. These relationships are shown in Fig. F.4. So far, the side study has developed an estimate of the proportions of only the two kinds of errors.

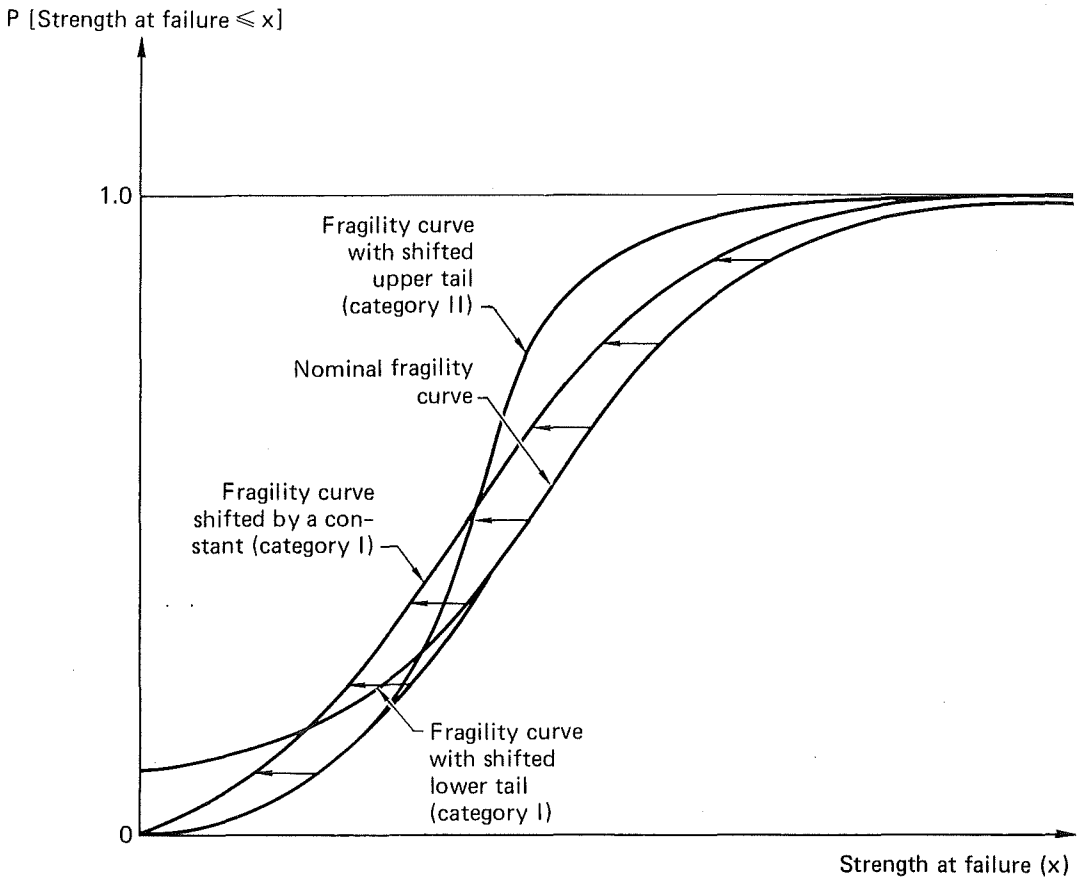


Figure F.4. Fragility function shifts.

SECTION F.5: VARIANCE REDUCTION METHODS FOR SIMULATION OF SYSTEM FAILURE PROBABILITY

System failure probability is a multivariate integral which can be evaluated by Monte Carlo simulation. The computer program MULTI (Wolff and Tanaka, 1981) simulates multivariate integrals as efficiently as possible. It helps validate SEISIM. It was developed for multivariate normal integrals but can be used to evaluate any multivariate integral of a probability density function. Program MULTI applies conditional Monte Carlo, stratified sampling (Haber, 1966-1969) and principal component analysis. It differs from previous work, Algorithm 440 CACM (Gallagher, 1971) which uses stratification but not principal component analysis and conditional Monte Carlo.

Principal component analysis is used first to transform the original response minus strength random variables into independent random variables, ordered according to variance. The independent variable with largest variance is the principal component. Stratified sampling is used to evaluate the probability of system failure conditional on a value of the principal component. Then the probability is unconditioned.

In our application, the objective is to estimate $P\left[X_1 \geq 0, \ldots, X_n \geq 0\right]$ where $(X_1, \ldots, X_n) \sim N(\underline{\mu}, \sum)$ by simulation. This is equivalent to simulating responses and strengths and then estimating failure probability as the proportion of simulations with all responses $\geq$ strengths. Figure F.5 illustrates how the simulation would be done without any variance reduction. Figure F.6 illustrates simulation with variance reduction. In order to generate values of normal random variables conditional on being in a specified stratum, the normal density was approximated by a parametric density (Abramson, 1976) from which conditional values are easily generated.

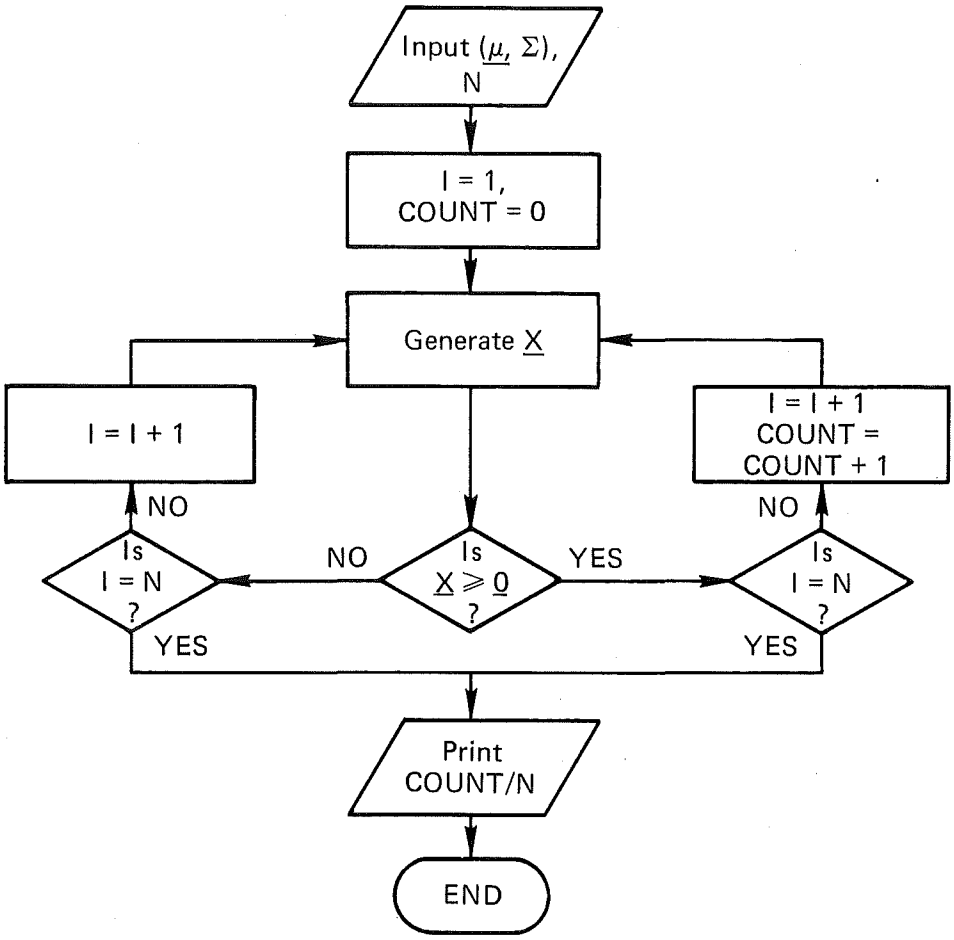


Figure F.5. Simulation of multivariate probability of failure without variance reduction.

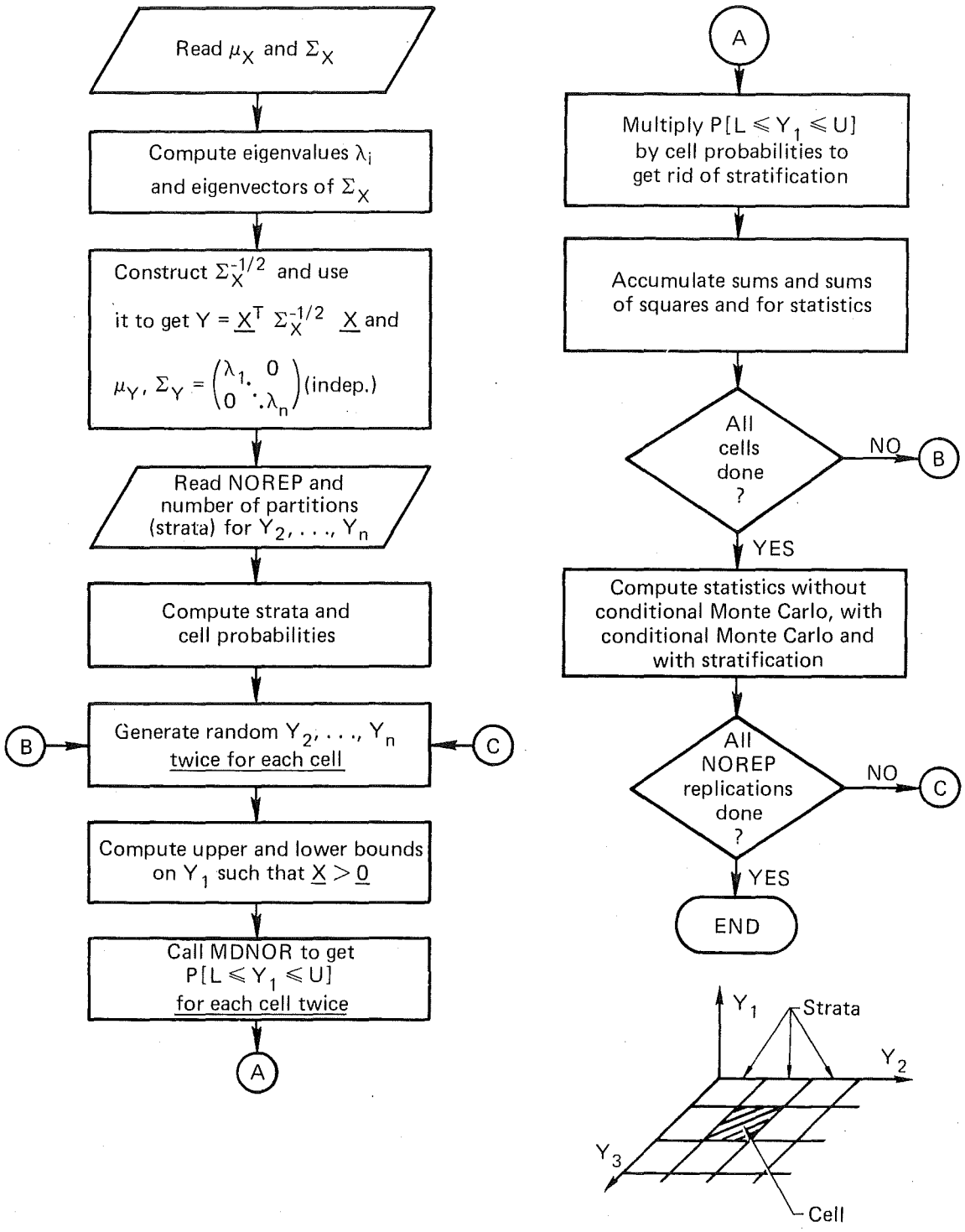


Figure F.6. Simulation of multivariate normal probability of failure with variance reduction.

REFERENCES

Please refer to the text references on pages 35 thru 38.

APPENDIX G

RELEASE CATEGORY DEFINITIONS

TABLE

This Appendix contains the release categories definitions as stated in the Reactor Safety Study (WASH 1400), Appendix VI. Table G.1 defines the fraction of core inventory released for each of the release categories defined.

RELEASE CATEGORY 1

This release category can be characterized by a core meltdown followed by a steam explosion on contact of molten fuel with the residual water in the reactor vessel. The containment spray and heat removal systems are also assumed to have failed and, therefore, the containment could be at a pressure above ambient at the time of the steam explosion. It is assumed that the steam explosion would rupture the upper portion of the reactor vessel and breach the containment barrier, with the result that a substantial amount of radioactivity might be released in a puff from the containment over a period of about 10 minutes. Due to the sweeping action of gases generated during containment-vessel meltthrough, the release of radioactive materials would continue at a relatively low rate thereafter. The total release would contain approximately 70% of the iodines and 40% of the alkali metals present in the core at the time of release. Because the containment would contain hot pressurized gases at the time of failure, a relatively high release rate of sensible energy from the containment could be associated with this category. This category also includes certain potential accident sequences that would involve the occurrence of core melting and a steam explosion after containment

Table G.1. Radionuclide release categories used in the Reactor Safety Study.

	Fraction of core inventory released							
Release category	Noble gases	Organic iodine	I	Cs	Te	Ba	Ru	La
1	0.9	6×10^{-3}	0.7	0.4	0.4	0.05	0.4	3×10^{-3}
2	0.9	7×10^{-3}	0.7	0.5	0.3	0.06	0.02	4×10^{-3}
3	0.8	6×10^{-3}	0.2	0.2	0.3	0.02	0.03	3×10^{-3}
4	0.6	2×10^{-3}	0.09	0.04	0.03	5×10^{-3}	3×10^{-3}	4×10^{-4}
5	0.3	2×10^{-3}	0.03	9×10^{-3}	5×10^{-3}	1×10^{-3}	6×10^{-4}	7×10^{-5}
6	0.3	2×10^{-3}	8×10^{-4}	8×10^{-4}	1×10^{-3}	9×10^{-5}	7×10^{-5}	1×10^{-5}
7	6×10^{-3}	2×10^{-5}	2×10^{-5}	1×10^{-5}	2×10^{-5}	1×10^{-6}	1×10^{-6}	2×10^{-7}

rupture due to overpressure. In these sequences, the rate of energy release would be lower, although still relatively high.

RELEASE CATEGORY 2

This category is associated with the failure of core-cooling systems and core melting concurrent with the failure of containment spray and heat-removal systems. Failure of the containment barrier would occur through overpressure, causing a substantial fraction of the containment atmosphere to be released in a puff over a period of about 30 minutes. Due to the sweeping action of gases generated during containment vessel meltthrough, the release of radioactive material would continue at a relatively low rate thereafter. The total release would contain approximately 70% of the iodines and 50% of the alkali metals present in the core at the time of release. As in Release Category 1, the high temperature and pressure within containment at the time of containment failure would result in a relatively high release rate of sensible energy from the containment.

RELEASE CATEGORY 3

This category involves an overpressure failure of the containment due to failure of containment heat removal. Containment failure would occur prior to the commencement of core melting. Core melting then would cause radioactive materials to be released through a ruptured containment barrier. Approximately 20% of the iodines and 20% of the alkali metals present in the core at the time of release would be released to the atmosphere. Most of the release would occur over a period of about 1.5 hours. The release of radioactive material from containment would be caused by the sweeping action of gases generated by the reaction of the molten fuel with concrete. Since these gases would be initially heated by contact with the melt, the rate of sensible energy release to the atmosphere would be moderately high.

RELEASE CATEGORY 4

This category involves failure of the core-cooling system and the containment spray injection system after a loss-of-coolant accident, together with a concurrent failure of the containment system to properly isolate. This

would result in the release of 9% of the iodines and 4% of the alkali metals present in the core at the time of release. Most of the release would occur continuously over a period of two to three hours. Because the containment recirculation spray and heat-removal systems would operate to remove heat from the containment atmosphere during core melting, a relatively low rate of release of sensible energy would be associated with this category.

RELEASE CATEGORY 5

This category involves failure of the core cooling systems and is similar to Release Category 4, except that the containment spray injection system would operate to further reduce the quantity of airborne radioactive material and to initially suppress containment temperature and pressure. The containment barrier would have a large leakage rate due to a concurrent failure of the containment system to properly isolate, and most of the radioactive material would be released continuously over a period of several hours. Approximately 3% of the iodines and 0.9% of the alkali metals present in the core would be released. Because of the operation of the containment heat-removal system, the energy release rate would be low.

RELEASE CATEGORY 6

This category involves a core meltdown due to failure in the core cooling systems. The containment sprays would not operate, but the containment barrier would retain its integrity until the molten core proceeded to melt through the concrete containment base mat. The radioactive materials would be released into the ground, with some leakage to the atmosphere occurring upward through the ground. Direct leakage to the atmosphere would also occur at a low rate prior to containment-vessel meltthrough. Most of the release would occur continuously over a period of about 10 hours. The release would include approximately 0.08% of the iodines and alkali metals present in the core at the time of release. Because leakage from containment to the atmosphere would be low and gases escaping through the ground would be cooled by contact with the soil, the energy release rate would be very low.

RELEASE CATEGORY 7

This category is similar to Release Category 6, except that containment sprays would operate to reduce the containment temperature and pressure as well as the amount of airborne radioactivity. The release would involve 0.002% of the iodines and 0.001% of the alkali metals present in the core at the time of release. Most of the release would occur over a period of 10 hours. As in Release Category 6, the energy release rate would be very low.