ENCLOSURE II

CEN-239 SUPPLEMENT 1, PROBABILISTIC AND RISK ASSESSMENT OF THE EFFECTS OF PORV'S ON DEPRESSURIZATION AND DECAY HEAT REMOVAL

SAN ONOFRE NUCLEAR GENERATING STATION
UNITS 2 AND 3

JUNE 1983

CEN-239
Supplement 1

PROBABILISTIC RISK ASSESSMENT OF THE EFFECTS OF PORVs ON DEPRESSURIZATION AND DECAY HEAT REMOVAL

SAN ONOFRE NUCLEAR GENERATING STATION UNITS 2 AND 3

Prepared for the C-E Owners Group

Nuclear Power Systems Division
June, 1983

LEGAL NOTICE

This report was prepared as an account of work sponsored by Combustion Engineering, Inc. Neither Combustion Engineering nor any person acting on its behalf:

a. Makes any warranty or representation, express or implied including the warranties of fitness for a particular purpose or merchantability, with respect to the accuracy, completeness, or usefulness of the information contained in this report, or that the use of any information, apparatus, method, or process disclosed in this report may not infringe privately owned rights; or

b. Assumes any liabilities with respect to the use of, or for damages resulting from the use of, any information, apparatus, method or process disclosed in this report.

SUMMARY OF SUPPLEMENT 1

The NRC has requested that utilities owning C-E supplied NSSS plants without power operated relief valves provide a plant specific evaluation of the "rapid depressurization and decay heat removal capabilities" of their plants and respond to a series of questions (Appendix A). The following questions extracted from the list in Appendix A request a probabilistic evaluation of the potential change in risk that would result from adding power operated relief valves to these plants. This change in risk can be incorporated into a value-impact evaluation. The brief answers presented for these questions provide a synopsis of the analyses that are contained within this document. These results are specific to the San Onofre Nuclear Generating Stations Units 2 and 3 (SONGS). Answers to questions 1-7, 8e and 12-14 are provided in CEN-239 (28).

Question 8: For extended loss of main and auxiliary feedwater case where feed/bleed would be a potential backup:

a. What is the frequency of loss of main feedwater events; break down initiators that affect more than MFW, e.g., DC power?

b. What is the probability of recovering main feedwater? Provide your bases such as availability of procedures and the human error rates?

c. What is the probability of losing all auxiliary feedwater (given Item a)? Include considerations of recovering auxiliary feedwater as well as common cause failures (including those which could affect main feedwater availability and support system dependencies) and failures that could be hidden from detection via tests?

d. What is the uncertainty in the estimates provided for a), b) and c)?

e. How long would it take for core melt to initiate?

f. Were core to melt under these conditions, what is the likelihood of steam generator tube rupture(s) due to steam pressure from slumping core?

g. Characterize the consequences from core melt events of e) and f).

Response to Question 8:

A review of operating experience and a fault tree analysis were performed to determine the frequency of loss of MFW events. The analysis was completed on a plant specific basis and the results of the analysis are quantified by a statistical distribution which represents the frequency of loss of MFW. For SONGS, the initiating event frequency can be expressed in terms of a median value of 1.23 events per year with an associated error factor of 3. The error factor is defined as the ratio of the 95^{th} to 50^{th} percentile.

The median value represents the estimate that, considering uncertainty, would be expected to be higher than the true value with 50% confidence. The associated error factor is a ratio, as defined above, which when multiplied with the median estimate yields an upper bound estimate which would be expected to be higher than the true value with 95% confidence.

These results were further incorporated into an extensive evaluation of the core damage frequency due to loss of the

secondary heat sink. The analysis included an investigation of the potential for recovering feedwater. The core damage frequency contribution resulting from a loss of the secondary heat sink was evaluated for the current plant design which includes low pressure pumps (condensate pumps) for secondary heat removal following SG depressurization but has no PORVs, and for an alternative plant design which does not credit the alternate secondary heat removal capability but includes PORV depressurization and decay heat removal capability. The resulting core damage frequencies for SONGS are 3.1E-7 per year with an associated error factor of 21 without PORVs and 1.6E-7 per year with an associated error factor of 28 with PORVs.

The core damage frequency for loss of heat sink events was also evaluated assuming no alternate secondary heat removal capability and no PORV depressurization and decay heat removal capability. The resulting core damage frequency was estimated to be 2.1E-6 per year with an associated error factor of 19.

The complete analysis is presented in this report.

Question 9: What is the risk from steam generator(s) tube failures? As a minimum, consider the following:

a. Scenarios leading to core melt from one or more steam generator tubes failing in one steam generator. Include paths which consider failure of relief or safety valve in the faulted steam generator, capability of (or loss thereof) to depressurize the secondary side, the role of the ECCS including inventory and Boron availability.

b. What is the frequency of steam generator tube ruptures in two steam generators? This

estimate should include consideration of common cause failures such as design errors, events resulting in extremely high ΔP across the tubes, aging, etc. If tubes were to fail in both steam generators, what is the probability of core melt and generally characterize the consequences.

c. For a) and b) above, discuss the likelihood of steamlines filling with subcooled water and any consequential failures.

d. For a) and b), discuss uncertainties including human error rates (carefully considering the clarity and unambiguity of procedures).

Response to Question 9:

The frequency of the SGTR accident sequences which could potentially lead to core damage were statistically combined into two categories: 1) scenarios resulting from SGTR in one or two steam generators assuming offsite power was available and 2) scenarios resulting from SGTR in one or two steam generators with a coincident loss of offsite power. The complete analysis (which includes a detailed evaluation of each accident sequence) is presented in this report. The core damage frequency contribution due to SGTR in one or two steam generators for SONGS assuming offsite power is available can be expressed in terms of a median value of 1.5E-5 per year with an associated error factor of 5. The error factor is defined as the ratio of the 95^{th} to 50^{th} percentile. The core damage frequency contribution due to SGTR in one or two steam generators with coincident loss of offsite power is estimated to be 1.5E-6 per year with an associated error factor of 11.

The decrease in core damage frequency due to the added depressurization capability of PORVs was determined to be negligible compared to the core damage frequency contribution from all other SGTR accident sequences.

The likelihood of steam lines filling with subcooled water during a SGTR was also investigated. The total frequency of sequences that could possibly lead to SG overfill conditions was determined to be approximately 2.5E-4 per year (median value) with an associated error factor of 7 (ratio of 95^{th} to 50^{th} percentile).

Question 10: What is the core melt frequency from PORV initiated LOCA? Characterize the consequences?

Response to Question 10:

The core damage frequency due to PORV initiated LOCA was evaluated based on a plant design which would be assumed to provide increased RCS decay heat removal and depressurization capability. In this design, the PORVs are manually opened and the plant is assumed to operate with the PORV block valves closed which tends to minimize the risk associated with PORV LOCA. The results of the analysis are quantified by a statistical distribution representing the core damage frequency of PORV LOCA. The core damage frequency contribution due to PORV LOCA can be expressed in terms of a median value of 7.2E-8 per year with an associated error factor of 10. The error factor is defined as the ratio of the 95^{th} to 50^{th} percentile. If automatic actuation of the PORVs were to be assumed and if the plant were to operate with the block valves open, the core damage frequency contribution due to PORV LOCA would become 7.9E-7 per year with an associated error factor of 9.

Question 11: What is the net gain (or loss) in safety considering 8, 9, and 10 above if PORVs were to be installed? Are there any additional benefits (or drawbacks) achieved by installing PORVs? Examples of potential benefits are mitigation of ATWS and pressurized thermal shock, and reduced risk associated with depressurized primary system during a core melt.

Response to Question 11:

The overall change in core damage frequency (net gain or loss in safety) due to the installation of PORVs was determined by examining only those events which were considered to significantly contribute to an increase or decrease in the total core damage frequency. The core damage frequency contribution due to LOHS events and PORV LOCA is impacted by the presence of PORVs while the change in SGTR core damage frequencies does not contribute to a net gain or loss in safety. The calculation was performed with the SAMPLE code at the sequence level to account for dependencies between the sequences. The result indicates a negligible decrease in total core damage frequency due to the installation of manually actuated PORVs (less than 1.0E-8 per year).

If automatic actuation of the PORVs were to be assumed and if the plant were to operate with the block valves open, the result would indicate a net increase in total core damage frequency of 6.1E-7 per year (median value).

It should be noted that the above values are very small compared to the proposed NRC safety guideline of 10^{-4} core melts per year.

LIST OF ACRONYMS

ADV	Atmospheric dump valve
ADS	Atmospheric dump system
AFW	Auxiliary feedwater
AFWS	Auxiliary feedwater system
ATWS	Anticipated transient without SCRAM
BPS	Blowdown processing system
CCAS	Containment cooling actuation system
CCW	Component cooling water
CCWS	Component cooling water system
CEA	Control element assembly
CEDM	Control element drive mechanism
CEOG	Combustion Engineering Owners Group
CIAS	Containment isolation actuation signal
CSAS	Containment spray actuation signal
CS	Containment spray
CSS	Containment spray system
CVCS	Chemical and volume control system
DG	Diesel generator
ECCS	Emergency core cooling system
EDS	Electrical distribution system
EFAS	Emergency feedwater actuation system
EFW	Emergency feedwater
EFWS	Emergency feedwater system
ESF	Engineering safety features
ESFAS	Engineering safety features actuation signal
FSAR	Final Safety Analysis Report
FWCS	Feedwater control system
gpm	Gallons per minute
HEP	Human error probability
HP	High pressure
HPSI	High pressure safety injection
HX	Heat exchanger
LOCA	Loss of coolant accident
LOHS	Loss of secondary heat sink
LOOP	Loss of offsite power
MCC	Motor control center

LIST OF ACRONYMS

(continued)

MFW	Main feedwater
MSIS	Main steam isolation signal
MSIV	Main steam isolation valve
MSSV	Main steam safety valve
NRC	Nuclear Regulatory Commission
NREP	National Reliability Evaluation Program
NSSS	Nuclear steam supply system
PLCS	Pressurizer level control system
PORV	Power operated relief valve
PPCS	Pressurizer pressure control system
PPS	Plant protective system
psia	Pounds per square inch, absolute
psig	Pounds per square inch, gage
PTS	Pressurized thermal shock
RAS	Recirculation actuation signal
RCP	Reactor coolant pump
RCS	Reactor coolant system
RPS	Reactor protective system
RWT	Refueling water tank
SBCS	Steam bypass control system
SBLOCA	Small break loss of coolant accident
SCS	Shutdown cooling system
SG	Steam generator
SGTR	Steam generator tube rupture
SIAS	Safety injection actuation signal
SONGS	San Onofre nuclear generating stations
TBV	Turbine bypass valve
TBS	Turbine bypass system
TCV	Turbine control valve
TT	Turbine trip
T_{HOT}	Reactor coolant system hot leg temperature
VCT	Volume control tank
λ_{CD}	Core damage frequency

TABLE OF CONTENTS

TABLE OF CONTENTS
(continued)

TABLE OF CONTENTS
(continued)

TABLE OF CONTENTS
(continued)

TABLE OF CONTENTS
(continued)

TABLE OF CONTENTS
(continued)

LIST OF FIGURES

LIST OF FIGURES

LIST OF TABLES

LIST OF TABLES
(continued)

LIST OF TABLES
(continued)

PROBABILISTIC RISK ASSESSMENT OF THE EFFECT OF PORVs ON DEPRESSURIZATION AND DECAY HEAT REMOVAL

1.0 INTRODUCTION

1.1 PURPOSE

The NRC has requested that utilities owning C-E supplied NSSS plants without power operated relief valves provide a plant specific evaluation of the "rapid depressurization and decay heat removal capabilities" of their plants and respond to a series of questions originally forwarded to C-E (1) (Appendix A).

The objective of the work reported herein is to develop responses to the NRC questions for San Onofre Nuclear Generating Station, Units 2 and 3.

1.2 APPROACH

The NRC questions cover a wide range of topics, not all directly related to the subject of depressurization and decay heat removal. The work reported herein provides responses to questions 8 through 11 (Appendix A). Responses to the other questions are being addressed separately.

Questions 8 through 11 request information regarding the probability of core melt due to loss of heat sink, PORV LOCA, and steam generator tube rupture. This report provides this probabilistic information. In addition, the questions include numerous requests for information concerning physical phenomena associated with core damage or "degraded core" conditions. C-E believes it is appropriate to fully answer these questions only after 1) the probability of C-E plants experiencing such

degraded core conditions has been quantified (including appropriate evaluation of capabilities of existing equipment to function beyond their design bases to prevent or minimize core damage) and, 2) this probability has been shown to be higher than a commonly accepted standard or goal.

1.3 BACKGROUND

The early C-E NSSS designs used Power Operated Relief Valves (PORVs) as non-safety grade equipment to limit overpressure transients to pressures below the ASME Code safety valve setpoint. This function was intended to reduce challenges to the safety valves, thereby minimizing weepage and avoiding potential leakage following actuation. The PORVs were not intended to prevent a high pressure reactor trip, but rather, were to be used in conjunction with the trip to mitigate the pressure transient.

As each of the early plants became operational, the effectiveness of the pressurizer spray system to limit pressure transients was demonstrated. Consequently, C-E was unable to substantiate any advantages to opening PORVs during transients to protect the safety valves from leakage. PORVs were also considered to be counterproductive in light of the PORV leakage problems that had been experienced. Furthermore, best estimate transient analysis had demonstrated that the pressure overshoot above the high pressure trip to be so minimal that, when PORV operation was not credited, the safety valves were still not challenged. Accordingly, the PORV function during power operation was not considered necessary, and was eliminated from subsequent C-E designs.

Recently, a contingency method of core cooling employing once-through flow in the RCS has been advanced by the NRC as an alternate decay heat removal system. This method would use PORVs in conjunction with the High Pressure Safety Injection (HPSI) pumps and has been referred to as "feed and bleed". In this regard, the Advisory Committee on Reactor Safeguards (ACRS), following its review of C-E's System 80, (which is similar to San Onofre 2 & 3 in this regard) stated:

"In recent years, the availability of reliable shutdown heat removal capability for a wide range of transients has been recognized to be of great importance to safety. The System 80 design does not include capability for rapid, direct depressurization of the primary system or for any method of heat removal immediately after shutdown which does not require use of the steam generators. In the present design, the steam generators must be operated for heat removal after shutdown when the primary system is at high pressure and temperature. This places extra importance on the reliability of the auxiliary feedwater system used in connection with System 80 steam generators and extra requirements on the integrity of the steam generators. The ACRS believes that special attention should be given to these matters in connection with any plant employing the System 80 design. The Committee also believes that it may be useful to give consideration to the potential for adding valves of a size to facilitate rapid depressurization of the System 80 primary coolant system to allow more direct methods of decay heat removal. The Committee wishes to review this matter further with the cooperation of Combustion Engineering and the NRC Staff." (3)

In meetings with the ACRS and NRC Staff, C-E has presented its position and the bases for designs which do not employ PORVs. The NRC has raised a series of concerns regarding this issue and provided a list of questions to C-E and applicant utilities. In recognition of the scope of these questions the NRC has requested justification for operation during the period of time the questions are being addressed.

Justifications for continued operation have been submitted on both the SONGS 2 and 3 and CESSAR-System 80 dockets (4,5). These justifications are based on the following.

1. The NSSS is coupled with a highly reliable, safety grade Auxiliary Feedwater (AFW) System.

2. The Plant is capable of achieving cold shutdown conditions using only safety grade systems, even without offsite power and with an additional single failure.

3. The steam generator design includes many features which will enhance tube integrity, minimizing concerns associated with operating reactors. Additionally, careful attention to the plant water chemistry program will ensure that the magnitude of the impurity ingress into the steam generators is maintained at a low level.

4. Even if all auxiliary feedwater supply were somehow lost, the potential exists for a contingency heat removal scheme by depressurizing the steam generators to allow the use of low head pumps.

5. Review of probabilistic analyses does not appear to show any justification for the addition of Reactor Coolant System (RCS) valves for decay heat removal purposes.

1.4 REPORT OUTLINE

The purpose of this section is to provide a brief summary of the information contained in subsequent sections and to convey to the reader the manner in which the report format was developed with respect to the input required to generate and complete each consecutive section.

Section 1.0 presents an introduction to the report by stating the work objective, the approach taken, and by providing a report background.

The purpose of Section 2.0 is to provide a discussion of the procedures used in the various analyses that were required to generate answers to the NRC questions. The methodology employed in these analyses is described in terms of information sources for the reliability data, analytical procedures and computer codes used in the analyses.

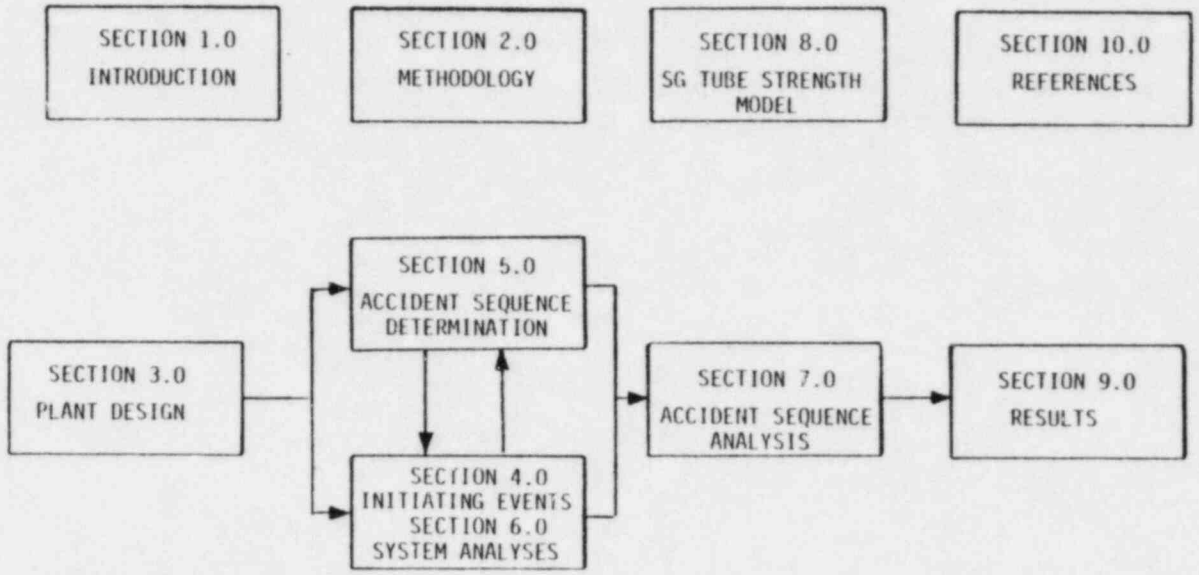


FIGURE 1.4-1

REPORT FLOWCHART

Section 3.0 provides a brief synopsis of the plant design and a list of design highlights for the plant systems addressed in the report. Also included is an overview of the interdependencies that exist between the various systems used to mitigate an event (i.e. LOHS, SGTR or PORV LOCA). The information in Section 3.0 is used to support event tree construction in Section 5.0 and fault tree development in Section 6.0.

The purpose of Section 4.0 is to identify and define the three initiating events considered to be most relevant to the PORV issue, i.e., Loss of Main Feedwater, SGTR and PORV LOCA. Also included is a brief description of each initiating event type and a presentation of the initiating event frequency associated with each event. These frequencies are used as input to the event tree analyses in Section 5.0 and the accident sequence analyses in Section 7.0.

Section 5.0 utilizes plant design data, transient analysis, and plant emergency procedures to develop event trees for each of the initiating events. The branches that are used to construct the event trees define the systems or actions that will require fault tree analysis. The quantitative fault tree results (presented in Section 6.0) are then input to the event trees in order to provide a basis for filtering out the low probability scenarios. The results of Section 5.0 include a list of accident sequences for each event tree. Each sequence is qualitatively evaluated to determine if it may or may not lead to core damage.

Section 6.0 contains the results of all fault tree analyses and probabilistic evaluations that are used as input to the event trees in Section 5.0. Plant design data and operating procedures were used to support development and construction of the fault tree logic diagrams. Each subsection includes a system description and schematic, a support system dependency diagram, a list of assumptions and quantitative results. The results are used as input to the event trees in Section 5.0 to provide

a basis for filtering out the low probability scenarios. The results are also used as input to the accident sequence analyses in Section 7.0 in order to statistically quantify core damage scenario frequencies.

The purpose of Section 7.0 is to identify and describe the minimal core damage scenarios that were selected from the lists of event tree output sequences in Section 5.0. The scenarios are statistically quantified using input failure data obtained from Sections 4.0 and 6.0.

Section 8.0 (in conjunction with Appendix B) provides an empirical SG tube strength model which is used to analyze the consequences of a group of events which provide excess primary/secondary pressure differences. The probability of SGTR is determined as a function of the number of tubes ruptured for an aged SG.

Section 9.0 summarizes the quantitative results of the study and provides the core damage frequency contribution due to each initiating event. The overall change in total core damage frequency associated with the installation of PORVs is evaluated and discussed.

2.0 METHODOLOGY

The four NRC questions, regarding the risk associated with the addition of PORVs to plants which do not initially have them, have all been addressed using standard risk assessment methodology (6). The underlying approach used in answering these questions consists of an estimation of the core damage frequency with and without PORVs and the determination of the net change. The NRC questions have limited the core damage frequency calculation to the consideration of three types of events for which the PORV is expected to play a major role, either as the initiator of the event or within some sequence of mitigating actions. The events are loss of secondary heat sink, steam generator tube ruptures in one or both steam generators and small break LOCA through an inadvertently open PORV.

The procedure for determining the core damage frequency used in this task is the same employed in all of the major PRA studies that have been performed to date, namely, to identify the event sequences which lead to core damage and to quantify the probability that any of these sequences occurs during a reactor-year of operation. Figure 2.0-1 contains a flowchart which illustrates the major elements of this procedure. The identification of the event sequences is accomplished using event tree analysis, incorporating design and reliability data, and input from any required human reliability analysis. The quantification of the sequence frequencies is a somewhat more complex operation involving fault tree analysis, interfacing of the fault tree results with the output of the event trees and uncertainty analysis.

This section describes the plant design and reliability data utilized in the various analyses and describes the methodology employed to perform the analyses referred to in Figure 2.0-1.

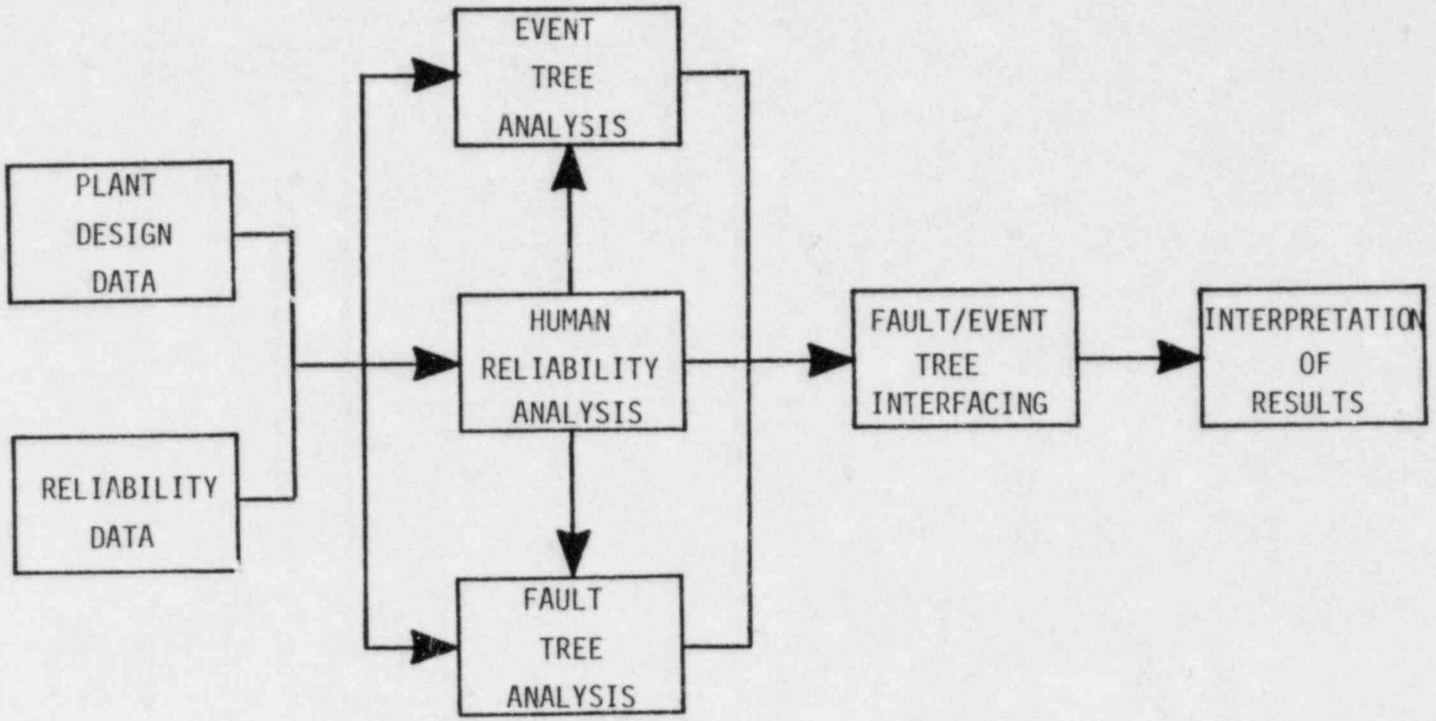


FIGURE 2.0-1

STUDY METHODOLOGY

2.1 INFORMATION SOURCES

Two general categories of information are used in performing risk assessment analyses, i.e., plant design and procedural information and reliability data. The various types of data within these categories and their sources are described in the following sections.

2.1.1 Plant Design and Procedural Information

Plant design and procedural information is used both in defining the event sequences and in determining the sequence occurrence frequencies. The enumeration of the event sequences first requires the definition of the nominal sequence of events, from the initiating event to stabilization of the plant parameters. The following data sources are used to obtain this:

- The plant FSAR (7) which provides
  - System descriptions
  - Descriptions of licensing transients
- The plant emergency procedures (8)
- CEN-152, C-E Emergency Procedure Guidelines (9)
- CEN-128, Responses of C-E NSSSs to Transients and Accidents (10)

Once the nominal sequence of events has been defined an event tree is assembled to identify off-nominal sequences. The event tree structure is defined by the physically logical sequences of events that can occur during the transient resulting from the initiating event and various combinations of additional failures. References (7) and (10) provided some insight into the behavior of the plant for several initiating events. Additional transient analyses, performed specifically to answer the NRC questions, were used to obtain further insight into plant behavior with the addition of several concurrent failures to the initiating event.

The quantification of the sequence occurrence frequencies requires the assembly and quantitative evaluation of fault tree and human failure models. The assembly of the fault tree model requires detailed information on system design and operation. The following data sources were used to obtain these:

- The plant FSAR (7) which provides
  - System descriptions
  - Piping and Instrumentation Diagrams (P&IDs)
- The plant system operating instructions (11)
- The plant electrical wiring diagrams (12)

The assembly of the human failure models requires the following data sources:

- The plant FSAR (7) which provides
  - Partial instrumentation lists
  - Equipment locations
- The plant emergency procedures (8)
- Plant system operating instructions (11)
- CEN-152, C-E Emergency Procedure Guidelines (9)
- Control panel layout drawings and instrumentation lists (13)

In addition to these sources, interviews with members of the SONGS staff and training personnel from the C-E simulator were conducted and the information obtained was factored into the models.

2.1.2 Reliability Data

The determination of the sequence occurrence frequencies involves two steps, i.e., the quantification of the individual elements of the sequence and the combination of these results to obtain a total frequency. The following types of numerical reliability data are necessary to perform these steps:

1. Initiating event frequencies

2. Component failure data, including
   - -Demand failure rates for standby components
   - -Operating failure rates for operating components
   - -Repair times
   - -Human failure probabilities
   - -Error factors for all of the above to be used in uncertainty calculations

A wide range of sources was used to assemble the data base used in these studies. The human failure data, including both human failure probabilities and associated error factors were obtained from the Handbook of Human Reliability Analysis (14). Data for mechanical and electrical components and for initiating events were obtained from the following sources:

- The National Reliability Evaluation Program (NREP) Data Base (15)
- The Reactor Safety Study (16)
- IEEE Standard 500 (17)
- C-E Reliability Data System (18)

- C-E Interim Data Base (19)

- Several specialized reports on
  - -Pumps (20)
  - -Loss of Offsite Power (21)
  - -Feedwater Transients and Small Break LOCAs (22)
  - -DC Power Supplies (23)

The majority of the data was obtained from References (15) and (16).

2.2 ANALYSIS

As stated previously the calculation of the core damage probability involves two major steps, each of which is accomplished through the use of one or more types of analyses. The following list specifies the elements of each step:

1. Definition of Core Damage Sequences
   a. Event Tree Analysis

2. Quantification of Sequence Probabilities
   a. Fault Tree Analysis
   b. Fault Tree/Event Tree Interfacing
   c. Human Reliability Analysis

Each of these elements appears in Figure 2.0-1 and will be described in detail in the following sections. A discussion of the methodology used in performing the human reliability analysis is contained in Section 6.17.

2.2.1 Event Tree Analysis

The objective of event tree analysis is to delineate the combinations of additional failures which can realistically occur following an initiating event. The types of additional failures considered in the analysis are limited to those which alone or in combination lead to a plant state of interest, in this case the occurrence of core damage.

Event trees were constructed for the three types of initiating events addressed in the NRC questions. These are as follows:

1. Loss of Secondary Heat Sink

2. Steam Generator Tube Rupture
   - Single generator
   - Double generator

3. Small Loss of Coolant Accident through a PORV

The event trees were constructed in two steps. The first involved the construction of a "functional" event tree in which the failures considered in conjunction with the initiating event were failures to perform safety functions. The second step was the expansion of the functional event tree into a system/action level event tree in which the additional failures were system failures or failures to perform a particular action. These steps and the computer code used to assemble the system/action level event trees are discussed below.

2.2.1.1 Function Level Event Trees

The function level event tree is an event tree in which the branch headings are defined as the failure to maintain safety functions required to protect the core. Table 2.2.1.1-1 contains a list of the five "anti-core melt" safety functions and their definitions

TABLE 2.2.1.1-1

ANTI-CORE MELT SAFETY FUNCTIONS

Safety Function	Purpose
Reactivity Control	Shut Reactor Down to Reduce Heat Production
Reactor Coolant System Inventory Control	Maintain a Coolant Medium around Core
Reactor Coolant System Pressure Control	Maintain the Coolant in the Proper State
Core Heat Removal	Transfer Heat from Core to a Coolant
Reactor Coolant System Heat Removal	Transfer Heat from the Core Coolant

(32). In the event tree analyses described in this report the safety function Reactivity Control was included only for illustrative purposes. Since ATWS scenarios were not considered to be within the scope of this study but have been addressed in previous studies (33,34) no detailed analysis was performed for the loss of this safety function.

Function level event trees are not quantified but represent an intermediate, qualitative step towards the assembly of the detailed system/action level event tree. The function event tree serves as a guide for the analyst and helps insure that all safety functions have been addressed. The assembly of the system/action level event tree proceeds directly from the function event tree through the expansion of each safety function heading into the one or more systems or actions required to maintain the safety function.

2.2.1.2 System/Action Level Event Trees

The system/action level event tree is an event tree in which the branch headings are defined as the failure of various systems or human operators to perform their required functions. The specific selection of system failures and operator actions is obtained through expansion of the function event tree.

The system/action level event tree is the final step in the event tree analysis and yields the list of event sequences (combinations of initiating event and additional failures) which will be quantified to obtain a core damage frequency. The quantification is discussed in Section 2.2.3.

One of the major considerations in the assembly of the system event tree is the treatment of the various support systems within the plant, e.g., offsite and emergency power, instrument air and component cooling water. Support systems have the potential for affecting the

reliability of several systems which appear on the event trees. For example, the loss of offsite power affects all systems which rely on offsite power and which must switch to diesel generators or station batteries in its absence.

There are two methods for treating support systems in the assembly of event trees. They are as follows:

1. Event tree boundary conditions
2. Fault tree linking

The use of event tree boundary conditions refers to the explicit incorporation of support system failures in the event tree, either as branch headings within the tree or as part of the specification of the initiating event. For example, loss of offsite power could be treated by defining the initiating event as "initiating event-with coincident loss of offsite power or -with no coincident loss of offsite power" and constructing two event trees, one for each situation. In this instance, the branch probabilities for those systems or actions which rely on offsite power would be different for the two trees. Alternatively, the loss of offsite power could appear as one of the branch headings within the tree. This would require the construction of a single tree but would increase its length and require any analysis codes to be capable of handling conditional branch probabilities for sequences in which the loss of offsite power appeared. The event trees constructed for the steam generator tube rupture analyses, in this report, treated loss of offsite power in the initiating event definition. Other support systems in the steam generator tube rupture trees as well as the event trees for loss of secondary heat sink and PORV LOCA employed the fault tree linking approach.

In the fault tree linking approach the support systems are treated within the fault tree models, for each system or action appearing in the event tree. This approach has the effect of minimizing the size

of the event tree, however, it increases the size of the individual fault trees and the complexity of the quantification procedure. This approach has been employed, to some degree, in all of the event trees presented in this report.

2.2.1.3 Description of the CEETAR Code

The construction of the event trees presented in this report was aided by the use of the computer code CEETAR (C-E Event Tree Analysis Routine). CEETAR requires the input of branch titles and logic rules, which are used to eliminate illogical sequences. Using this input, CEETAR produces a complete event tree which can be drafted automatically on an X-Y plotter or output on a line printer (if fewer than 15 branch headings are required). In addition, CEETAR will produce a listing of the output sequences using the literal descriptions of the branch headings.

If the initiating event frequency and branch probabilities are also provided as input, CEETAR will calculate the sequence frequencies. In addition, CEETAR can filter out sequences with frequencies below a specified cut-off value.

CEETAR is written in FORTRAN IV for use on the CDC 7600 computer.

2.2.2 Fault Tree Analysis

The quantification of the event tree sequences requires knowledge of the failure probabilities for each branch of the tree. When a branch represents a specific failure of a single component the failure probability can typically be obtained directly from one of the data sources described in Section 2.1.2. However, when a branch represents a specific failure mode of a system or subsystem it is necessary to construct a fault tree model of the system and to perform a quantitative evaluation of the model.

Below is a discussion of the construction and evaluation of the fault trees and a description of the computer code used to perform the analysis.

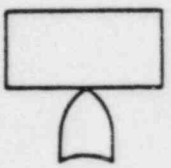
2.2.2.1 Fault Tree Construction

Each event tree branch which represents the failure of a system or subsystem requires the construction of a fault tree. The construction of the fault tree requires a complete definition of the functional requirements of the system, given the initiating event to which it is responding. The inability to meet these requirements defines the "top event" of the fault tree. The fault tree itself is a graphic model of the various parallel and sequential combinations of failures that will result in the top event. The symbols used in constructing the fault tree are illustrated and defined in Figure 2.2.2.1-1.

2.2.2.2 Fault Tree Evaluation

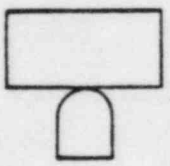
The evaluation of each fault tree yields both qualitative and quantitative information. The qualitative information consists of the "cutsets" of the model. The cutsets are the various combinations of component failures that result in the top event, i.e., the failure of the system. The cutsets form the basis of the quantitative evaluation which yields the failure probabilities required for the quantification of the event sequence frequencies.

FIGURE 2.2.2.1-1
FAULT TREE SYMBOLOGY



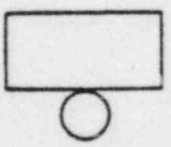
OR GATE

Output event occurs if one or more of the input events occurs.



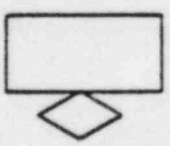
AND GATE

Output event occurs if and only if all input events occur.



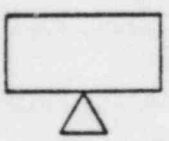
BASIC EVENT

Basic fault event requiring no further development.



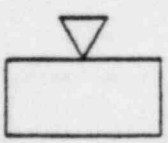
EXTERNAL INPUT

An event which is described by a fault tree model developed independently - typically a support system failure.



TRANSFER IN

Used as method of conveniently segmenting the tree for drafting purposes and to avoid duplication of portions of the tree. Indicates continuation to other portions of the tree.



TRANSFER OUT

The quantitative evaluation of the fault trees yields several numerical measures of a systems failure probability, two of which are typically employed in the event tree quantification, i.e., the unavailability and unreliability. The unavailability is the probability that a system will not respond when demanded. This value is used when the event tree branch represents a system function or action which is performed quickly, such as the reseating of a previously opened safety valve, or if the branch represents a particular condition, such as offsite power unavailable at turbine trip. The unreliability is the probability that a system will fail (at least once) during a given required operating period. This value is typically used when the event tree branch specifies a required operating period for a system, such as auxiliary feedwater system fails to deliver feedwater for four hours. The unreliability is usually added to the unavailability when the event tree branch represents the failure of a standby system to actuate and then run for a specified period of time.

2.2.2.3 Human Failures

Two types of human failures are included in the fault tree analyses performed in this study. They are "pre-existing maintenance errors" and failures of the operator to respond to various demands. Pre-existing maintenance errors are undetected errors committed since the last periodic test of a standby system. An example of this type of error is the failure to reopen a mini-flow valve which was closed for maintenance. A failure of the operator to respond includes the failure of the operator to perform a required function at all or to perform it correctly. An example of this type of error is the failure of the operator to back-up the automatic actuation of a safety system.

The probabilities for these types of human failures were obtained from Reference (14).

2.2.2.4 Description of the CEREC Code

The evaluation of the fault trees constructed for this study was aided by the use of the computer code CEREC (C-E Reliability Evaluation Code). CEREC is an extensively modified version of the PREP and KITT codes (24). The PREP portion of the code, which generates the cutsets, has several modifications to its output format. The KITT portion of the code, which performs the quantitative evaluations, has several major additions to the original KITT capabilities. They are as follows:

1. The capability of calculating the unavailability for a periodically tested standby system using either the demand failure rate (inhibit condition) or the standby failure rate, test interval and allowable downtime.

2. The capability of filtering out cutsets based on cutoff values for any of five calculated reliability parameters.

3. The capability of automatically performing sensitivity analyses on any parameter.

4. The capabilty of determining the uncertainty of any of the output reliability parameters based on the uncertainty of the component failure data.

CEREC is written in FORTRAN IV for use on the CDC 7600 computer.

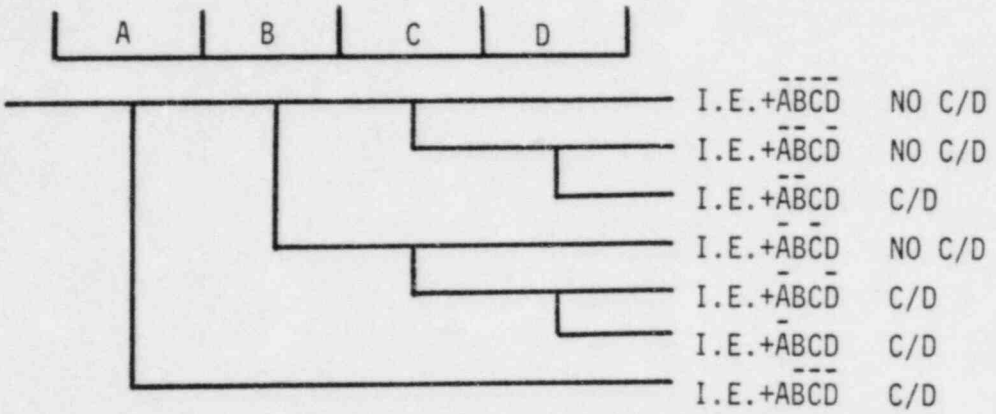
2.2.3 Fault Tree/Event Tree Interfacing

The goal of the event tree and fault tree modeling is the determination of a core damage frequency for initiating events. The previous sections discussed the development of the event trees to delineate the relevant failure sequences and the performance of the fault tree analyses to obtain the failure probabilities for the elements of the sequences. This section will describe the procedure used to combine these results to obtain a total core damage frequency for each initiating event.

The two primary concerns in this calculation are the effect of dependencies between the elements of a sequence and the uncertainty in the total core damage frequency due to uncertainties in the basic component failure data.

2.2.3.1 Calculation of Total Core Damage Frequency

Consider the following event tree



The first step in calculating the total core damage frequency, λ_{CD}, is the identification of the event tree sequences that lead to core damage. In the calculations performed for this study the core damage sequences were identified using several representative transient analyses and the definition of a peak cladding temperature of 2200°F as the on-set of core damage. In the example above, the core damage sequences are identified as such by the label on the right.

For this example, the total core damage frequency can be expressed as

$$\lambda_{CD} = \lambda_{I.E.} \times P\,[\bar{A}\bar{B}CD \cup \bar{A}BC\bar{D} \cup \bar{A}BCD \cup A\bar{B}\bar{C}\bar{D}] \qquad [1]$$

where $\lambda_{I.E.}$ = The occurrence frequency of the initiating event

$\cup$ signifies the union of the specified elements and the A, $\bar{A}$ notation indicates branch taken (failure) and branch not taken (success), respectively.

If no credit is taken for the probability of successful operation of a system, the "non-minimal" sequence, i.e., BCD, can be eliminated. A non-minimal sequence is one which contains additional failures beyond those necessary to obtain core damage. Since BC alone results in core damage, BCD is a non-minimal sequence. Equation 1 can be rewritten as

$$\lambda_{CD} = \lambda_{I.E.} \times P[CD \cup BC \cup A] \qquad [2]$$

This can be rewritten as

$$\lambda_{CD} = \lambda_{I.E.} \times [P_{CD} + P_{BC} + P_A \pm (\text{higher order terms})]. \qquad [3]$$

In the calculations performed in this report, the higher order terms, which are quite small, have been ignored.

If dependencies exist between the elements, Equation 3 can be written as

$$\lambda_{CD} = \lambda_{I.E.} \times \left[P_{C|I.E} \times P_{D|I.E.,C} + P_{B|I.E.} \times P_{C|I.E.,B} + P_{A|I.E.}\right] \qquad [4]$$

where $P_{X|I.E.}$ = The conditional probability of X given that the initiating event has occurred.

2.2.3.2 Dependent Failures

The existence of dependencies between the elements of the sequences gives rise to the need for conditional probabilities, as illustrated in the example in the previous section. The dependencies result from the sharing of components or support systems between the elements. The conditional probabilities resulting from the shared components is calculated as follows:

1. The particular components and/or support systems shared between two systems are identified.

2. The probability that each shared component is failed, given that the first system is failed, is calculated.

3. These conditional component failure probabilities are used in calculating the failure probability of the second system.

2.2.3.3 Description of the CEDAR Code

The CEDAR code (C-E Dependency Analysis Routine) is a utility code designed to automate the identification of shared components and the calculation of their conditional failure probabilities. The PREP portion of the CEREC code produces and stores a file containing the cutsets of a system fault tree model. CEDAR identifies common components within these files and calculates their conditional failure probability as the ratio of the sum of the probabilities of the cutsets containing the shared components to the total system failure probability.

CEDAR is written in FORTRAN IV for use on the CDC 7600 computer.

2.2.3.4 Uncertainty Analysis

As described in Section 2.2.2.4, the CEREC code has the capability of performing uncertainty analysis on the failure probability calculations for a fault tree. The uncertainty analysis uses Monte Carlo sampling of the component failure rates which are assumed to be represented by log-normal distributions. The output of the uncertainty analysis consists of a median and error factor for the fault tree model. Note that the use of error factors implies that the system failure probabilities are also represented by log-normal distributions.

Analytical results in this report are generally in terms of a median value with an error factor which, when multiplied by the median value, yields an upper bound estimate at 95% confidence. The median value, rather than the mean value, was chosen in order to be consistent with

WASH-1400, the IREP studies and most other PRAs and also in order to be consistent with the methodology recommended in the NRC's July 1982 draft Action Plan for Implementing the Commission's Proposed Safety Goal Policy statement.

Given the equation for the total core damage frequency (e.g. Equation 4), based on the event tree core damage sequences, and given the CEREC Monte Carlo outcome data for each element in the equation, the representative distributions for each element are determined and sampled to yield a distribution for the total frequency. This operation is performed by the SAMPLE code.

2.2.3.5 Description of the SAMPLE Code

The SAMPLE code, which was used in the Reactor Safety Study, is designed to perform uncertainty analysis on any generalized equation. The required input consists of a Fortran function subroutine to describe the function of interest, specification of the type of distributions to be used in modeling the variables of the function and the parameters used to define the distributions for each variable.

Monte Carlo simulation is performed by sampling the variable distributions and evaluating the function numerous times. These trials then define the distribution of the total function values and SAMPLE provides various descriptions of this distribution.

In the analyses performed for this task, the generalized equations consisted of individual sequence and total core damage frequency equations analogous to Equation 4. The probabilities of the sequence elements were represented by log-normal distributions. The parameters of the distributions were obtained from the CEREC runs for each element.

SAMPLE is written in Fortran IV for the CDC 7600.

3.0 PLANT DESIGN

3.1 PLANT DESCRIPTION

San Onofre Nuclear Generating Stations Units 2 and 3, operated by the Southern California Edison Company are part of a three unit station located on the West Coast of Southern California in San Diego county. The nuclear steam supply systems (NSSSs) are designed and supplied by Combustion Engineering. Each unit employs a pressurized water reactor. Major components of each NSSS include a reactor vessel and internals, control element assemblies, two steam generators, a pressurizer, four reactor coolant pumps and various control systems and instrumentation. The balance of the plants, including prestressed concrete reactor containment buildings in which each NSSS is located, are designed and constructed by the Los Angeles Power Division of Bechtel Power Corporation.

The San Onofre station features separate containments, safety equipment buildings, turbine buildings, diesel generator buildings, and fuel handling buildings for Units 2 and 3 and a shared auxiliary building and intake structure. The Pacific Ocean is the ultimate heat sink for all seismic category 1 cooling water systems. Saltwater is supplied to the component cooling water heat exchangers by saltwater cooling pumps located within separate intake conduits for each unit. Seawater pumped from the intake conduits by the circulating water pumps also serves as the heat sink for heat rejected by the main condensers and the turbine plant cooling water system.

The NSSS generates approximately 3410 MWt, producing saturated main steam. Each of the two NSSS units contains two primary coolant loops, each of which has two reactor coolant pumps, a reactor vessel outlet (hot) pipe and two inlet (cold) pipes. All safety systems are totally independent for each of the two units. The ECCS consists of redundant high pressure injection trains and redundant low pressure injection trains. Hot leg as well as cold leg injection capability exists. The Auxiliary Feedwater

System, serving the secondary side of the steam generators, is also separate for each unit. Each unit has 3 AFW pumping trains, each capable of supplying 100% flow. Each steam generator is supplied by a motor-driven pump with the third train, a steam turbine-driven pump, supplying both generators.

The containment systems for each unit include the containment structure, the containment heat removal systems, the containment air purification and cleanup systems, the containment isolation system, and the containment combustible gas control system. The containment design basis is to limit releases of radioactive materials subsequent to postulated accidents, such that resulting calculated offsite doses are less than the guideline values of 10CFR100. Each containment is served by both fan cooler and containment spray systems. These systems provide redundant and diverse containment heat removal capability.

Electrical power is supplied to plant equipment through multiple power sources. The main turbine-generator supplies the auxiliary loads during normal plant operation. Three reserve auxiliary transformers can be supplied by any one of the four Southern California Edison Company lines or the four San Diego Gas & Electric lines. Each unit has 2 backup diesel generators available for safety related loads in the event offsite power is lost. In addition, each unit's ESF auxiliary power system is capable of supplying power to the companion unit. Batteries are available for supplying the necessary DC power.

The power conversion system with the appropriate controls, converts the thermal energy generated in the reactor into electrical energy. This system consists of a turbine-generator, condenser, condensate pumps, feedwater heaters, and steam generator feed pumps. Two identical U-tube steam generators produce saturated steam. The two steam generator outlets are connected through a common header, to the turbine stop and turbine governing control valves of the turbine-generator.

The turbine is a horizontal, 1800 r/min, tandem-compound, impulse reaction machine. It consists of one double-flow, high-pressure (HP) element in tandem with three double-flow, low pressure (LP) elements. Moisture separation and reheating of the steam is provided between the HP and LP elements by horizontal-axis, cylindrical-shell, combined moisture separator reheater assemblies. The generator is a General Electric Corporation three-phase, 60 Hz, four-pole, cylindrical rotor, synchronous machine, directly coupled to the last low-pressure stage of the turbine. The generator employs a hydrogen-cooled rotor and a water cooled stator.

Electrical power from the generator is conducted from the generator terminals by an isolated-phase bus to a three-phase transformer that steps up the generator output voltage to the 230kV transmission voltage.

The reactor power levels and corresponding net electrical output are as follows:

- Core thermal power level - 3390 MWt
- Net electrical power output at generator terminal - 1127 MWe
- Electrical power output consumed onsite - 70 MWe
- Net electrical power output consumed offsite - 1057 MWe

3.2 PLANT SYSTEMS

Table 3.2-1 presents a list of plant systems that were evaluated for this task. System design highlights are also included. A more detailed description of each system is provided in Section 6.0.

TABLE 3.2-1

PLANT SYSTEMS

SYSTEM	DESIGN HIGHLIGHTS
High Pressure Safety Injection System	• Two Train Safety System • One Motor Driven Pump in Each Train • Installed Spare Motor Driven Pump
Auxiliary Spray System	• Safety System • Flow Provided by any One of Three Charging Pumps
Containment Heat Removal Systems	• Two Train Containment Fan Cooler System • Two Train Containment Spray System
Power Operated Relief Valves[1]	• Two Flow Paths • Block Valve and Coded Relief Valve in each Path
Primary Feed and Bleed System[1]	• Feed Flow Required From One HPSI and One Charging Pump or From Two HPSI Pumps • Two of Two Flow Paths required for Bleed Portion
Turbine Bypass System	• Control System • 45% Turbine Bypass Capacity
Main Steam Isolation	• Safety System with Redundancy • Safety Coded Valve in Each Path
Atmospheric Dump System	• Safety System • One Safety Coded Valve per Steam Generator
Main Steam Safety Valves	• Banks of Coded Safety Valves with Redundancy
Main Feedwater System	• Four Motor Driven Condensate Pumps • Two Turbine Driven Feed Pumps
Auxiliary Feedwater System	• Safety System with Redundancy • Two Motor Driven Pumps • One Turbine Driven Pump
Blowdown Processing System	• Non-Safety System
Alternate Secondary Heat Removal Capability (Condensate System)	• Non-Safety System

1. Assuming PORVs are installed.

TABLE 3.2-1
(continued)

PLANT SYSTEMS

SYSTEM	DESIGN HIGHLIGHTS
Electrical Distribution System	• Two Redundant Power Divisions • One Diesel Generator in Each Class 1E Power Division
Component Cooling Water System	• Safety System with Redundancy • One Motor Driven Pump in Each Train • Installed Spare Motor Driven Pump
Instrument Air System	• Non-Safety System

3.3 SYSTEM INTERDEPENDENCIES

3.3.1 Mitigating versus Support Systems

The successful operation of front line safety systems may require the operability of one or more support systems. An understanding of front line versus support systems interdependencies is fundamental to the study of accident scenarios. Also nuclear industry operating experience has indicated that some of the more severe accidents have originated from failures originating in support systems. A matrix of front line vs. support systems can be a useful tool for readily evaluating the extent of system interdependencies in a power plant. Table 3.3.1-1 provides a list of the mitigating systems addressed in this study vs. support systems. It should be understood that any interdependence identified in the matrix does not necessarily indicate that the loss of a particular support system is sufficient to cause failure of the associated mitigating systems.

3.3.2 Support versus Support systems

In many instances, successful operation of support systems requires the operability of other support systems. Table 3.3.2-1 depicts the SONGS support system interdependencies. It should be understood that any interdependence identified in the matrix does not necessarily indicate that the loss of a particular support system is sufficient to cause failure of the associated support system.

TABLE 3.3.1-1

MITIGATING VERSUS SUPPORT SYSTEMS[1]

MITIGATING SYSTEMS / SUPPORT SYSTEMS	Onsite AC Non-1E	Offsite AC	Onsite AC Class 1E	125V DC Class 1E	Instrument Air	Component Cooling Water	ESFAS
High Pressure Safety Injection		X	X	X		X	X
Auxiliary Spray System[2]	X	X	X	X	X		X
Containment Heat Removal System		X	X	X		X	X
PORV[3]		X	X	X			
Primary Feed and Bleed[3]		X	X	X		X	X
Turbine Bypass System	X	X			X		
Main Steam Isolation				X			X
Atmospheric Dump System				X	X		
Main Steam Safety Valves							
Main Feedwater System	X	X			X		X
Auxiliary Feedwater System		X	X	X			X
Blowdown Processing System	X	X			X		X
Alternate Secondary Heat Removal Capability	X	X					

[1]Any interdependency identified in the matrix does not necessarily indicate that the loss of a particular support system is sufficient to cause failure of the associated mitigating systems.

[2]System boundries are assumed to include the charging pumps.

[3]Assuming PORVs are installed.

TABLE 3.3.2-1

SUPPORT SYSTEM VERSUS SUPPORT SYSTEM[1]

SUPPORT SYSTEMS	Onsite AC Non-1E	Offsite AC	Onsite AC Class 1E	125V DC Class 1E	Component Cooling Water	ESFAS	Instrument Air
Onsite AC Non-1E							
Offsite AC							
Onsite AC Class 1E				X		X	
125V DC Class 1E							
Component Cooling Water		X	X	X		X	
ESFAS		X	X	X			
Instrument Air	X	X					

[1]Any interdependency identified in the matrix does not necessarily indicate that the loss of a particular support system is sufficient to cause failure of the associated support systems.

TABLE 4.3.1-1

LOSS OF MAIN FEEDWATER INITIATING EVENT FREQUENCY

Frequency (Median Value per year)	Error Factor
1.23	3

Note: The above frequency is used as input to the Loss of Secondary Heat Sink Event Trees discussed in Section 5.1. The initiating event frequency is combined with mitigating system failure probabilities to evaluate accident sequences.

4.3.2 Steam Generator Tube Rupture

A SGTR is usually defined as a tube leak or rupture whose maximum leak flow rate exceeds the capacity of the charging system. Four distinct initiating events were defined for input to the SGTR analyses:

- Initiating event 1 is defined as one or more tube ruptures occurring in one steam generator. Offsite power is assumed to be available at the time of the initiating event.

- Initiating event 2 is defined as one or more tube ruptures occurring in one steam generator with a coincident loss of offsite power.

- Initiating event 3 is defined as one or more tube ruptures occurring in both steam generators. Offsite power is assumed to be available at the time of the initiating event.

- Initiating event 4 is defined as one or more tube ruptures occurring in both steam generators with a coincident loss of offsite power.

A survey of operating history was conducted to provide a basis for estimating the above initiating event frequencies. A SGTR was further defined as a tube leak or rupture whose maximum flow rate was equal to or greater than 125 gpm. The following events were interpreted as SGTRs (25).

Plant	Date	Maximum Flow Rate (gpm)
Point Beach 1	2/26/75	125
Prairie Island 1	10/2/79	390
R. E. Ginna 1	1/25/82	630
Surry 2	9/25/76	330

These four events are assumed to be the only recognized SGTRs in US PWR commercial experience to date. The total number of reactor years of experience was evaluated to be 361.0 years as of December, 1982 (18).

The distribution of time to occurrence of SGTR in one SG was assumed to be exponential. The probability of SGTR in one SG by time t is expressed mathematically as

$$F(t) = 1 - e^{-\theta t} \qquad t \geq 0 \qquad [1]$$

where θ is the occurrence rate for SGTR. Confidence bounds on the occurrence rate are obtained from percentiles of the χ^2 distribution since the distribution of the sample mean $\hat{\theta}$, an estimate of θ, is distributed as χ^2. (26). The confidence bounds are obtained by solving the following equations for θ_L and θ_u from tables provided in Reference (26).

$$\int_{\theta_u}^{\infty} g(x)dx = \alpha/2 \qquad [2]$$

$$\int_{0}^{\theta_L} g(x)dx = \alpha/2 \qquad [3]$$

where $g(x)$ is the χ^2 probability density function with $\gamma = 2n$ degrees of freedom for the lower bound and $\gamma = 2(n+1)$ degrees of freedom for the upper bounds. The $100(1-\alpha)\%$ confidence interval for θ is then

$$\frac{\hat{\theta}}{2n} \chi^2_{\alpha/2,2n} \leq \theta \leq \frac{\hat{\theta}}{2n} \chi^2_{1-\alpha/2,\ 2n+2} \qquad [4]$$

For the SGTR in one SG events which have been experienced

$n = 4$

$$\hat{\theta} = 4./T = 4./361.\ \text{years} = 1.108 \times 10^{-2}\ /\ \text{year}$$

T = total number of reactor years

The table values of the χ^2 distribution are

$\chi^2_{.05,8} = 2.733$ $\chi^2_{.95,10} = 18.307$

The 90% confidence interval for θ is then

$$\frac{1.108 \times 10^{-2}}{8} (2.733) \leq \theta \leq \frac{1.108 \times 10^{-2}}{8} (18.307)$$

$$3.8 \times 10^{-3} \leq \theta \leq 2.5 \times 10^{-2}$$

The median value of is determined by using the following expression

$$\theta_{.5} = \frac{\chi^2_{.5,10}}{2n} \hat{\theta} = \frac{9.432 (1.108 \times 10^{-2})}{8} = 1.3 \times 10^{-2}/\text{year}$$

The distribution of θ was approximated by a lognormal when initiating event probability distributions were simulated by combining distributions with a Monte Carlo (stochastic sampling) computer code. In this case, the 5th and 95th percentiles of the χ^2 distribution were matched to the 5th and 95th percentiles of a lognormal distribution. The median of the lognormal distribution is estimated by

$$\tilde{\theta} = [(3.8 \times 10^{-3})(2.5 \times 10^{-2}]^{1/2} = 9.7 \times \text{E-3 per year}$$

The error factor for the lognormal distribution approximation was calculated to be

$$EF = \frac{\theta_{.95}}{\theta_{.5}} = \frac{2.5 \times 10^{-2}}{9.7 \times 10^{-3}} = 2.6$$

A value of EF = 3 was used in the analysis

To determine the frequency of the initiating event SGTR in One SG with Coincident Loss of Offsite Power, the above results were combined with a loss of offsite power median failure probability of 10^{-3} assuming a lognormal distribution and an error factor of 10 (16). (It should be noted that this is a generic value and for SONGS this number might be lower, i.e., the transmission system has a high transient stability limit due to high installed capacity and extensive grid interconnections with

other utilities.) Monte Carlo uncertainty analysis was used to determine the median value and approximate error factor for the combined probabilities. The resulting initiating event frequency is 9.8E-6 per year with an associated error factor of 13.

There have been no known SGTRs in two SGs in the history of PWR commercial operation. An event frequency for SGTRs in two SGs can be estimated given that T = 361.0 years and n = 0. The median occurrence rate is approximated by

$$\frac{\chi^2_{.50,\ 2n+2}}{2T} = \frac{1.39}{2(361)} = 1.9\ \text{E-3 per year}$$

The error factor was estimated by taking the ratio of the 95 to 50 percentile.

$$\frac{\chi^2_{.95,\ 2n+2}}{2T} = \frac{5.99}{2(361)} = 8.3\ \text{E-3 per year}$$

$$\frac{8.3\text{E-3}}{1.9\text{E-3}} = 4.4 \approx 5$$

To determine the frequency of the initiating event SGTR in Two SGs with Coincident Loss of Offsite power, the above results were combined with a loss of offsite power median failure probability of 10^{-3} (assuming a log normal distribution and an error factor of 10 (16). Monte Carlo uncertainty analysis was used to determine the median value and error factor for the combined probabilities. The resulting initiating event frequency is 1.9E-6 per year with an associated error factor of 13.

SGTR initiating event frequencies are summarized in Table 4.3.2-1. Section 8.0 presents a discussion of a steam generator tube strength model for aged steam generators.

TABLE 4.3.2-1

SGTR INITIATING EVENT FREQUENCIES

Event Description	Frequency (Median Value per Year)	Error Factor
SGTR in One SG	9.7E-3	3
SGTR in One SG with Coincident LOOP	9.8E-6	13
SGTR in Two SGs	1.9E-3	5
SGTR in Two SGs with Coincident LOOP	1.9E-6	13

Note: The above frequencies are used as input to the SGTR event trees discussed in Section 5.2. The initiating event frequencies are combined with mitigating system failure probabilities to evaluate accident sequences.

4.3.3 PORV LOCA

PORV LOCA was identified as one of the three types of events to be considered in the core damage frequency calculations. The assumed PORV design allows for the valves to be opened manually to reduce RCS pressure following a steam generator tube rupture event or a loss of secondary heat sink. The PORVs are assumed not to be designed to minimize challenges to the primary safety valves.

A PORV LOCA is a breach of the RCS pressure boundary that results in an initial rapid uncontrolled depressurization of the RCS. Therefore, mitigation of this transient requires makeup of the lost RCS inventory as well as removal of heat from the reactor core and RCS. The success criteria for RCS inventory makeup and heat removal were determined by transient analyses (7,36). Success for RCS inventory makeup requires at least one HPSI pump to inject borated water into the RCS loops. Successful removal of RCS heat can be accomplished by the steam generators or the containment heat removal systems. Success for RCS heat removal by the steam generators requires at least one steam generator with feedwater available to maintain the steam generator water level. Success for RCS heat removal by the containment heat removal systems requires at least two emergency containment fan coolers or at least one containment spray train to remove thermal energy discharged into the containment from the RCS.

Based on the assumed PORV design, three types of PORV LOCAs were considered. The three types are as follows:

1. PORV LOCA Following Loss of Secondary Heat Sink. This type of PORV LOCA refers to manually opening the PORV flowpaths following a loss of secondary heat sink. The steam generators are unavailable to remove RCS heat.

2. PORV LOCA Following SGTR. This type of PORV LOCA refers to manually opening the PORV flowpaths following a tube rupture in one steam generator. The unaffected steam generator is available to remove RCS heat.

3. Spurious PORV LOCA. This type of PORV LOCA includes error induced opening of either PORV flowpath. Both steam generators are available to remove RCS heat.

For each type of PORV LOCA considered, a fault tree analysis was performed (See Section 6.4) to quantify the occurrence frequency. The occurrence frequencies for loss of secondary heat sink and tube rupture in one steam generator were incorporated into the fault trees to evaluate the occurrence frequencies for these types of PORV LOCA. Nuclear operating experience information (27) was used along with an assumed valve testing frequency that varies from two weeks to quarterly to evaluate the Spurious PORV LOCA occurrence frequency. These frequencies are presented in Table 4.3.3-1.

TABLE 4.3.3-1

PORV LOCA INITIATING EVENT FREQUENCIES

Event Description	Frequency (Median Value per Year)	Error Factor
PORV LOCA Following LOHS	1.5E-6	29
PORV LOCA Following SGTR	1.3E-4	7
Spurious PORV LOCA	3.2E-5	16

Note: The above frequencies are used as input to the PORV LOCA event trees discussed in Section 5.3. The initiating event frequencies are combined with mitigating system failure probabilities to evaluate accident sequences.

5.0 ACCIDENT SEQUENCE DETERMINATION

The sequence of malfunctions or failures of systems that lead to core damage conditions for each initiating event considered, were determined by developing functional and systemic event trees. The functional event tree interrelates an initiating event (Loss of Main Feedwater, SG tube rupture or PORV induced LOCA) with plant safety function failures and yields functional accident sequences. The systemic event tree interrelates each initiating event with system failure events and yields system accident sequences. Section 2 provides a more detailed description of the methodology used in the development of the event trees and fault trees and the treatment of system interactions and support system dependencies.

The accident sequences for the loss of secondary heat sink, PORV induced LOCA, and steam generator tube rupture were determined using event tree/fault tree methodology. In order to provide consistency in identifying the accident sequences for these transients, the following general rules were followed:

- Event tree models, both functional and systemic, are developed from the initiating event to a state representing either shutdown cooling entry conditions or core damage conditions.

- Core damage conditions are defined as peak cladding temperatures of 2200°F.

- All systems are in the normal, automatic mode of operation at the time of the initiating event.

- Reactor trip will occur when plant protection system setpoints are reached.

- The event tree/fault tree analyses are based on the SONGS Unit 2 design. The results are considered to be applicable to Unit 3.

5.1 LOSS OF HEAT SINK

A loss of secondary heat sink refers to the inability to remove RCS and core heat via the steam generators as a result of losing main feedwater and auxiliary feedwater flow. During normal plant operations, the MFW system provides a continuous supply of feedwater to the steam generators at required pressure and temperature for full load to zero load operations. Following the loss of main feedwater, the AFW system automatically supplies feedwater to the steam generators for reactor decay heat removal and to cooldown the RCS to shutdown cooling entry conditions. A loss of main and auxiliary feedwater flow and failure to re-establish a secondary heat sink will cause RCS temperature and pressure to increase and eventually threaten core integrity.

During a loss of secondary heat sink event, RCS temperature is controlled at a value slightly above that corresponding to steam generator saturation conditions until a substantial portion of the tube bundle in each steam generator is uncovered. At this point, RCS temperature will begin to increase. When the steam generators boil dry, RCS temperature and pressure will rise rapidly. If conditions in the RCS reach the setpoints for the primary safety valves, RCS inventory will begin to discharge out the safety valves. If a secondary heat sink is not re-established and loss of RCS inventory continues at high pressure, core uncovery will occur. Core damage conditions, defined for this study as peak cladding temperatures of 2200°F, will be reached in approximately 1 hour following a reactor trip signal based on low steam generator level (28, Section 2.8).

5.1.1 Initiating Event

A loss of normal operating feedwater is defined as a reduction in feedwater flow to the steam generators, when operating at power, without a corresponding reduction in steam flow from the steam generators. The result of this flow mismatch leads to reduction in steam generator water inventory and a subsequent heatup of the primary coolant. The PPS provides

protection against the loss of normal feedwater by the steam generator low water level trip. The Main Feedwater System is designed to automatically provide 5% bypass flow to meet RCS decay heat removal requirements following a reactor trip event.

The initiating event for the loss of heat sink analysis will be defined as the loss of normal operating main feedwater flow resulting from automatic plant/reactor trip events and the loss of the post-trip 5% bypass flow. Included in this definition are plant trips that are a result of perturbations in the main feedwater system or its support systems. The frequency of loss of main feedwater was evaluated by fault tree analysis (See Section 6.10).

5.1.2 Normal Sequence of Events

The normal sequence of events following a loss of operating MFW flow and post-trip 5% bypass flow, is a continued decrease in steam generator water level and the automatic initiation of the Auxiliary Feedwater System. The Auxiliary Feedwater System, consisting of two motor-driven and one turbine-driven feedwater pumps, is employed to effectuate core cooldown. Following a reactor trip, the TBVs are normally used to control steam generator pressure. If the TBVs are unavailable, steam pressure may be controlled by the ADVs or the MSSVs. The pressurizer auxiliary sprays provide RCS pressure control and are used to reduce primary pressure.

Table 5.1.2-1 presents the normal sequence of events following loss of main feedwater from the initiating event until event termination at shutdown cooling entry conditions.

5.1.3 Functional Event Tree

The Loss of Secondary Heat Sink functional event tree, presented in Figure 5.1.3-1, was developed to determine the functional accident sequences that could lead to potential core damage. The functional event tree was

TABLE 5.1.2-1

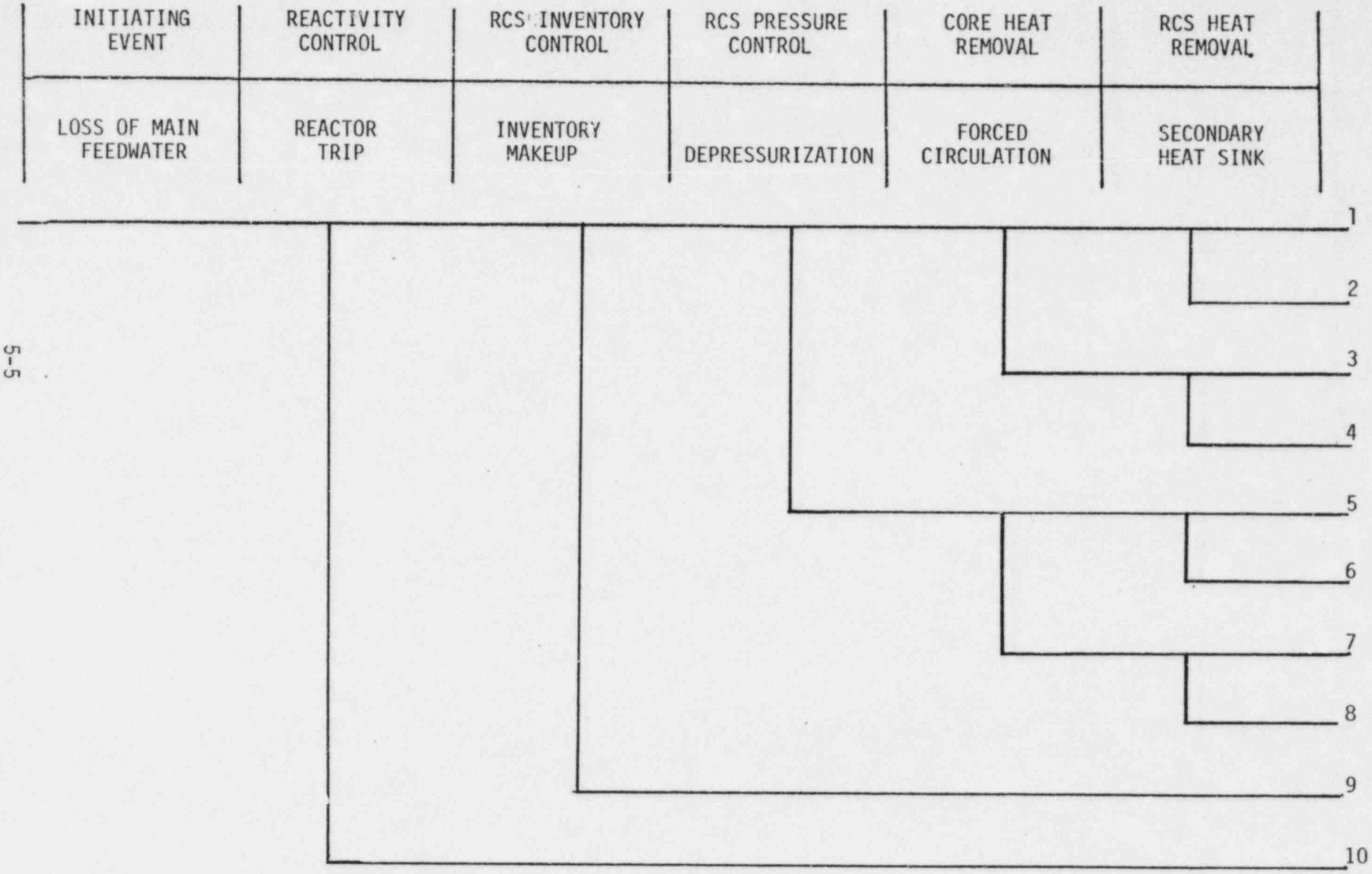
NORMAL SEQUENCE OF EVENTS FOR LOSS OF FEEDWATER

1. Termination of main feedwater flow
2. SBCS Quick Open of TBVs
3. Reactor/Turbine Trip on low steam generator water level
4. MSSVs open
5. AFW flow actuated and delivered
6. MSSVs close
7. Cooldown controlled using AFW, SBCS and Pressurizer Auxiliary Spray
8. When condenser vacuum becomes unavailable, continue cooldown with ADVs
9. Shutdown cooling entry conditions reached

FIGURE 5.1.3-1

LOSS OF SECONDARY HEAT SINK

FUNCTIONAL EVENT TREE



developed for the current plant design and for the plant design assuming feed and bleed capability is provided. As depicted in Table 5.1.3-1, each safety function can be defined in terms of functional elements which are used as intermediaries to correlate the five anti-core melt safety functions (32) to the specific plant systems or actions required to mitigate a loss of secondary heat sink. The list of associated systems/actions provides the logical groundwork for constructing a system/action level event tree which can be used to generate more detailed accident scenarios.

The functional accident sequences for the loss of heat sink event are discussed as follows:

Sequence 1 — Sequence 1 is the transient when all safety functions are satisfied following the initiating event. In this sequence, the core is cooled, secondary system and core integrity are maintained and shutdown cooling entry conditions are reached.

Sequence 2 — Sequence 2 is the transient when the safety function, RCS Heat Removal, is not maintained. This sequence results in core damage conditions.

Sequence 3 — Sequence 3 represents the transient when Core Heat Removal by forced circulation, RCP operation, is not maintained. In this sequence, the secondary system and core integrity are maintained and shutdown cooling entry conditions are reached with natural circulation conditions existing in the RCS.

Sequence 4 — Sequence 4 results in core damage conditions due to failure to provide RCS Heat Removal and failure the of Core Heat Removal safety function.

Sequence 5 — Sequence 5 represents the transient when RCS Pressure Control, depressurization of the primary system, fails. In this sequence, the core and RCS are cooled, but the primary

TABLE 5.1.3-1

LOSS OF SECONDARY HEAT SINK FUNCTIONAL EVENT TREE CONSIDERATIONS

SAFETY FUNCTION	FUNCTIONAL ELEMENTS	ASSOCIATED SYSTEMS/ACTIONS
Reactivity Control	Reactor Trip	Reactor Trip [1]
RCS Inventory Control	Inventory Makeup	There are no specific systems/actions required for RCS Inventory control except through RCS Pressure Control and RCS Heat Removal.
RCS Pressure Control	Depressurization	Auxiliary Sprays Feed and Bleed Operation [2]
Core Heat Removal	Forced Circulation	RCP Operation
RCS Heat Removal	Secondary Heat Sink	Auxiliary Feedwater System Restoration of Feed Flow Alt. Sec. Heat Removal Capability Removal of Secondary Steam Feed and Bleed Operation [2] Containment Sprays [2] HP Recirculation [2]

[1] ATWS will not be considered in the scope of this evaluation

[2] Associated systems/actions assuming feed and bleed capability is provided

pressure criteria for shutdown cooling entry conditions is not achieved. This results in a stable core configuration with a long term demand on the safety function, RCS Heat Removal.

Sequence 6 — Sequence 6 results in core damage conditions due to failure to provide the RCS Heat Removal and RCS Pressure Control safety functions.

Sequence 7 — In Sequence 7, RCS Heat Removal is provided but safety functions RCS Pressure Control and Core Heat Removal have failed. Sequence 7 results in a stable core state but impacts the actions associated with RCS Heat Removal. See Sequences 3 and 5.

Sequence 8 — Sequence 8 results in core damage conditions due to failure to provide RCS Heat Removal and failure of Core Heat Removal and RCS Pressure Control.

Sequence 9 — The safety function, RCS Inventory Control, is satisfied by RCS Pressure Control and RCS Heat Removal.

Sequence 10 — As discussed in Section 2.2.1.1, ATWS is not considered in the scope of this program.

5.1.4 Systemic Event Tree

The systemic event trees were developed by determining the systems/actions which perform in response to the loss of secondary heat sink transient for each of the safety functions identified in Table 5.1.3-1. The systems/actions define the systemic event tree branch headings. The systems/actions were then placed in approximately the chronological order that they will be called upon following the transient. The initiating event, Loss of Main Feedwater, and transient analysis determine the success

criteria for those systems or actions. These criteria dictate the top failure logic for the system fault trees. In addition to the system success, accident mitigation also requires the successful operation of support systems upon which the systems depend. Section 3.3 details the mitigating system/support system dependencies for the systems required in the loss of secondary heat sink transient.

Two systemic event trees were developed for Loss of Secondary Heat Sink. The Loss of Secondary Heat Sink Event Tree discussed in Section 5.1.4.1 determines the core damage scenarios for the current plant design including alternate secondary heat removal capability. The event tree in Section 5.1.4.2, Loss of Secondary Heat Sink with Feed and Bleed Operation Event Tree, determines the core damage scenarios assuming primary feed and bleed capability is provided. Table 5.1.4-1 defines the event tree branches and associated failure criteria that are used as input to both event trees. The fault tree results for the systems specified in the systemic event trees are presented in Section 6.0.

5.1.4.1 The Loss of Secondary Heat Sink Event Tree

The Loss of Secondary Heat Sink Event Tree is presented in Figure 5.1.4.1-1. The safety function, RCS Heat Removal, is provided by the Auxiliary Feedwater System, Restoration of Feed Flow, Alternate Decay Heat Removal (low pressure secondary heat sink) and Secondary Steam Removal. (Refer to Table 5.1.3-1). The safety function, Core Heat Removal, refers to termination of RCP Operation and the safety function, RCS Pressure Control, refers to operation of auxiliary sprays.

The event tree accident sequences were filtered using a frequency cutoff of 10^{-8} per year. The sequences that lead to core damage conditions are discussed in detail in Section 7.1.1. The branch headings are briefly discussed below:

TABLE 5.1.4-1

LOSS OF SECONDARY HEAT SINK
EVENT TREE BRANCH DEFINITIONS

Branch Designation	Branch Title	Failure Criteria
LF	Initiating Event	Loss of Main Feedwater Flow, Plant/Reactor Trip Events and Failure to Deliver 5% MFW Bypass Flow from 1 of 2 MFW Pumps to 1 SG
G_1	Fail to Deliver AFW Flow	Failure to Automatically Deliver AFW Flow from 1 of 3 AFW Pumps to One SG
U_1	Failure to Restore Feed Flow	Failure to Manually Restore AFW Flow from 1 of 3 AFW Pumps to 1 SG in 50 Minutes Following a Loss of Main and Auxiliary Feed Flow
U_2	Failure to Restore Feed Flow	Failure to Manually Restore AFW Flow from 1 of 3 AFW Pumps to 1 SG in 20 Minutes Following a Loss of Main and Auxiliary Feed Flow[1]
V	Failure of Alt. Sec. Capability	Failure to Manually Establish Feed Flow from a Low Pressure Secondary Heat Sink (Flow from 1 of 3 Condensate Pumps delivered to 1 SG) in 50 minutes
W_1	Failure to Remove Secondary Steam	Failure to Remove Steam from SG by Opening 1 of 4 TBVs, 1 of 2 ADVs or 1 of 18 MSSVs
X	Failure to Terminate RCP Operation	Failure to Manually Terminate RCP Operation Upon Indication of Total Loss of Feed Flow
N	Failure to Initiate Auxiliary Spray Flow	Failure to Deliver Auxiliary Spray Flow from 1 of 3 Charging Pumps to the Pressurizer

1 These branches are applicable assuming feed and bleed capability is provided.

TABLE 5.1.4-1
(continued)
LOSS OF SECONDARY HEAT SINK
EVENT TREE BRANCH DEFINITIONS

Branch Designation	Branch Title	Failure Criteria
Y	Failure of Feed and Bleed Operation	Failure to Establish Flow through 2 of 2 PORV Trains and to Deliver Makeup Flow from 1 of 3 HPSI Pumps and 1 of 2 Charging Pumps or 2 of 3 HPSI Pumps[1]
S_2	Failure of Containment Sprays	Failure of 2 of 2 Containment Spray Trains to Deliver Flow to Containment[1]
R	Failure to Achieve HP Recirculation	Failure to Provide Flow to the RCS from 1 of 2 HP Pumps Taking Suction from the Containment Sump[1]

1 These branches are applicable assuming feed and bleed capability is provided.

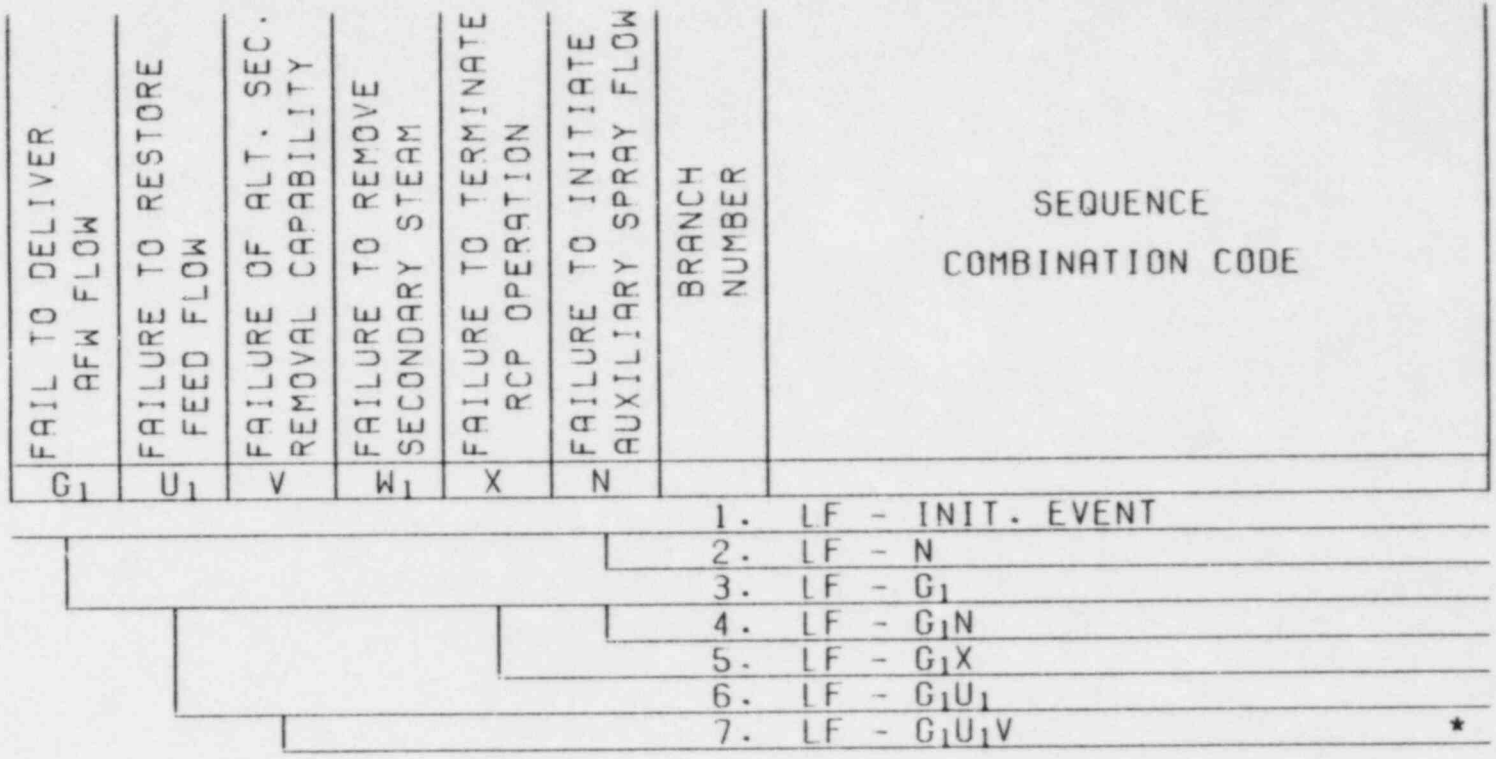


FIGURE 5.1.4.1-1

LOSS OF SECONDARY HEAT SINK SYSTEMIC EVENT TREE

*The above minimal core damage sequence is evaluated and discussed in Section 7.1.

Note: Any branches excluded from the above event tree have been eliminated due to logic rules or the frequency cut-off as discussed in Section 2.2.1.

LF The initiating event is defined as the frequency of loss of operating main feedwater flow from plant/reactor trip events and the probability of loss of the 5% MFW bypass flow. The frequency of the initiating event was determined by fault tree analysis in Section 6.10.

G_1 The failure probability of the Auxiliary Feedwater System was also determined by fault tree analysis presented in Section 6.11. The analysis models the failure to automatically deliver AFW flow. No operator action to start or restore AFW flow is included in the model. Recovery actions are addressed in a separate analysis (Section 6.17) and are based on the dominant AFW system cutsets.

U_1 Following the initiating event and loss of AFW flow, operator action will be directed towards restoration of AFW system. The operator has approximately 50 minutes to re-establish AFW flow before core damage conditions are unavoidable (28, Section 2.8). A task analysis was performed to determine the human error probability for failure to restore AFW in the 50 minute time period in Section 6.17.

V At 50 minutes following reactor trip, operating procedures will guide the operator to depressurize the secondary system and feed the steam generators directly with a condensate pump. This secondary heat sink is referred to as the Alternate Secondary Heat Removal Capability. The fault tree analysis is presented in Section 6.13. Note that the Alternate Secondary Heat Removal Capability (condensate system) is dependent upon offsite power. Use of this system will be implemented only after restoration of AFW fails.

W_1 Failure to remove secondary steam refers to the inability to release steam energy through the steam generators. Following a loss of feedwater event, steam generated in the steam generators may be conveyed directly to the condenser via the TBVs or directly released to the atmosphere by the ADVs or MSSVs. Failure to remove secondary steam is equivalent to a loss of heat sink in this analysis (See Section 6.9).

X Per Combustion Engineering Emergency Procedure Guidelines (9), RCP operation is to be terminated upon indication of a total loss of feed flow event. Termination of pump operation results in natural circulation in the core and minimizes the heat added to the primary coolant by the pump operation.

N The pressurizer auxiliary sprays are used to depressurize the primary side. Due to failure of the auxiliary sprays, the primary pressure criteria for shutdown cooling entry conditions is not achieved. This results in a stable core configuration with a long term demand on the safety function, RCS Heat Removal. The fault tree analysis for Fail to Initiate Auxiliary Spray Flow is presented in Section 6.2.

5.1.4.2 Loss of Secondary Heat Sink with Feed and Bleed Operation Event Tree

The Loss of Secondary Heat Sink with Feed Bleed Operation Event Tree is presented in Figure 5.1.4.2-1. The safety function, RCS Heat Removal, is provided by the Auxiliary Feedwater System, Restoration of Feed Flow, Secondary Steam Removal and direct RCS heat removal by primary Feed and Bleed Operation. The safety function Core Heat Removal refers to termination of RCP operation. The safety function, RCS Pressure Control, is provided directly by PORV operation (Refer to Table 5.1.3-1).

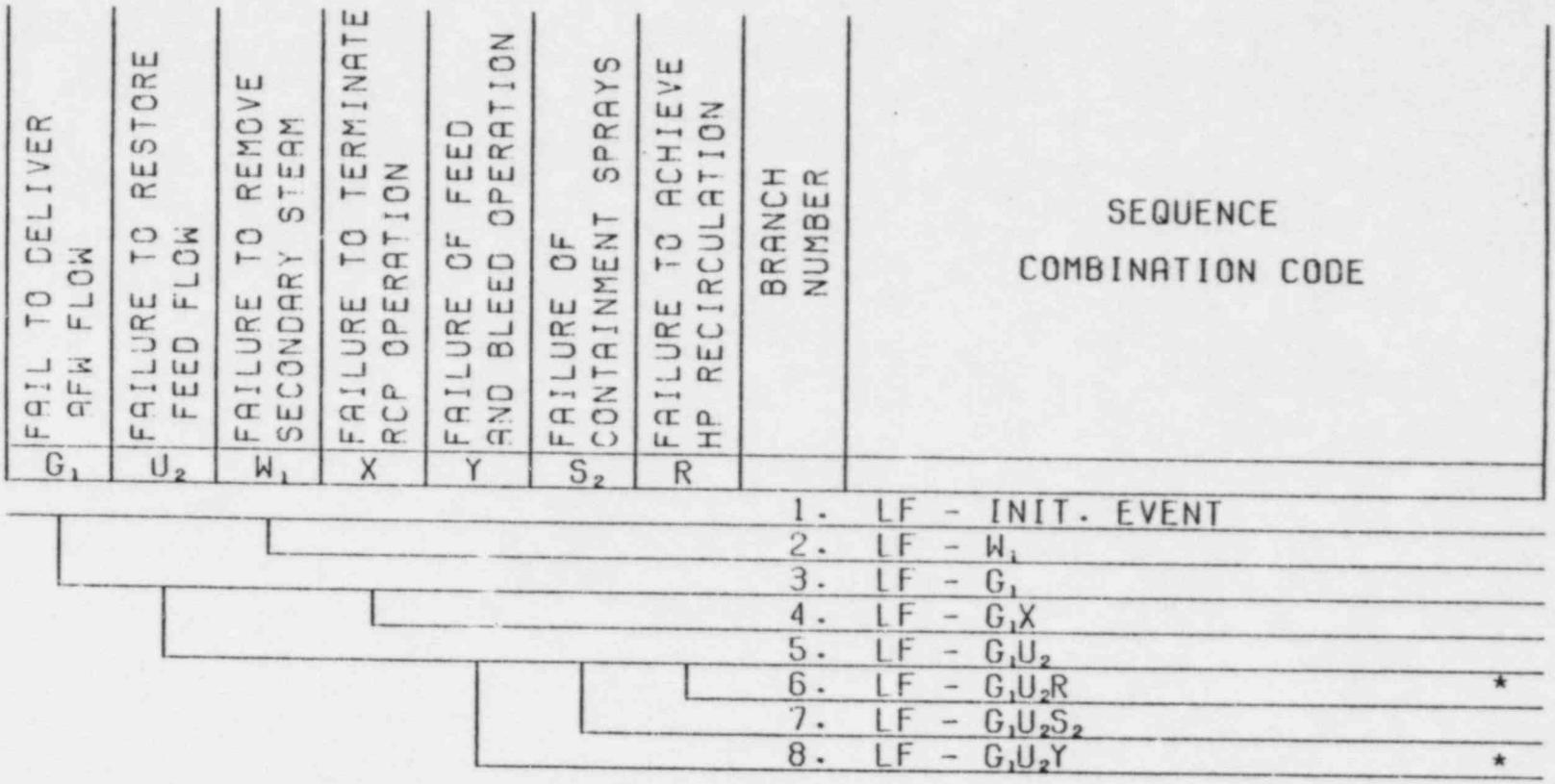


FIGURE 5.1.4.2-1

LOSS OF SECONDARY HEAT SINK WITH FEED AND BLEED OPERATION
SYSTEMIC EVENT TREE

*The above minimal core damage sequences are evaluated and discussed in Section 7.1.

Note: Any branches excluded from the above event tree have been eliminated due to logic rules or the frequency cut-off as discussed in Section 2.2.1.

Feed and Bleed Operation, in addition to establishing flow through PORVs and providing the associated makeup flow, requires the establishment of High Pressure (HP) Recirculation flow. The discharge of primary coolant into containment via the PORVs is conservatively assumed to result in the automatic initiation of the containment sprays. Containment spray pumps and the HPSI System initially utilize the same source of water, the Refueling Water Tanks (RWTs). Upon depletion of RWT inventory, HP pump suction will automatically switch to the containment sump and enter the recirculation mode of operation. It is assumed that shutdown cooling entry conditions will be achieved following successful feed and bleed operation.

The event tree accident sequences were filtered using a cutoff frequency of 10^{-9} per year in order to add visibility to certain sequences. The core damage sequences are discussed in Section 7.1.2. The branch headings are defined in Table 5.1.3-1 and are discussed below:

LF Initiating Event - same as Section 5.1.4.1.

G_1 Failure to Deliver Auxiliary Feed Flow - See discussion for Branch G_1 in Section 5.1.4.1.

U_2 Following the initiating event and loss of auxiliary feed flow, operator action will be directed towards restoration of Auxiliary Feedwater System. However, at 20 minutes following the reactor trip event, the operator is assumed to commence primary feed and bleed operation by opening the power-operated relief valves (PORVs) (28, Section 2.8). Once feed and bleed operation is initiated, the operator will terminate restoration actions and use the direct RCS heat removal system. The restoration task analysis presented in Section 6.17 therefore allowed only 20 minutes for restoration actions.

W_1 Failure to Remove Secondary Steam - See discussion for Branch W_1 in Section 5.1.4.1.

X Failure to Terminate RCP Operation - See discussion for Branch X in Section 5.1.4.1.

Y The failure probability for the primary Feed and Bleed System was determined by fault tree analysis in Section 6.5. The successful initiation of Feed and Bleed flow at 20 minutes, opening of both PORV trains and providing the required primary inventory makeup, result in acceptable core conditions, i.e. peak cladding temperatures less than 2200°F. (28, Section 2.8). Note that the Feed and Bleed System design employed in the analysis, is not redundant; both PORV trains are required for successful operation.

S_2 Failure of the containment sprays to deliver flow to containment results in a larger RWT inventory for feed and bleed operation. If containment sprays are not actuated, the RWT inventory is sufficient for continued Feed and Bleed Operation until shutdown cooling entry conditions are reached. If containment sprays are actuated, Feed and Bleed Operation requires operation of the HP recirculation mode. Failure of containment cooling (containment sprays and fans) is investigated in the event tree analysis on PORV induced LOCA. (See Section 5.3)

R Failure to achieve high pressure recirculation refers to inability to provide flow to the RCS loops by at least one of two high pressure pumps that take suction from the containment sump. Additional information on high pressure recirculation and the fault tree results are provided in Section 6.1.

5.2 STEAM GENERATOR TUBE RUPTURE

5.2.1 Initiating Events

For this evaluation, a SGTR is defined as a tube leak or rupture whose maximum leak flowrate exceeds the capacity of the charging system. Four distinct initiating events focusing on SGTR were defined for input to the SGTR analysis. Each initiating event addresses a slightly different aspect of tube rupture and challenges the plant in a slightly different fashion. The four initiating events are defined as follows:

- Initiating event 1 is defined as one or more tube ruptures occurring in one steam generator. Offsite power is assumed to be available at the time of the initiating event.

- Initiating event 2 is defined as one or more tube ruptures occurring in one steam generator with a coincident loss of offsite power.

- Initiating event 3 is defined as one or more tube ruptures occurring in both steam generators. Offsite power is assumed to be available at the time of the initiating event.

- Initiating event 4 is defined as one or more tube ruptures occurring in both steam generators with a coincident loss of offsite power.

The procedure for determining SGTR initiating event frequencies and the calculated results are presented in Section 4.3.2.

5.2.2 Normal Sequence of Events

The normal sequence of events following a SGTR is similar for tube ruptures in one or two steam generators. For a SGTR in one steam generator, the affected SG is isolated and secondary cooldown is initiated and maintained from the unaffected steam generator. For tube ruptures in both steam

generators the most affected SG is isolated and cooldown is accomplished using the least affected SG. Table 5.2.2-1 presents the normal sequence of events for SGTR assuming offsite power is available at the time of the initiating event.

The normal sequence of events varies for the cases where offsite power is unavailable at the time of the initiating event. In this instance the initiating event will be defined as tube rupture(s) in one or two SGs with a coincident loss of offsite power. The normal sequence of events is presented in Table 5.2.2-2.

5.2.3 Functional Event Tree

The SGTR functional event tree, presented in Figure 5.2.3-1, was developed to determine the functional accident sequences that could lead to potential core damage. The functional event tree was developed for the current plant design and for the plant design assuming PORVs were installed. As depicted in Table 5.2.3-1, each safety function can be defined in terms of functional elements which are used as intermediaries to correlate the five anti-core melt safety functions (32) to the specific plant systems or actions required to mitigate a SGTR. The list of associated actions provides the logical groundwork for constructing a system/action level event tree which can be used to generate more detailed accident scenarios.

The following functional accident sequences were obtained from the SGTR functional event tree:

Sequence 1 — Sequence 1 represents the initiating event, steam generator tube rupture. For this case, all safety functions are maintained and the core is protected.

TABLE 5.2.2-1

NORMAL SEQUENCE OF EVENTS FOR SGTR

1. Reactor/Turbine Trip.

2. SBCS Quick Open of TBVs - TBVs reclose.

3. SIAS on Low Pressurizer Pressure.

4. Operator initiates cooldown by manually operating the Turbine Bypass System in conjunction with either Main Feedwater or Auxiliary Feedwater.

5. At $T_{HOT} \leq 535°F$ the operator isolates the affected or most affected steam generator and continues cooling with the unaffected or least affected SG.

6. Auxiliary Spray is initiated to commence RCS depressurization. [1] (PORVs could be used if the Auxiliary Spray System was unavailable).

7. Throttle HPSI Flow to prevent repressurization.

8. If necessary, blowdown can be initiated from the isolated SG to prevent overfilling.

9. When condenser vacuum can no longer be maintained, cooldown continues by establishing flow from the ADV on the unaffected or least affected SG.

10. Shutdown cooling entry conditions achieved.

[1] PORVs are not included in the current plant design.

TABLE 5.2.2-2

NORMAL SEQUENCE OF EVENTS FOR SGTR WITH COINCIDENT LOOP

1. Reactor/Turbine Trip.
2. MSSVs automatically open and reclose.
3. SIAS is generated on Low Pressurizer Pressure.
4. Cooldown is initiated by operation of the Atmospheric Dump System in conjunction with the Auxiliary Feedwater System.
5. At $T_{HOT} \leq 535°F$ the operator isolates the affected or most affected SG and continues cooling with the unaffected or least affected SG.
6. Auxiliary Spray is initiated to commence RCS depressurization. (PORVs could be used if the Auxiliary Spray System was unavailable).[1]
7. Throttle HPSI flow to prevent repressurization.
8. Continue cooling using the ADV on the unaffected or least affected SG.
9. Shutdown cooling entry conditions achieved.

[1] PORVs are not included in the current plant design.

FIGURE 5.2.3-1

SGTR FUNCTIONAL EVENT TREE

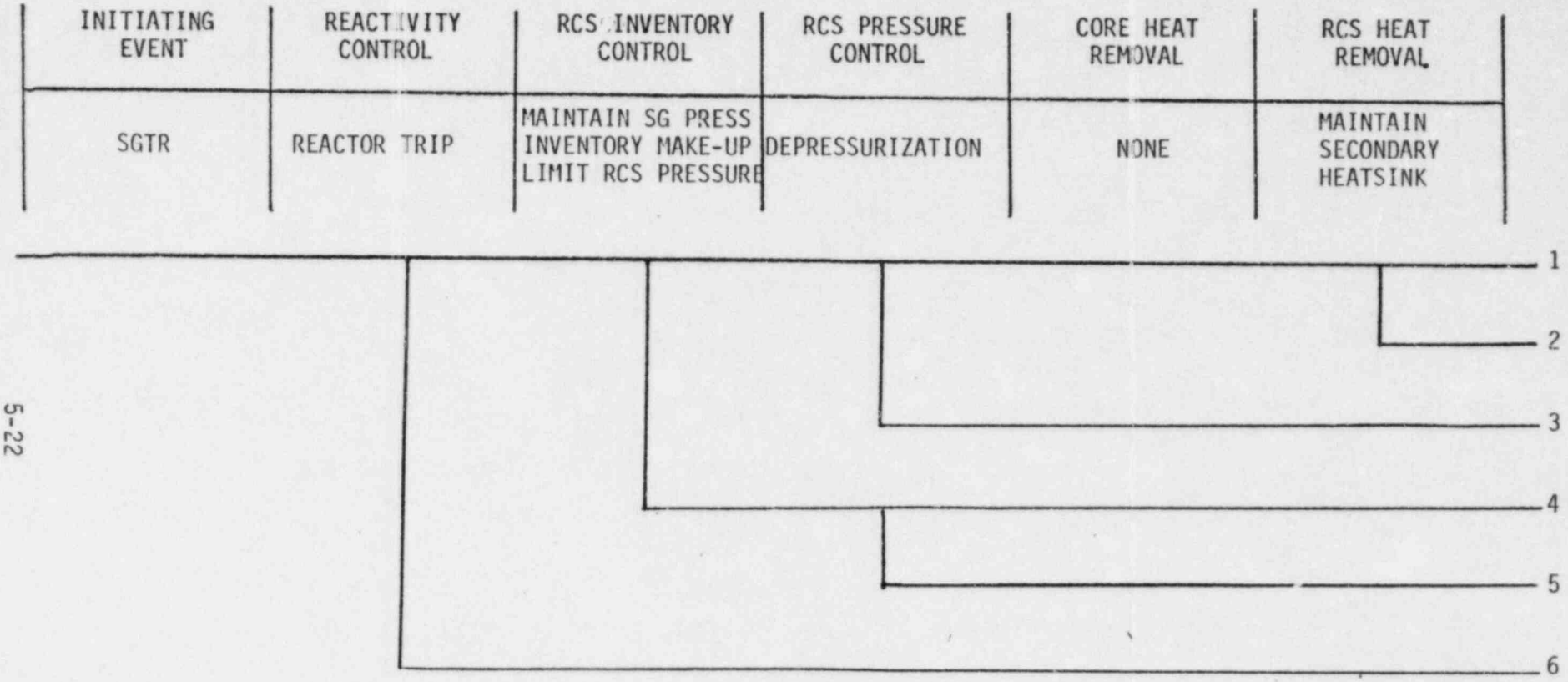


TABLE 5.2.3-1

SGTR FUNCTIONAL EVENT TREE CONSIDERATIONS

SAFETY FUNCTION	FUNCTIONAL ELEMENTS	ASSOCIATED SYSTEMS/ACTIONS
Reactivity Control	Reactor Trip	Reactor Trip[1]
RCS Inventory Control	Inventory Makeup	High Pressure Safety Injection
	Maintain SG Pressure	Trip Turbine Reclose Normally Opening Secondary Steam Valves Prevent Unnecessary Opening of Secondary Steam Valves
	Limit RCS Pressure	Throttle HPSI
RCS Pressure Control	Depressurization	Auxiliary Sprays PORVS
Core Heat Removal	None	There are no specific systems/actions required for Core Heat Removal except through RCS Inventory Control
RCS Heat Removal	Maintain Secondary Heat Sink	Loss of Secondary Heat Sink is addressed in Section 5.1

[1] ATWS will not be considered in the scope of this evaluation

Sequence 2 — Sequence 2 consists of a SGTR with a coincident loss of secondary heat sink (LOHS). Since the transient and long term effects of a loss of secondary heat sink are rigorously addressed in Section 5.1, it was felt that evaluating the consequences of a SGTR with a coincident LOHS would not yield any new information. Therefore, LOHS is considered to be outside the scope of this evaluation.

Sequence 3 — Failure to depressurize the RCS could lead to a large integrated leak flow. If all other safety functions are maintained, shutdown cooling entry conditions should still be achieved.

Sequence 4 — Sequence 4 is best discussed in terms of the SGTR functional elements that define RCS inventory control.

- Inventory Make-Up: If depleting RCS inventory is not replenished, the core will eventually uncover.
- Maintain SG Pressure: If SG pressure is not maintained, the pressure differential between the primary and secondary side can lead to a high integrated leak flow. Core damage will result if the total volume of the leak flow exceeds the long term capacity of the RWT.
- Limit RCS Pressure: HPSI flow should be throttled during RCS cooldown to limit RCS pressure and prevent a large integrated leak flow. Failure to throttle HPSI can lead to SG overfill provided the blowdown system is unavailable for draining. SG overfill can result in unnecessary openings of the ADVs or MSSVs.

Sequence 5 — Failure to depressurize the RCS combined with any of the functional elements in sequence 4 will increase the leak flow rate and, if applicable, hasten the time to core uncovery.

Sequence 6 As discussed in Section 2.2.1.1, ATWS is not considered in the scope of this program.

5.2.4 Systemic Event Trees

The system/action level event trees for SGTR were developed by expanding the associated systems/actions list presented in Table 5.2.3-1 to include the various secondary valves and the failure mechanisms that could lead to unnecessary valve openings. A separate event tree was constructed for each of the four SGTR initiating events defined in Section 5.2.1. It was felt that a complete re-evaluation of each SGTR event tree, assuming PORVs were installed (i.e. including an extra branch in each event tree to model the PORVs), would not provide any new information for the following reasons:

- PORV LOCA following SGTR is addressed in Section 5.3.4.2.

- The assumed role of PORVs in SGTR events is to provide backup RCS depressurization capability should the Auxiliary Spray System be unavailable. (It should be noted that the Auxiliary Spray System provides a safety related capability for depressurization.) The results of the SGTR event tree analysis (assuming no PORVs are installed) do not indicate the Auxiliary Spray System to be a significant contributor to the SGTR core damage frequencies, therefore, the impact of PORVs on SGTR core damage frequency is assumed to be negligable. This assumption is supported by a quantitative discussion of the use of PORVs as a backup to the Auxiliary Spray System in Section 7.2.5.

- Re-evaluating each SGTR event tree with a extra branch to model PORV depressurization capability would unnecessarily increase the sizes of the event trees (and therefore the required computer time) without generating any new core damage sequences, i.e. any core damage sequence including the PORVs would be filtered out on low frequency.

Table 5.2.4-1 defines the event tree branches and associated failure criteria that are used as input to the four event trees. Fault tree results for each branch are presented in Section 6.0.

5.2.4.1 SGTR in One SG Event Tree

The SGTR in One SG Event Tree is presented in Figure 5.2.4.1-1. The safety function, RCS Inventory Control, is provided by the following actions:

- Delivery of High Pressure Safety Injection
- Turbine Trip
- Successful Operation of Normally Opening Secondary Steam Valves
- Prevention of Unnecessary Openings of Secondary Steam Valves
- Throttling of High Pressure Safety Injection

The safety function, RCS Pressure Control, is provided by the Auxiliary Spray System. If the Auxiliary Spray System was unavailable PORVs could provide back-up depressurization capability. (See Section 7.2.5.) PORVs are not included in the current plant design.

For this event tree the accident sequences were filtered using a frequency cutoff of 10^{-8} per year. The scenarios that lead to potential core damage are presented in Section 7.2.1. The event tree branches used to construct the event tree, SGTR in One SG, are discussed below.

T_1 The initiating event is defined as one or more tube ruptures in steam generator SG-088 with offsite power available at the time of the initiating event. The initiating event frequency is calculated in Section 4.3.2.

TABLE 5.2.4-1

SGTR EVENT TREE BRANCH DEFINITIONS

Branch Designation	Branch Title	Failure Criteria
T1	Initiating Event	SGTR in one SG
T2		SGTR in one SG with coincident LOOP
T3		SGTR in two SGs
T4		SGTR in two SGs with coincident LOOP
A	Fail to Deliver Sufficient HPSI Flow	Failure to deliver flow from 1 of 3 HPSI pumps to the RCS on SIAS and failure to maintain sufficient HPSI flow (A').
B	Turbine Fails to Trip on Reactor Trip	Failure to completely terminate steam flow to the high pressure turbine on reactor trip.
C_1	Turbine Bypass Valves Fail to Quick Open	4 of 4 TBVs fail to quick open following turbine trip.
D	Turbine Bypass Valve Fails to Reclose	1 of 4 TBVs fails to reclose following quick open or during cooldown.
E_1	MSIV on Affected (or Most Affected) SG Fails to Close	The MSIV on the affected SG fails to close on MSIS.
F_1	Loss of TBV Flow Prior to Isolation of the Affected (or Most Affected) SG	Termination of TBV flow prior to isolation of the affected SG
F_2	Loss of TBV Flow After Isolation of the Affected (or Most Affected) SG	Termination of TBV flow after isolation of the affected SG
H	ADV on Unaffected (or Least Affected) SG Fails to Close	Failure to terminate ADV flow on the unaffected SG
I_1	MSSV on Unaffected (or Least Affected) SG Fails to Reclose	One MSSV on the unaffected SG fails to reseat or reclose

TABLE 5.2.4-1
(continued)
SGTR EVENT TREE BRANCH DEFINITIONS

Branch Designation	Branch Title	Failure Criteria
J	ADV on Unaffected (or Least Affected) SG Unavailable	Failure to initiate steam flow through the ADV on the unaffected SG.
K	ADV on Affected (or Most Affected) SG Unavailable	Failure to initiate steam flow through the ADV on the affected SG.
L	ADV on Affected (or Most Affected) SG Fails to Close	Failure to terminate ADV flow on the affected SG.
M	MSSV on Affected (or Most Affected) SG Fails to Reclose	One MSSV on the affected SG fails to reseat or reclose.
N	Fail to Initiate Auxiliary Spray flow[1]	Failure to deliver auxiliary spray flow from 1 of 3 charging pumps to the pressurizer.
O	Fail to Throttle HPSI	The operator fails to throttle HPSI flow.
P_1	Excess Feedwater to Affected (or Most Affected) SG	Excess AFW flow to the affected or most affected SG.
Q_1	Fail to Initiate Blowdown from the Affected SG	Fail to initiate blowdown from the affected SG.
I_2	MSSV on Least Affected SG Fails to Close on Turbine Trip	One MSSV on the least affected SG fails to reclose following turbine trip.
M_2	MSSV on Most Affected SG Fails to Close on Turbine Trip	One MSSV on the most affected SG fails to reclose following turbine trip.

1 The use of PORVs as a backup to the Auxiliary Spray System will be addressed in Section 7.2.5.

TABLE 5.2.4-1
(continued)
SGTR EVENT TREE BRANCH DEFINITIONS

Branch Designation	Branch Title	Failure Criteria
E_2	MSIV on Least Affected SG Fails to Close	The MSIV on the least affected SG fail to close on MSIS.
Q_2	No blowdown from Most Affected SG	Blowdown isolation valve on most affected SG fails to open.
Q_3	No Blowdown from Least Affected SG	Blowdown isolation valve on least affected SG fails to open.
Q_4	Fail to Initiate Blowdown	Failure to initiate blowdown from both steam generators.
P_2	Excess Feedwater to Least Affected SG	Excess AFW flow to the least affected SG.
P_3	Excess Feedwater to Least Affected SG	Excess MFW or AFW flow to least affected SG.

A Failure to Deliver Sufficient HPSI flow refers to the delivery of one pump flow to two RCS loops. The fault tree analysis for Failure to Deliver Sufficient HPSI flow (assuming offsite power is available at the time of the initiating event) is presented in Section 6.1.

B Failure of the Turbine to Trip on reactor trip refers to one flowpath through the turbine remaining open long enough to generate a MSIS on low SG pressure. If the MSIV on the affected SG fails to close, uncontrolled SG blowdown will occur through the turbine. If the MSIV closes successfully, the sudden termination in steam flow will result in a challenge to one MSSV on the affected SG. The probability for Failure to Trip the Turbine is presented in Section 6.6.4.

C_1 The TBVs normally quick open following turbine trip to prevent unnecessary opening of the MSSVs. Should the TBVs fail to quick open, a combination of MSSVs with steam flow capacity equal to that of the TBVs will open to relieve SG pressure. The fault tree analysis for TBVs Fail to Quick Open is presented in Section 6.6.

D Failure of one TBV to reclose following quick open or during cooldown prior to isolation of the affected SG will result in generation of a MSIS. Should the MSIV on the affected SG fail to close, uncontrolled SG blowdown will occur through the Turbine Bypass System. If the MSIV closes successfully, the sudden termination in steam flow will result in a challenge to one MSSV on the affected SG. The fault tree analysis for One TBV Fails to Reclose is presented in Section 6.6.

E_1 MSIV on Affected SG Fails to Close refers to the MSIV on SG-088 failing to close on MSIS. The fault tree analysis for MSIV on SG-088 Fails to Close is presented in Section 6.7.

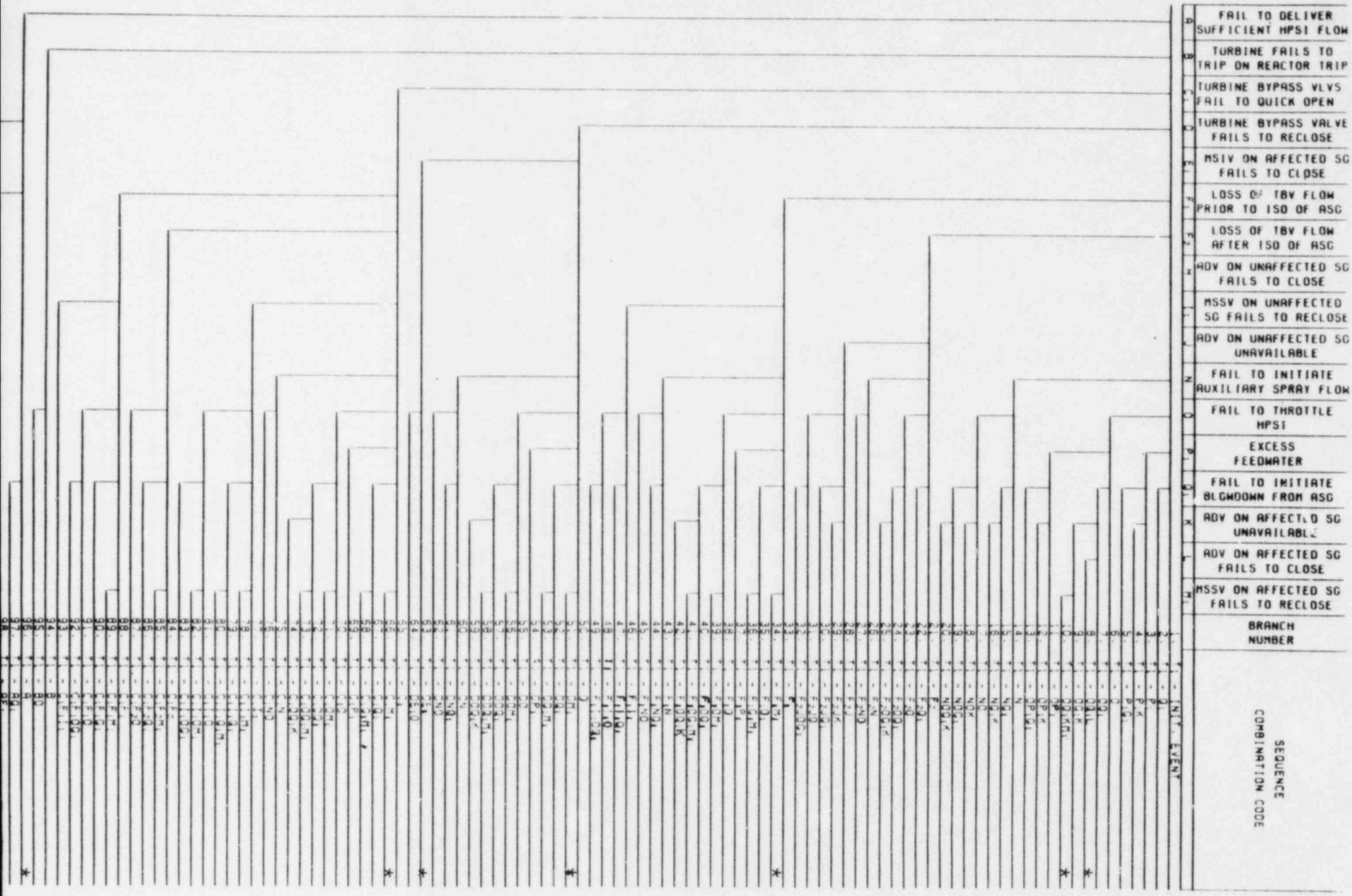

FAIL TO DELIVER SUFFICIENT HPSI FLOW
TURBINE FAILS TO TRIP ON REACTOR TRIP
TURBINE BYPASS VLVS FAIL TO QUICK OPEN
TURBINE BYPASS VALVE FAILS TO RECLOSE
MSIV ON AFFECTED SG FAILS TO CLOSE
LOSS OF TBV FLOW PRIOR TO ISO OF ASG
LOSS OF TBV FLOW AFTER ISO OF ASG
ADV ON UNAFFECTED SG FAILS TO CLOSE
MSSV ON UNAFFECTED SG FAILS TO RECLOSE
ADV ON UNAFFECTED SG UNAVAILABLE
FAIL TO INITIATE AUXILIARY SPRAY FLOW
FAIL TO THROTTLE HPSI
EXCESS FEEDWATER
FAIL TO INITIATE BLOWDOWN FROM ASG
ADV ON AFFECTED SG UNAVAILABLE
ADV ON AFFECTED SG FAILS TO CLOSE
MSSV ON AFFECTED SG FAILS TO RECLOSE
BRANCH NUMBER
COMBINATION CODE
SEQUENCE

FIGURE 5.2.4.1-1

SGTR IN ONE SG SYSTEMIC EVENT TREE

*The above minimal core damage sequences are evaluated and discussed in Section 7.2.

Note: Any branches excluded from the above event tree have been eliminated due to logic rules or the frequency cut-off as discussed in Section 2.2.1.

F_1 Loss of turbine bypass flow prior to isolation of the affected SG will result in a challenge to one MSSV associated with the affected SG. The fault tree analysis is presented in Section 6.6.

F_2 Loss of turbine bypass flow after isolation of the affected SG will eventually result in a challenge to one MSSV associated with the unaffected SG. This is based on the assumption that the isolated SG is in a relatively steady state condition while the sudden termination of steam flow from the unaffected SG results in an upward pressure transient. If the ADV on the unaffected SG is unavailable (e.g. the operator fails to open the ADV), one MSSV on the unaffected SG will open. The fault tree analysis for Loss of TBV Flow After Isolation of the Affected SG is presented in Section 6.6.

H ADV on Unaffected SG Fails to Close refers to the ADV associated with SG-089 failing to close after being manually opened following a turbine bypass system failure after isolation of the affected SG. The failed open ADV results in a MSIS, however, the MSIS would have no impact on the isolated SG. The fault tree analysis for ADV on SG-089 Fails to Close is presented in Section 6.8.

I_1 MSSV on Unaffected SG Fails to Reclose refers to one MSSV on SG-089 failing to close after being challenged on turbine trip (following a TBS failure) or following a failure of the associated ADV to open. Five MSSVs are assumed to open on SG-089 if the TBVs fail to quick open. If the ADV is unavailable when required, one MSSV will open. The fault tree analysis is presented in Section 6.9.

J ADV on Unaffected SG Unavailable refers to the ADV associated with SG-089 failing to open (e.g., operator fails to open ADV) in response to a TBS failure following isolation of the affected SG. The fault tree analysis is presented in Section 6.8.

K ADV on Affected SG Unavailable refers to the ADV on SG-088 failing to open (e.g., operator fails to open ADV) in response to SG overfill conditions. The fault tree analysis is presented in Section 6.8.

L ADV on Affected SG Fails to Close refers to the ADV on SG-088 failing to close after being manually opened following a SG overfill. A failed open ADV on the affected SG results in a direct flowpath for RCS inventory from the primary system to the atmosphere (outside containment LOCA). The fault tree analysis for ADV on SG-088 Fails to Close is presented in Section 6.8.

M_1 MSSV on Affected SG Fails to Reclose refers to one MSSV on SG-088 failing to close after being challenged by a failure of the TBVs to quick open or a failure of the ADV on the affected SG to open. Five MSSVs are assumed to open on SG-088 if the TBVs fail to quick open. If the ADV is unavailable when required, one MSSV will open. A failed open MSSV on the affected SG results in an outside containment LOCA. The fault tree analysis is presented in Section 6.9.

N Failure to Initiate Auxiliary Spray Flow results in a high primary to secondary pressure ratio which leads to a large integrated leak flow. The failure to deliver auxiliary spray in conjunction with the failure to initiate blowdown from the affected SG results in SG overfill and a challenge to the ADV. The fault tree analysis for Fail to Initiate Auxiliary Spray Flow (assuming offsite power is available at the time of the initiating event) is presented in Section 6.2.

O Fail to Throttle HPSI refers to maintaining a relatively high RCS pressure through continued delivery of safety injection near the shutoff head. Failure to Throttle HPSI in conjunction with the failure to initiate blowdown from the affected SG results in SG overfill and a challenge to the ADV. The probability for Fail to Throttle HPSI is presented in Section 6.1.

P_1 Excess feedwater refers to uncontrolled delivery of auxiliary feedwater to SG-088. Excess feedwater in conjunction with failure to initiate blowdown from the affected SG results in SG overfill and a challenge to the ADV. The fault tree analysis is presented in Section 6.11.

Q_1 Fail to Initiate Blowdown from the Affected SG refers to failing to initiate blowdown flow from SG-088. The fault tree analysis is presented in Section 6.12.

5.2.4.2 SGTR in One SG with Coincident LOOP Event Tree

The SGTR in One SG with Coincident Loss of Offsite Power event tree is presented in Figure 5.2.4.2-1. The safety functions are provided by the systems/actions listed in Section 5.2.4.1. For this event tree the accident sequences were filtered using a frequency cutoff of 10^{-10} per year. Because the initiating event frequency includes the probability of loss of offsite power, it was felt that a cutoff frequency of 10^{-10} per year rather than 10^{-8}per year would provide increased visibility of the significance of the output scenarios obtained from the event tree. The scenarios that lead to potential core damage are presented in Section 7.2.2. The event tree branches used to construct the event tree, SGTR in One SG with Coincident LOOP, are discussed below.

T2 The initiating event is defined as one or more tube ruptures in SG-088 with a coincident loss of offsite power on turbine trip. The initiating event frequency is calculated in Section 4.3.2. It should be noted that for SONGS a loss of offsite power results in loss of the Turbine Bypass System and loss of the Blowdown Processing System.

A Failure to Deliver Sufficient HPSI Flow refers to the delivery of one pump flow to two RCS loops. When offsite power is unavailable, the unreliability of the HPSI system becomes a significant contributor (>10%) to the overall system failure

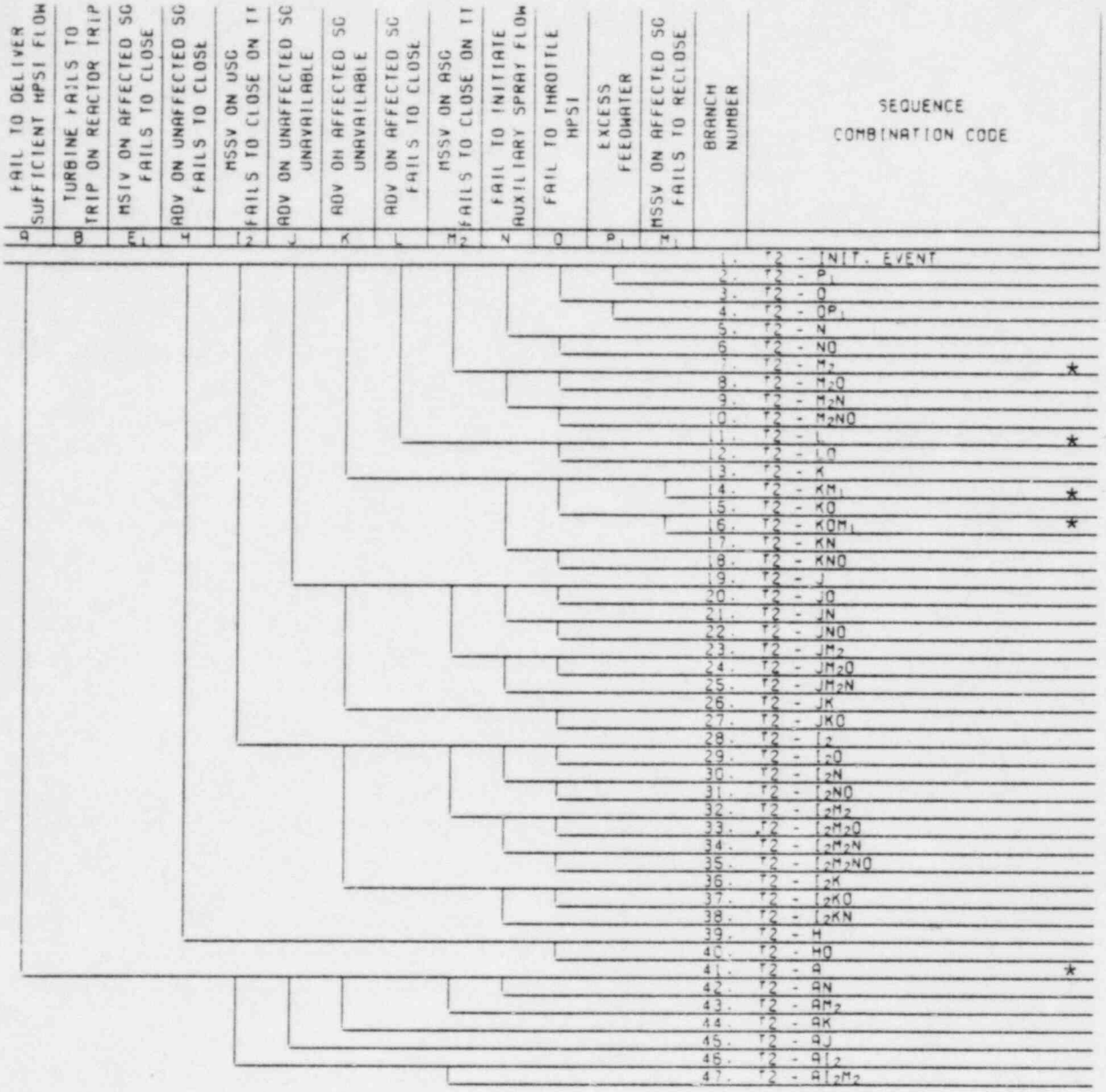


FIGURE 5.2.4.2-1

SGTR IN ONE SG WITH COINCIDENT LOOP SYSTEMIC EVENT TREE

*The above minimal core damage sequences are evaluated and discussed in Section 7.2.

Note: Any branches excluded from the above event tree have been eliminated due to logic rules or the frequency cut-off as discussed in Section 2.2.1.

probability. Branch A can actually be separated into two distinct failure modes; failure of the system to supply sufficient flow on SIAS and failure of the system to maintain flow. Although the event tree only includes one input branch for the HPSI system, separate uncertainty analyses were performed on the unavailability and the unreliability. Failure of the HPSI system to maintain flow is defined by branch A' in the scenarios presented in Section 7.2.2. The fault tree analysis for Failure to Deliver Sufficient HPSI flow (assuming offsite power is unavailable) is presented in Section 6.1.

B Turbine Fails to Trip on Reactor Trip. See discussion for branch B in Section 5.2.4.1.

E_1 MSIV on Affected SG Fails to Close. See discussion for branch E_1 in Section 5.2.4.1.

H ADV on Unaffected SG Fails to Close. For this event tree, the ADVs are opened by the operator to initiate cooldown. A failed open ADV on SG-089 results in a MSIS. The fault tree analysis for ADV on SG-089 Fails to Close is presented in Section 6.8.

I_2 MSSV on Unaffected SG Fails to Close on Turbine Trip refers to one MSSV on SG-089 failing to close on turbine trip. Five MSSVs are assumed to open on SG-089 following turbine trip. A subsequently failed open MSSV results in a MSIS. The fault tree analysis is presented in Section 6.9.

J ADV on Unaffected SG Unavailable refers to the ADV associated with SG-089 failing to open (e.g., operator fails to open ADV) when required i.e., initiation of cooldown or following an MSIS to prevent a MSSV from opening. The fault tree analysis for ADV on SG-089 Fails to Open is presented in Section 6.8.

K ADV on Affected SG Unavailable refers to the ADV on SG-088 failing to open (e.g. operator fails to open ADV) in response to a challenge i.e., initiation of cooldown, MSIS, or SG overfill. The fault tree analysis is presented in Section 6.8.

L ADV on Affected SG Fails to Close refers to the ADV on SG-088 failing to close after being manually opened. A failed open ADV on the affected SG results in a direct flowpath for RCS inventory from the primary system to the atmosphere (outside containment LOCA). The fault tree analysis is presented in Section 6.8.

M_2 MSSV on affected SG Fails to Close on Turbine Trip refers to one MSSV on SG-088 failing to close on turbine trip. Five MSSVs are assumed to open on SG-088. For this event tree, branch M_1, as defined in Section 5.2.4.1, is separated into branches M_1 and M_2. The separation of these branches simplifies the logical construction of the event tree, i.e. branch M_2 represents the case where the MSSVs open on turbine trip and branch M_1 represents all other cases where one MSSV opens only if the associated ADV is unavailable. The fault tree analysis is presented in Section 6.9.

M_1 MSSV on Affected SG Fails to Reclose refers to one MSSV associated with SG-088 failing to close after being challenged by a failure of the ADV associated with SG-088 to open due to initiation of cooldown, MSIS or SG overfill. A failed open MSSV on the affected SG results in an outside containment LOCA. The fault tree analysis is presented in Section 6.9.

N Fail to Initiate Auxiliary Spray Flow. See discussion for branch N in Section 5.2.4.1. Since the blowdown system is unavailable, failure to initiate auxiliary spray will result in SG overfill. The fault tree analysis for Fail to Initiate Auxiliary Spray Flow (assuming offsite power is unavailable) is presented in Section 6.2.

0 Fail to Throttle HPSI. See discussion for branch 0 in Section 5.2.4.1. Since the blowdown system is unavailable, failure to throttle HPSI will result in SG overfill.

P_1 Excess Feedwater. See discussion for branch P_1 in Section 5.2.4.1. Since the blowdown system is unavailable, excess feedwater will result in SG overfill.

5.2.4.3 SGTR in Two Steam Generators Event Tree

The SGTR in Two Steam Generators Event Tree is presented in Figure 5.2.4.3-1. The safety functions are provided by the systems/actions listed in Section 5.2.4.1. For this event tree the accident sequences were filtered using a frequency cutoff of 10^{-8} per year. The scenarios that lead to potential core damage are presented in Section 7.2.3. The event tree model includes the assumption that the operator will be able to define a most affected and a least affected SG. He will isolate the most affected SG and cooldown the plant with the least affected SG. The event tree branches used to construct the event tree, SGTR in Two Steam Generators, are discussed below.

T3 The initiating event is defined as one or more tube ruptures in both steam generators with offsite power available at the time of the initiating event. The initiating event frequency is calculated in Section 4.3.2.

A Fail to Deliver Sufficient HPSI. See discussion for branch A in Section 5.2.4.1.

B Failure of the turbine to trip on reactor trip refers to one flowpath through the turbine remaining open long enough to generate a MSIS on low SG pressure. If the MSIV on either the most affected or least affected SG fails to close, uncontrolled SG blowdown will occur through the turbine. If both MSIVs close

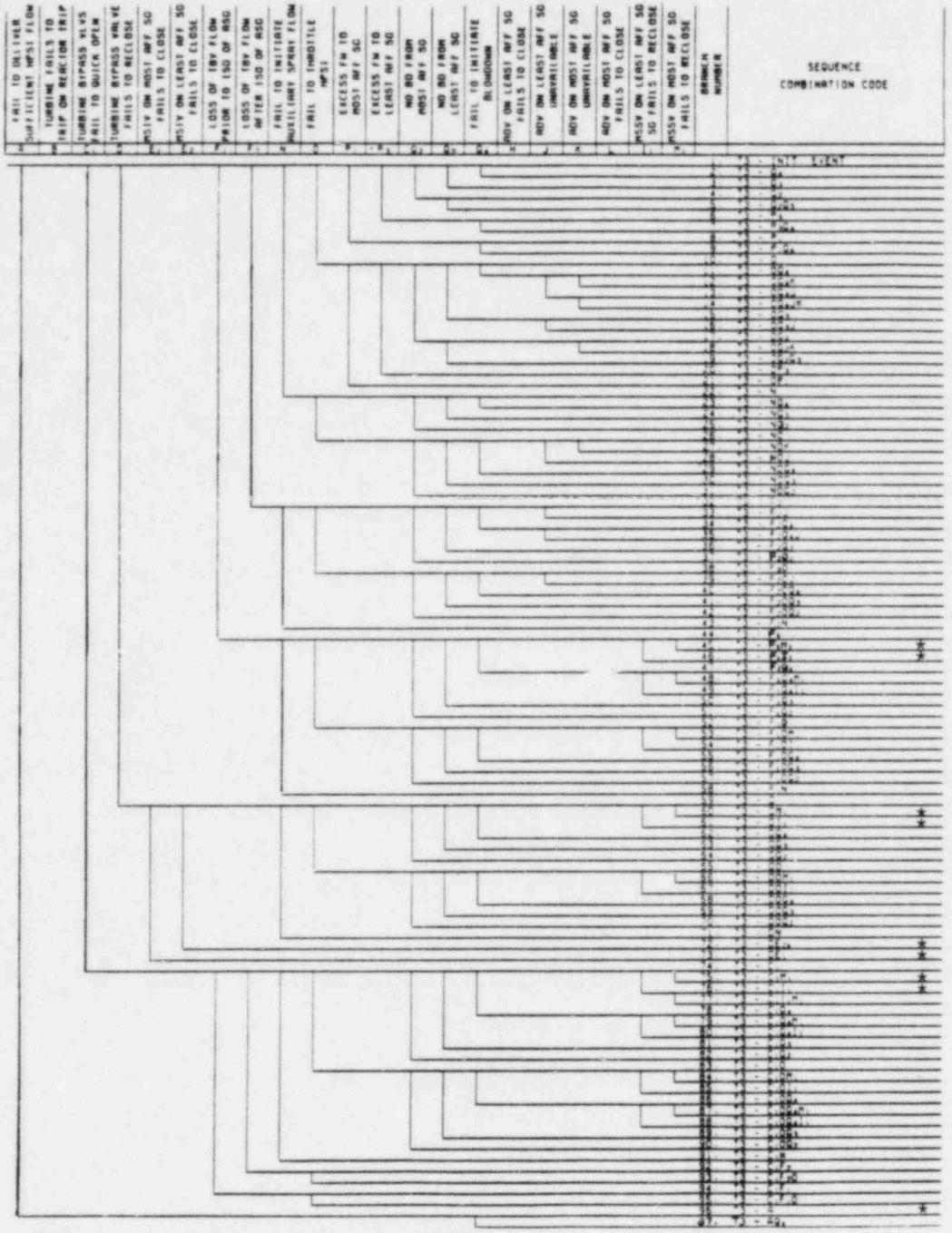


FIGURE 5.2.4.3-1

SGTR IN TWO SGs SYSTEMIC EVENT TREE

*The above minimal core damage sequences are evaluated and discussed in Section 7.2.

Note: Any branches excluded from the above event tree have been eliminated due to logic rules or the frequency cut-off as discussed in Section 2.2.1.

successfully, the sudden termination in steam flow will result in a challenge to one MSSV on the most and least affected steam generators. The probability for Failure to Trip the Turbine is presented in Section 6.6.4.

C_1 TBVs Fail to Quick Open. See discussion for branch C_1 in Section 5.2.4.1.

D Failure of One TBV to reclose following quick open or during cooldown prior to isolation of the most affected SG will result in generation of a MSIS. Should either MSIV fail to close, uncontrolled SG blowdown will occur through the Turbine Bypass System. If both MSIVs close successfully, the sudden termination in steam flow will result in a challenge to one MSSV on each SG. The fault tree analysis is presented in Section 6.6.

E_1 MSIV on Most Affected SG Fails to Close. See discussion for branch E_1 in Section 5.2.4.1.

E_2 MSIV on Least Affected SG Fails to Close refers to the MSIV on SG-089 failing to close on MSIS. The fault tree analysis is presented in Section 6.7.

F_1 Loss of turbine bypass flow prior to isolation of the most affected SG will result in a challenge to one MSSV on each SG. The fault tree analysis is presented in Section 6.6.

F_2 Loss of turbine bypass flow after isolation of the most affected SG will eventually result in a challenge to one MSSV associated with the least affected SG. This is based on the assumption that the isolated SG is in a relatively steady state condition while the sudden termination in steam flow from the least affected SG results in an upward pressure transient. The

ADV on the least affected SG could be opened by the operator (to prevent the MSSV from opening) and fail to close, or if it was unavailable, one MSSV on the least affected SG would open. The fault tree analysis is presented in Section 6.6.

H ADV on Least Affected SG Fails to Close refers to the ADV associated with SG-089 failing to close after being manually opened following a TBS failure or SG overfill. A failed open ADV on the least affected SG results in a direct flowpath for RCS inventory from the primary system to the atmosphere (outside containment LOCA). The fault tree analysis is presented in Section 6.8.

I_1 MSSV on Least Affected SG Fails to Reclose refers to one MSSV on SG-089 failing to close after being challenged by a failure of the TBVs to quick open or a failure of the ADV on the least affected SG to open. A failed open MSSV on the least affected SG results in an outside containment LOCA. The fault tree analysis is presented in Section 6.9.

J ADV on Least Affected SG Unavailable. See discussion for branch J in Section 5.2.4.1.

K ADV on Most Affected SG Unavailable. See discussion for branch K in Section 5.2.4.1.

L ADV on Most Affected SG Fails to Close. See discussion for branch L in Section 5.2.4.1.

M_1 MSSV on Most Affected SG Fails to Reclose. See discussion for branch M_1 in Section 5.2.4.1.

N Failure to Initiate Auxiliary Spray Flow results in a high primary to secondary pressure ratio which leads to a large integrated leak flow to both SGs. The failure to deliver auxiliary spray in conjunction with the failure to initiate

blowdown from either or both SGs results in SG overfill and challenges one or both ADVs. The fault tree analysis for Fail to Initiate Auxiliary Spray Flow (assuming offsite power is available at the time of the initiating event) is presented in Section 6.2.

O Fail to Throttle HPSI refers to maintaining a relatively high RCS pressure through continued delivery of safety injection near the shutoff head. Failure to throttle HPSI in conjunction with failure to initiate blowdown from either or both SGs results in SG overfill and challenges one or both ADVs. The probability for Fail to Throttle HPSI is presented in Section 6.1.

P_1 Excess Feedwater to the Most Affected SG. See discussion for branch P_1 in Section 5.2.4.1.

P_3 Excess Feedwater to the Least Affected SG refers to uncontrolled delivery of main feedwater or auxiliary feedwater to SG-089. Excess feedwater in conjunction with failure to initiate blowdown from SG-089 results in SG overfill and a challenge to the ADV on that SG. The fault tree analysis is presented in Section 6.11.

Q_2 No Blowdown from Most Affected SG refers to a loss of blowdown flow only from SG-088. (Blowdown can still be initiated from SG-089). This branch includes failure to open the blowdown isolation valve on SG-088. The fault tree analysis is presented in Section 6.12.

Q_3 No Blowdown from Least Affected SG refers to a loss of blowdown flow only from SG-089. (Blowdown can still be initiated from SG-088). This branch includes failure to open the blowdown isolation valve on SG-089. The fault tree analysis is presented in Section 6.12.

Q_4 Fail to Initiate Blowdown refers to the failure to initiate blowdown from both steam generators. This branch includes only the blowdown system failures which will result in a loss of the entire blowdown system. The fault tree analysis is presented in Section 6.12.

5.2.4.4 SGTR in Two SG with Coincident LOOP Event Tree

The SGTR in Two SG with Coincident Loss of Offsite Power Event Tree is presented in Figure 5.2.4.4-1. The safety functions are provided by the systems/actions listed in Section 5.2.4.1. For this event tree the accident sequences were filtered using a frequency cutoff of 10^{-10} per year. Because the initiating event frequency includes the probability of loss of offsite power, it was felt that a cutoff frequency of 10^{-10} per year rather than 10^{-8} per year would provide increased visibility of the significance of the output scenarios obtained from the event tree. The scenarios that lead to potential core damage are presented in Section 7.2.4. The event tree branches used to construct the event tree, SGTR in Two SG with Coincident LOOP, are discussed below.

T4 The initiating event is defined as one or more tube ruptures in both steam generators with a coincident loss of offsite power on turbine trip. The initiating event frequency is calculated in Section 4.3.2. It should be noted that for SONGS a loss of offsite power results in loss of the Turbine Bypass System and loss of the Blowdown Processing System.

A Failure to Deliver Sufficient HPSI. See discussion for branch A in Section 5.2.4.2. Failure of the HPSI system to maintain flow is defined by branch A' in the scenarios presented in Section 7.2.4.

B Turbine Fails to Trip on Reactor Trip. See discussion for branch B in Section 5.2.4.1.

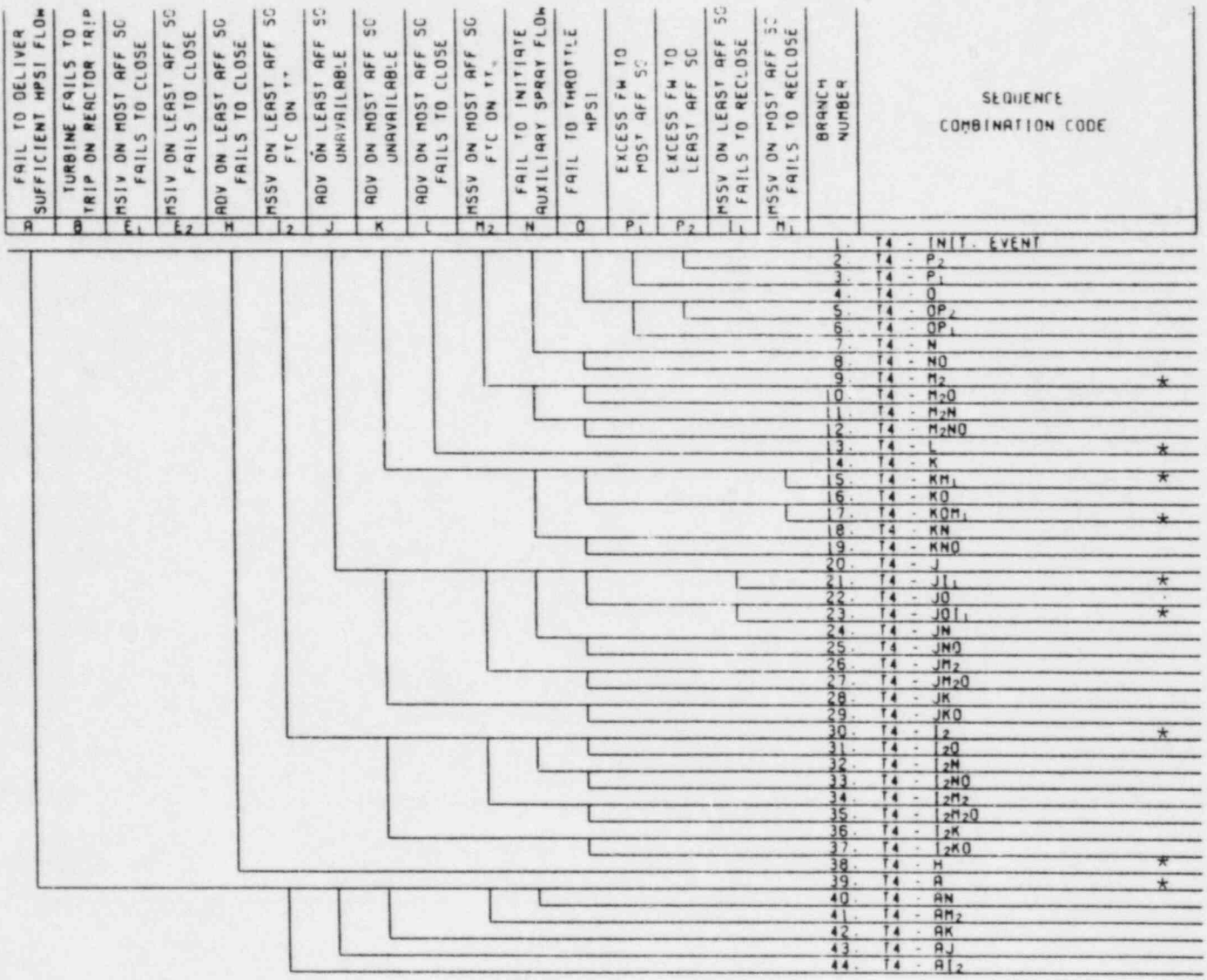


FIGURE 5.2.4.4-1

SGTR IN TWO SGs WITH COINCIDENT LOOP SYSTEMIC EVENT TREE

*The above minimal core damage sequences are evaluated and discussed in Section 7.2.

Note: Any branches excluded from the above event tree have been eliminated due to logic rules or the frequency cut-off as discussed in Section 2.2.1.

E_1 MSIV on Most Affected SG Fails to Close. See discussion for branch E in Section 5.2.4.1.

E_2 MSIV on Least Affected SG Fails to Close refers to the MSIV on SG-089 failing to close on MSIS. The fault tree analysis is presented in Section 6.7.

H ADV on Least Affected SG Fails to Close refers to the ADV associated with SG-089 failing to close after being opened by the operator to initiate cooldown or to prevent a MSSV from opening. A failed open ADV on the least affected SG results in a direct flowpath for RCS inventory from the primary system to the atmosphere (outside containment LOCA). The fault tree analysis is presented in Section 6.8.

I_2 MSSV on Least Affected SG Fails to Close on Turbine Trip refers to one MSSV on SG-089 failing to close on turbine trip. Five MSSVs are assumed to open on SG-089. For the event tree, branch I_1, as defined in Section 5.2.4.1, is separated into branches I_1 and I_2. The separation of these branches simplifies the logical construction of the event tree, i.e. branch I_2 represents the case where the MSSVs open on turbine trip and branch I_1 represents all other cases where one MSSV opens only if the associated ADV is unavailable. The fault tree analysis is presented in Section 6.9.

I_1 MSSV on Least Affected SG Fails to Reclose refers to one MSSV associated with SG-089 failing to close after being challenged by a failure of the ADV on SG-089 to open due to initiation of cooldown, MSIS or SG overfill. A failed open MSSV on the least affected SG results in an outside containment LOCA. The fault tree analysis is presented in Section 6.9.

J ADV on Least Affected SG Unavailable. See discussion for branch J in Section 5.2.4.1.

K ADV on Most Affected SG Unavailable. See discussion for branch K in Section 5.2.4.1.

L ADV on Most Affected SG Fails to Close. See discussion for branch L in Section 5.2.4.2.

M_2 MSSV on Most Affected SG Fails to Close on Turbine Trip. See discussion for branch M_2 in Section 5.2.4.2.

M_1 MSSV on Most Affected SG Fails to Reclose. See discussion for branch M_1 in Section 5.2.4.2.

N Fail to Initiate Auxiliary Spray Flow. See discussion for branch N in Section 5.2.4.3. The fault tree analysis for Fail to Initiate Auxiliary Spray Flow (assuming offsite power is unavailable) is presented in Section 6.2.

O Fail to Throttle HPSI. See discussion for branch O in Section 5.2.4.3. Since the blowdown system is unavailable, failure to throttle HPSI will result in SG overfill.

P_1 Excess Feedwater to the Most Affected SG. See discussion for branch P_1 in Section 5.2.4.1. Since the blowdown system is unavailable, excess feedwater will result in SG overfill.

P_2 Excess Feedwater to the Least Affected SG refers to uncontrolled delivery of auxiliary feedwater to SG-089. Since the blowdown system is unavailable, excess feedwater will result in SG overfill. The fault tree analysis is presented in Section 6.11.

5.3 PORV LOCA

Power Operated Relief Valve (PORV) Loss of Coolant Accident (LOCA) as described in this section refers to the uncontrolled release of RCS mass through the PORV. In order for a PORV LOCA to occur and have significant impact on the reactor core integrity the following conditions have to be met.

- Continuous flow through the PORV
- Failure of PORV LOCA mitigating systems

During a PORV LOCA, RCS mass is released into the containment through the PORV. This condition results in RCS pressure and inventory decrease in conjunction with simultaneous containment pressure and temperature increase. Failure to terminate RCS mass flow through the PORV and failure to restore or maintain RCS inventory eventually leads to core uncovery and core damage.

5.3.1 Initiating Event

The assumed PORV design features two 50% capacity PORV flow paths. Each path consists of a motor operated block valve and a PORV. During plant operation the motor operated block valve and PORV are closed. These valves are designed to be openedmanually to reduce RCS pressure following a steam generator tube rupture event. These valves are also opened manually to establish a means of alternate decay heat removal following the loss of the preferred heat sink. The PORVs are not designed to minimize challenges to the primary safety valves.

The assumed PORV design allows for the valves to be manually open following a steam generator tube rupture event or loss of the preferred secondary heat sink event. In addition to procedural opening of the valves, there is also the possibility that the valves can open inadvertently. Therefore, the PORV LOCA initiating event refers to the opening of either or both PORV flow paths and the inability to terminate flow through the path(s)

when required. Included in this definition are the operator actions necessary to close either the block valve or the PORV in each path. Based on the assumed design of the PORV and the definition for PORV LOCA, a fault tree was developed and evaluated to determine the occurrence frequency for each condition that can cause the PORV flow path to be open. The fault tree analysis is presented in Section 6.4.

5.3.2. Normal Sequence of Events

PORV LOCA is characterized by depressurization of the RCS which leads to a reactor trip, if the reactor has not been tripped by other parameters. Continued depressurization of the RCS causes the HPSI pumps to actuate, take suction from the refueling water tank and discharge to the RCS loops. Continued depressurization of the RCS also causes the containment spray pumps to actuate and take suction from the refueling water tank; however, the borated water is recirculated back to the refueling water tank until a high-high containment pressure setpoint is reached. When containment pressure reaches the high-high setpoint, the containment header valves open to allow the containment spray pumps to discharge to the containment atmosphere. Upon depletion of the refueling water tank inventory, the suctions of the HPSI and containment spray pumps are realigned to the containment sump to continue cooldown of the primary system.

Immediately after the reactor and turbine trip, the turbine bypass valves open to relieve secondary steam and cool the steam generator. If the turbine bypass valves are not available, steam generator cooling can be accomplished by utilizing the atmospheric dump valves or the main steam safety valves. Feedwater to the steam generator is maintained by the MFW System which ramps back to 5% of its flow capacity upon reactor trip. Should 5% main feedwater become unavailable, the AFW System is actuated to maintain feedwater delivery to the steam generators.

Table 5.3.2-1 presents a summary of the normal sequence of events for PORV LOCA from the initiating event until shutdown entry conditions are reached.

TABLE 5.3.2-1

NORMAL SEQUENCE OF EVENTS FOR PORV LOCA

1. PORV LOCA
2. Reactor/Turbine Trip on Low Pressurizer Pressure
3. Steam Bypass Control System opens the TBVs, if the steam generators are available
4. Actuation of the HPSI System by the SIAS
5. Actuation and delivery of AFW flow, if the steam generators are available
6. Actuation of the Containment Spray System and the emergency containment fan coolers by the CSAS and CCAS respectively
7. Realign suction of the HPSI and containment spray pumps to containment sump to initiate and maintain recirculation
8. When the TBVs become unavailable, continue secondary side cooldown with the ADVs, if the steam generators are available
9. Shutdown cooling entry conditions reached.

5.3.3 Functional Event Trees

There are three events which cause or result in the opening of the PORVs and their associated block valves. These events are inadvertent opening of the PORV flow path, manual opening of the PORV flow paths following a loss of the preferred secondary heat sink, and manual opening of the PORV flow paths following a steam generator tube rupture event. Each type of PORV LOCA initiating event requires that functional elements be satisfied or maintained in order to preclude core uncovery and damage. Certain functional elements are common to all PORV LOCA initiating events while others are unique to a particular PORV LOCA initiating event. Therefore, three functional event trees were developed to reflect the three different types of PORV LOCA initiating events.

PORV LOCA is characterized by depressurization of the RCS. Therefore, by nature of a PORV LOCA the RCS Pressure Control Safety Function is not challenged or threatened. The other four anti-core melt safety functions are required to be satisfied or maintained following a PORV LOCA in order to preclude core uncovery and damage.

5.3.3.1 PORV LOCA Following Loss of Secondary Heat Sink Functional Tree

The functional event tree for PORV LOCA following loss of the preferred secondary heat sink is presented in Figure 5.3.3.1-1. Table 5.3.3.1-1 identifies the functional elements which are used as intermediaries to correlate the five anti-core melt safety functions (32) to specific plant systems or actions required to mitigate a PORV LOCA following the loss of secondary heat sink. In this functional event tree both steam generators are unavailable.

System interactions and system availability provide the bases for the general assumptions that were used to develop the functional event tree. The general assumptions used are as follows:

FIGURE 5.3.3.1-1

PORV LOCA
FOLLOWING LOSS OF SECONDARY HEAT
SINK FUNCTIONAL EVENT TREE

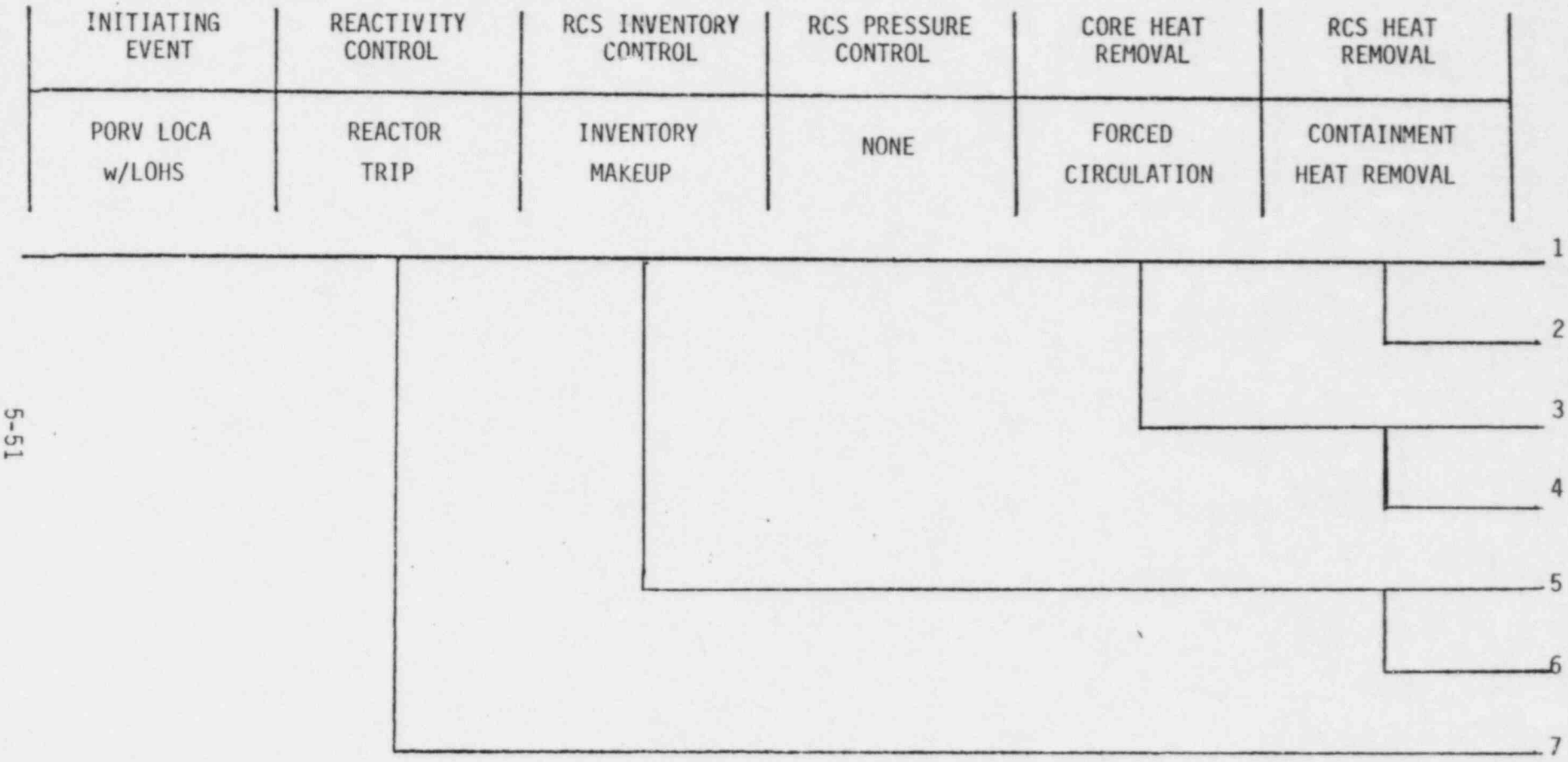


TABLE 5.3.3.1-1

PORV LOCA FOLLOWING LOSS OF SECONDARY HEAT SINK

FUNCTIONAL EVENT TREE CONSIDERATIONS

SAFETY FUNCTION	FUNCTIONAL ELEMENTS	ASSOCIATED SYSTEMS/ACTIONS
Reactivity Control	Reactor Trip	Reactor Trip[1]
RCS Inventory Control	Inventory Make-up	High Pressure Safety Injection
RCS Pressure Control	None	PORV LOCA is characterized by depressurization of the RCS. Therefore, RCS Pressure Control is not challenged.
Core Heat Removal	Forced Circulation	High Pressure Recirculation
RCS Heat Removal	Containment Heat Removal	Containment Sprays and Fans

[1] ATWS is not considered in the scope of this evaluation

1. PORVs open to their full position, fail to close when required and result in uncontrolled bleeding of the primary system.

2. Partial opening of either PORV leads to core damage. This sequence is addressed in the Section 5.1.3.

3. Successful operation of high pressure recirculation is conditional on successful operation of high pressure injection.

Based on the above assumptions, the functional accident sequences for PORV LOCA following loss of secondary heat sink (Refer to Figure 5.3.3.1-1) are as follows:

Sequence 1 — The core is protected. All anti-core melt safety functions are satisfied or maintained; therefore core uncovery and damage do not occur.

Sequence 2 — In this sequence, high pressure injection and recirculation are maintained prior to containment cooling failure. Loss of containment cooling results in containment temperature and pressure increases but the increases are not severe enough to cause containment failure. Therefore, the core is not threatened.

Sequence 3 — In this sequence, high presure injection and containment cooling are accomplished but high pressure recirculation is not accomplished. The inability to accomplish high pressure recirculation prevents circulation of reactor coolant flow through the core to remove core heat. Therefore, this accident sequence will result in core uncovery and damage.

Sequence 4 — In this sequence high pressure injection is maintained. However, high pressure recirculation and containment cooling are unavailable. The inability to

accomplish high pressure recirculation inhibits removal of core heat. Therefore this sequence will result in core uncovery and damage.

Sequence 5 — In this sequence containment cooling is maintained but high pressure injection is unavailable. Because high pressure recirculation is conditional on successful high pressure injection, high pressure recirculation will also be lost. Failure to provide high pressure injection leads to core uncovery and damage.

Sequence 6 — In this sequence high pressure injection and containment cooling are not maintained. High pressure recirculation will also be lost because of the conditionality on successful high pressure injection. This sequence leads to core uncovery and damage.

Sequence 7 — As discussed in Section 2.2.1.1, ATWS is not considered in this program.

5.3.3.2 PORV LOCA Following Steam Generator Tube Rupture Functional Event Tree

The functional event tree for PORV LOCA following steam generator tube rupture is presented in Figure 5.3.3.2-1. Table 5.3.3.2-1 identifies the functional elements which are used as intermediaries to correlate the five anti-core melt safety functions (32) to specific plant systems or actions required to mitigate a PORV LOCA following steam generator tube rupture. In this functional event tree the intact steam generator is available to remove heat from the RCS.

FIGURE 5.3.3.2-1

PORV LOCA

FOLLOWING STEAM GENERATOR
TUBE RUPTURE FUNCTIONAL EVENT TREE

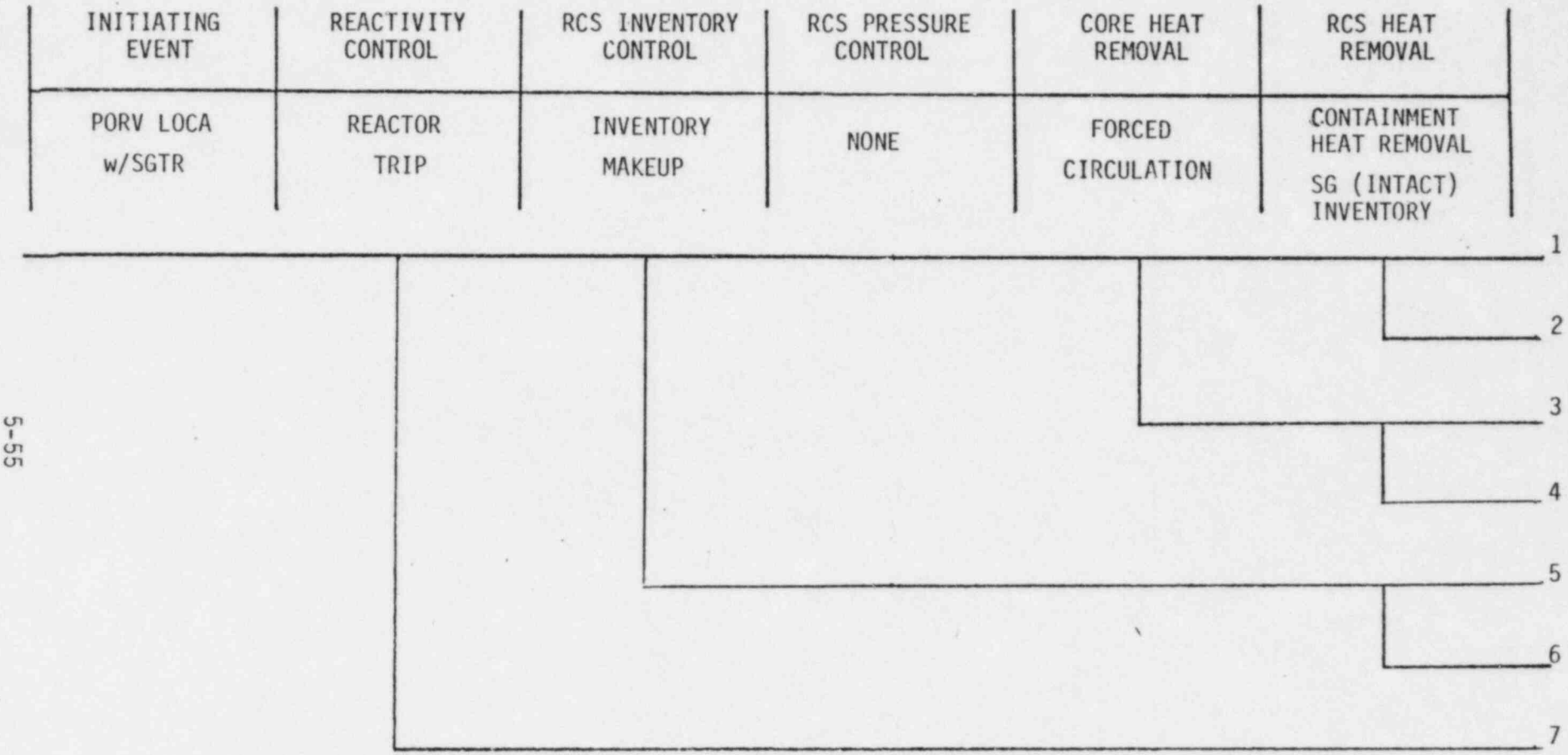


TABLE 5.3.3.2-1

PORV LOCA FOLLOWING SGTR
FUNCTIONAL EVENT TREE CONSIDERATIONS

SAFETY FUNCTION	FUNCTIONAL ELEMENTS	ASSOCIATED SYSTEMS/ACTIONS
Reactivity Control	Reactor Trip	Reactor Trip[1]
RCS Inventory Control	Inventory Make-up	High Pressure Safety Injection
RCS Pressure Control	None	PORV LOCA is characterized by depressurization of the RCS. Therefore, RCS Pressure Control is not challenged.
Core Heat Removal	Forced Circulation	High Pressure Recirculation
RCS Heat Removal	Containment Heat Removal	Containment Sprays and Fans
	SG (Intact) Inventory	5% Main Feedwater Auxiliary Feedwater
	SG (Intact) Pressure	This functional element is addressed in Section 5.2.

[1] ATWS is not considered in the scope of this evaluation

System interactions and system availability provide the bases for the general assumptions that were used to develop the functional event tree. The general assumptions used are as follows:

1. Successful operation of high pressure recirculation is conditional on successful operation of high pressure injection.

2. Uncontrolled secondary pressure decrease leads to core uncovery and damage. This sequence is discussed in Section 5.2.3.

Based on the above assumptions, the functional accident sequences for PORV LOCA following steam generator tube rupture are as follows:

Sequence 1 — The core is protected. All anti-core melt safety functions are satisfied or maintained; therefore, core uncovery and damage do not occur.

Sequence 2 — In this sequence, high pressure injection and recirculation are maintained. The intact steam generator inventory is not maintained in addition to containment cooling. The combined failures result in containment temperature and pressure increases in addition to a large pressure differential between the RCS and the affected steam generator that supports continued leak flow. The continued leak flow will eventually cause the core to uncover and subsequently core damage will occur.

Sequence 3 — In this sequence high pressure injection, containment cooling, and delivery of inventory to the intact steam generator are accomplished; however, high pressure recirculation is unavailable. The inability to accomplish high pressure recirculation prevents

circulation of reactor coolant flow through the core to remove core heat. Therefore, this accident sequence will result in core uncovery and damage.

Sequence 4 — In this sequence high pressure injection is maintained. However, inventory to the intact steam generator, containment cooling, and high pressure recirculation are unavailable. The inability to accomplish high pressure recirculation inhibits removal of core heat. The inability to provide inventory to the intact steam generator inhibits rapid RCS cooldown which causes a large pressure differential between the RCS and the affected steam generator. This condition will continue to support loss of RCS inventory outside the containment and will eventually cause the core to become uncovered and subsequent core damage will occur.

Sequence 5 — In this sequence containment cooling and delivery of inventory to the intact steam generator are maintained; however, high pressure injection is unavailable. Because high pressure recirculation is conditional on successful high pressure injection, high pressure recirculation will also be lost. Failure to provide high pressure injection leads to core uncovery and damage.

Sequence 6 — In this sequence high pressure injection, containment cooling, and delivery of inventory to the intact steam generator are not maintained. High pressure recirculation will also be lost because of the conditionality on successful high pressure injection. This sequence leads to core uncovery and damage.

Sequence 7 — As discussed in Section 2.2.1.1, ATWS is not considered in the scope of this program.

5.3.3.3 Spurious PORV LOCA Functional Event Tree

The functional event tree for inadvertent PORV LOCA is presented in Figure 5.3.3.3-1. Table 5.3.3.3-1 identifies the functional elements which are used as intermediaries to correlate the five anti-core melt safety functions (32) to specific plant systems or actions required to mitigate a spurious PORV LOCA. In this functional event tree, both steam generators are available to remove heat from the RCS. Successful operation of high pressure recirculation is conditional on successful operation of high pressure injection.

Based on the above assumptions, the functional accident sequences for spurious PORV LOCA are as follows:

Sequence 1 — The core is protected. All anti-core melt safety functions are satisified or maintained; therefore core uncovery and damage do not occur.

Sequence 2 — In this sequence, high pressure injection and recirculation are maintained. Steam generator inventory is not maintained and steam generator pressure is not controlled in addition to containment cooling failure. The combined failures result in containment temperature and pressure increases but the increases are not severe enough to cause containment failure.

Sequence 3 — In this sequence high pressure injection, containment cooling, delivery of inventory to the steam generators and steam generator pressure control are accomplished; however, high pressure recirculation is unavailable. The inability to accomplish high pressure recirculation prevents circulation of reactor coolant flow through the core to remove core heat. Therefore, this accident sequence will result in core uncovery and damage.

FIGURE 5.3.3.3-1

SPURIOUS
PORV LOCA

INITIATING EVENT	REACTIVITY CONTROL	RCS INVENTORY CONTROL	RCS PRESSURE CONTROL	CORE HEAT REMOVAL	RCS HEAT REMOVAL
SPURIOUS PORV LOCA	REACTOR TRIP	INVENTORY MAKEUP	NONE	FORCED CIRCULATION	CONTAINMENT HEAT REMOVAL SG INVENTORY SG PRESSURE

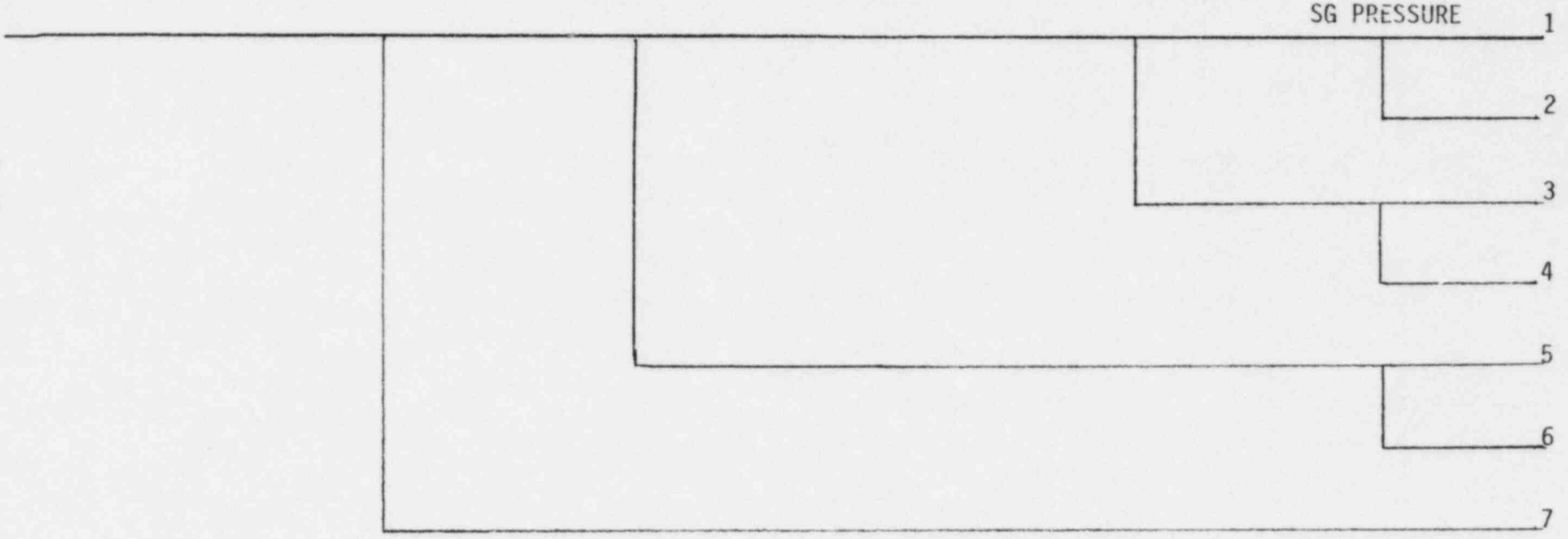


TABLE 5.3.3.3-1

SPURIOUS PORV LOCA
FUNCTIONAL EVENT TREE CONSIDERATIONS

SAFETY FUNCTION	FUNCTIONAL ELEMENTS	ASSOCIATED SYSTEMS/ACTIONS
Reactivity Control	Reactor Trip	Reactor Trip[1]
RCS Inventory Control	Inventory Makeup	High Pressure Safety Injection
RCS Pressure Control	None	PORV LOCA is characterized by depressurization of the RCS. Therefore, RCS Pressure Control is not challenged.
Core Heat Removal	Forced Circulation	High Pressure Recirculation
RCS Heat Removal	Containment Heat Removal	Containment Sprays and Fans
	SG Inventory	5% Main Feedwater Auxiliary Feedwater
	SG Pressure	Bypass Steam to Main Condenser Dump Steam to Atmosphere

[1] ATWS is not considered in the scope of this evaluation

Sequence 4 — In this sequence high pressure injection is maintained. However, steam generator inventory, steam generator pressure, high pressure recirculation, and containment cooling are unavailable. The inability to accomplish high pressure recirculation inhibits removal of core heat. Therefore, this sequence will result in core uncovery and damage.

Sequence 5 — In this sequence containment cooling, delivery of inventory to the steam generators and steam generator pressure control are accomplished; however, high pressure injection is unavailable. Because high pressure recirculation is conditional on successful high pressure injection, high pressure recirculation will also be lost. Failure to provide high pressure injection leads to core uncovery and damage.

Sequence 6 — In this sequence high pressure injection, containment cooling, steam generator inventory, and steam generator pressure are not maintained. High pressure recirculation will also be lost because of the conditionality on successful high pressure injection. This sequence leads to core uncovery and damage.

Sequence 7 — As discussed in Section 2.2.1.1, ATWS is not considered in the scope of this program.

5.3.4 Systemic Event Trees

Three PORV LOCA systemic event trees were developed and constructed to represent the specific plant system response to the different types of PORV LOCA defined in Section 5.3.1. Each event tree was constructed by incorporating, as event tree branch headings, the systems/actions required

to mitigate PORV LOCA. Event tree branch headings are placed in the approximate chronological order that they will be called upon following a PORV LOCA, and interdependencies between event tree branches are logically incorporated.

Table 5.3.4-1 defines the event tree branches and associated failure criteria that are used as input to the event trees. Fault tree results for each branch are presented in Section 6.0.

5.3.4.1 PORV LOCA Following Loss of Secondary Heat Sink Event Tree

The event tree for PORV LOCA Following Loss of Secondary Heat Sink is presented in Figure 5.3.4.1-1. As shown in Table 5.3.3.1-1, the system/action associated with RCS Inventory Control is high pressure safety injection; with Core Heat Removal is high pressure recirculation; and with RCS Heat Removal are containment sprays and fans. These systems are used as the branch headings for the event tree.

The event tree branch headings are discussed as follows:

P1 The initiating event is defined as the frequency of manually opening both PORV flow paths following a loss of secondary heat sink and the probability that the flow paths are not isolated to prevent uncontrolled depressurization of the RCS. The frequency of the initiating event was determined by fault tree analysis which is presented in Section 6.4.

A Failure to deliver sufficient HPSI flow is defined as failure to provide flow to the RCS loops by at least one of three high pressure pumps that take suction from the refueling water tank. Additional descripton of the HPSI System and the fault tree results are given in Section 6.1.

TABLE 5.3.4-1

PORV LOCA EVENT TREE BRANCH DEFINITIONS

Branch Designation	Branch Title	Failure Criteria
P1	Initiating Event	PORV LOCA following loss of secondary heat sink
P2	Initiating Event	PORV LOCA following steam generator tube rupture in one steam generator
P3	Initiating Event	Spurious opening of either PORV flowpath
A	Failure to Deliver Sufficient HPSI Flow	Failure to provide flow to the RCS from at least 1 of 3 high pressure pumps, taking suction from the RWT.
S_1	Failure to Provide Containment Cooling	Failure to provide flow from at least 1 of 2 containment spray pumps into the containment atmosphere; and failure to remove thermal energy from the containment atmosphere by at least 2 of 4 emergency containment fans
R	Failure to Achieve High Pressure Recirculation	Failure to provide flow to the RCS from at least 1 of 2 high pressure pumps, taking suction from the containment sump
Z_1	Failure to Deliver 5% Main Feedwater to 1 Steam Generator	Failure to provide cooling to the intact steam generator via 5% main feedwater
Z_2	Failure to Deliver 5% Main Feedwater	Failure to provide cooling to either steam generators via 5% main feedwater
G_1	Failure to Deliver Auxiliary Feedwater Flow	Failure to automatically deliver AFW flow from at least one AFW pump to either steam generator
G_2	Failure to Deliver Auxiliary Feedwater to 1 Steam Generator	Failure to provide cooling to the intact steam generator by at least 1 of 2 auxiliary feedwater pumps

TABLE 5.3.4-1
(continued)
PORV LOCA EVENT TREE BRANCH DEFINITIONS

Branch Designation	Branch Title	Failure Criteria
C_2	Failure to Open TBVs	Failure to control steam generator pressure by not opening at least 1 of 4 turbine bypass valves
W_2	Failure to Open MSSVs	Failure to control steam generator pressure by not opening at least 1 of 9 MSSVs in each bank
T	Failure to Open ADVs	Failure to control steam generator pressure by not opening at least 1 of 2 ADVs

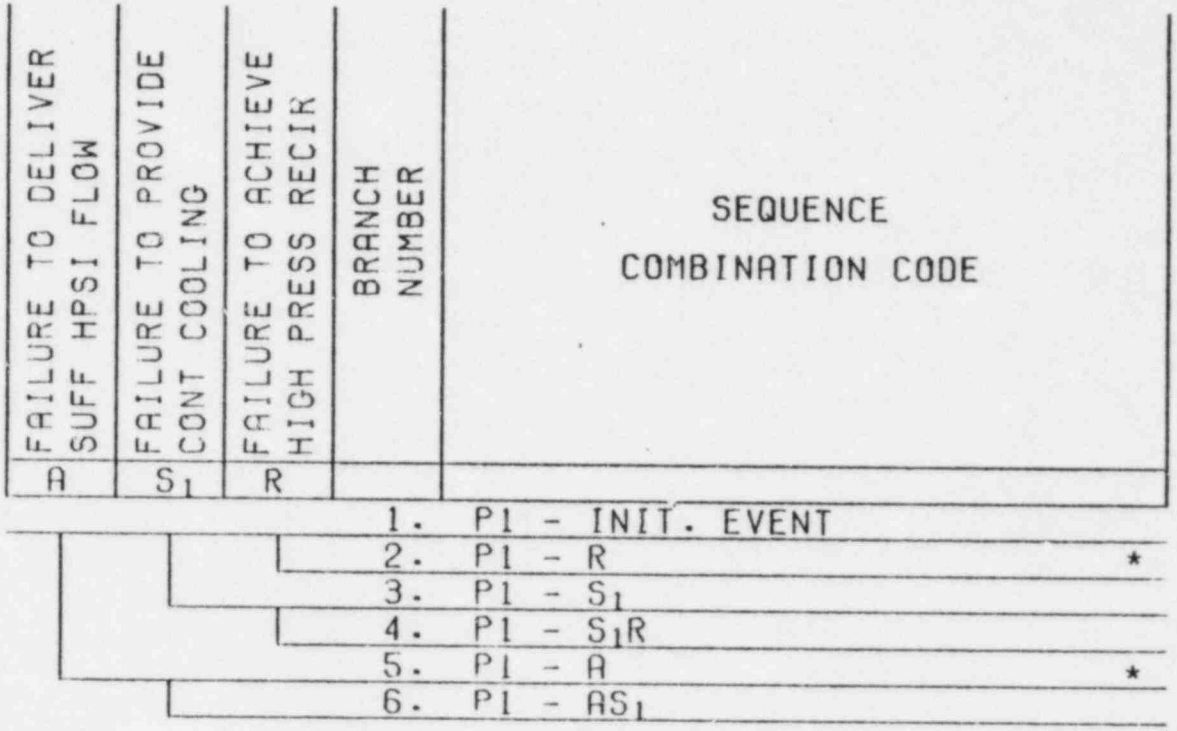


FIGURE 5.3.4.1-1

PORV LOCA FOLLOWING LOSS OF SECONDARY HEAT SINK
SYSTEMIC EVENT TREE

* The above minimal core damage sequences are evaluated and discussed in Section 7.3.

Note: Any branches excluded from the above event tree have been eliminated due to logic rules or the frequency cut-off as discussed in Section 2.2.1.

S_1 Failure to provide containment cooling refers to the inability to provide containment spray and to remove thermal energy from the containment atmosphere. Containment spray is provided by the Containment Spray System. Removal of thermal energy from the containment atmosphere is accomplished by the emergency Containment Cooling System in conjunction with the Containment Spray System. Additional information on the Containment Spray and Containment Cooling Systems along with the fault tree results are given in Section 6.3.

R Failure to achieve high pressure recirculation refers to inability to provide flow to the RCS loops by at least one of two high pressure pumps that take suction from the containment sump. Additional information on high pressure recirculation and the fault tree results are given in Section 6.1.

5.3.4.2 PORV LOCA Following Steam Generator Tube Rupture Event Tree

The event tree for PORV LOCA Following Steam Generator Tube Rupture is presented in Figure 5.3.4.2-1. As shown in Table 5.3.3.2-1, the system/action associated with RCS Inventory Control is high pressure safety injection; with Core Heat Removal is high pressure recirculation; and with RCS Heat Removal are containment sprays and fans and feedwater to the intact steam generator. These systems are used as the branch headings for the event tree.

The event tree branch headings are discussed as follows:

P_2 The initiating event is defined as the frequency of manually opening both PORV flow paths following a tube rupture in one steam generator and the probability that the flow paths are not isolated to prevent uncontrolled depressurization of the RCS. The frequency of the initiating event was determined by fault tree analysis which is presented in Section 6.4.

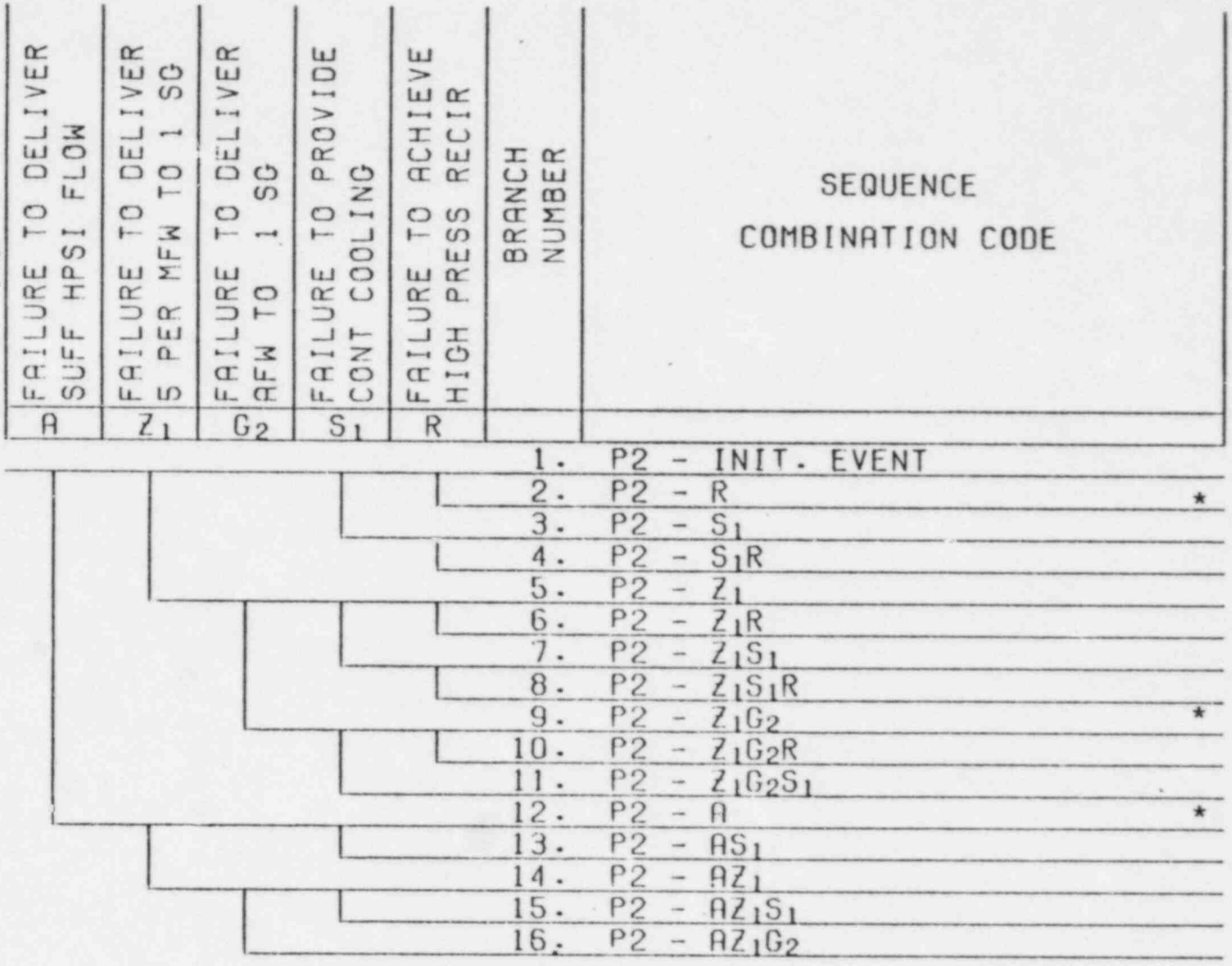


FIGURE 5.3.4.2-1

PORV LOCA FOLLOWING SGTR
SYSTEMIC EVENT TREE

*The above minimal core damage sequences are evaluated and discussed in Section 7.3.

Note: Any branches excluded from the above event tree have been eliminated due to logic rules or the frequency cut-off as discussed in Section 2.2.1.

A — Failure to deliver sufficient HPSI flow. See discussion for branch heading A given in Section 5.3.4.1.

Z_1 — Failure to deliver 5% main feedwater to the intact steam generator is defined as the inability of the Main Feedwater System to ramp back to provide 5% flow to the steam generator with no tube rupture. Additional information on the Main Feedwater System is presented in Section 6.10.

G_2 — Failure to deliver auxiliary feedwater to the intact steam generator refers to the inability of the auxiliary feedwater system to provide flow for cooling the steam generator with no tube rupture. Once 5% main feedwater becomes unavailable, feedwater for cooling the intact steam generator is provided by the auxiliary feedwater system. The delivery of auxiliary feedwater continues until shutdown cooling entry conditions are met. The auxiliary feedwater system failure probability was determined by fault tree analysis. The fault tree model includes the unavailability of the steam generator with the tube rupture and only the automatic actions needed to deliver auxiliary feedwater to the intact steam generator. Additional information on the Auxiliary Feedwater System and the fault tree results are given in Section 6.11.

S_1 — Failure to provide component cooling. See discussion for branch heading S_1 given in Section 5.3.4.1.

R — Failure to achieve high pressure recirculation. See discussion for branch heading R given in Section 5.3.4.1.

5.3.4.3 Spurious PORV LOCA Event Tree

The event tree for Spurious PORV LOCA is presented in Figure 5.3.4.3-1. As shown in Table 5.3.3.3-1, the system/action associated with RCS Inventory Control is high pressure safety injection; with

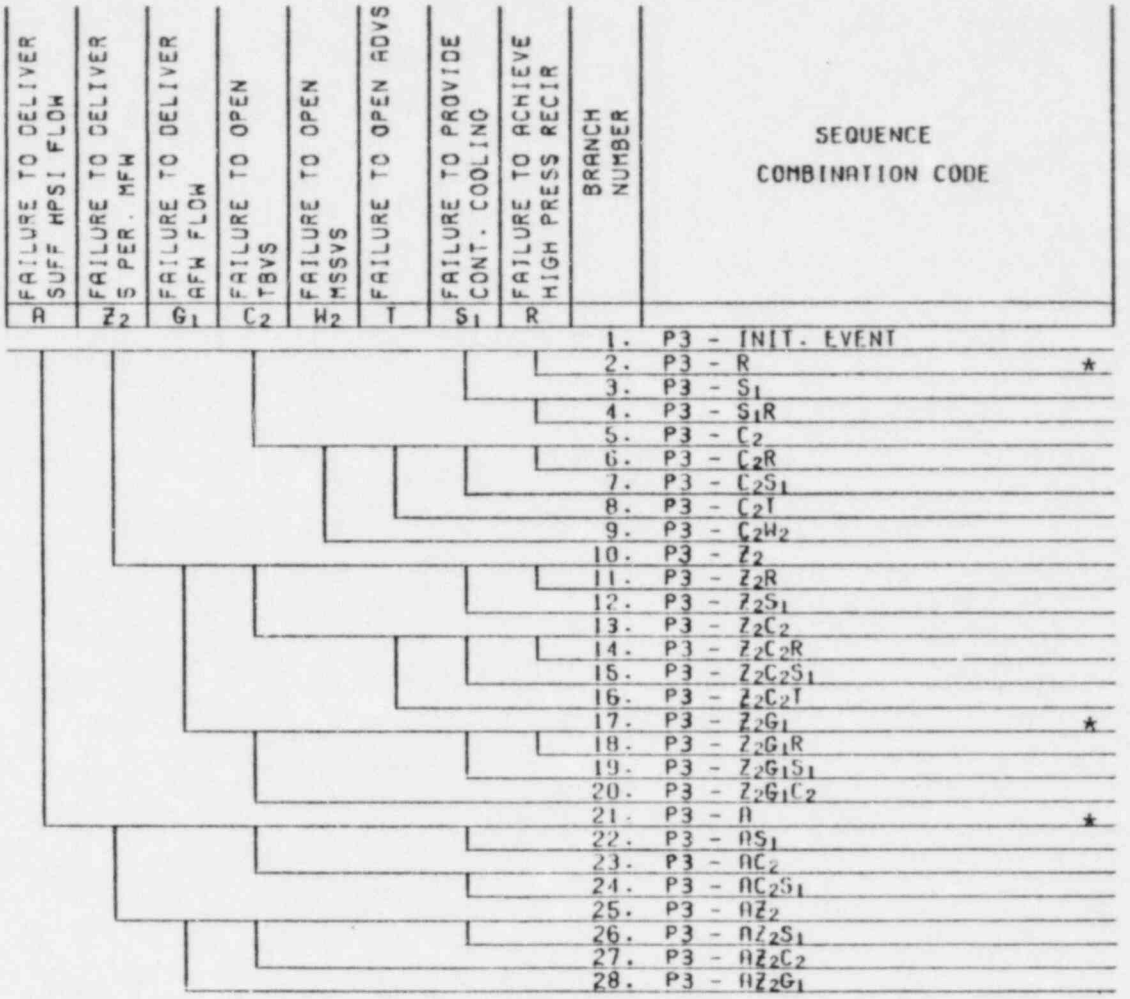


FIGURE 5.3.4.3-1

SPURIOUS PORV LOCA
SYSTEMIC EVENT TREE

* The above minimal core damage sequences are evaluated and discussed in Section 7.3.

Note: Any branches excluded from the above event tree have been eliminated due to logic rules or the frequency cut-off as discussed in Section 2.2.1.

Core Heat Removal is high pressure recirculation and with RCS Heat Removal are containment sprays and fans, 5% main and auxiliary feedwater and dumping steam to the condenser or to the atmosphere. These systems/actions are used as the branch headings for the event tree.

The event tree branch headings are discussed as follows:

P3 — The initiating event is defined as the frequency of either PORV flow path opening spuriously and the probability that the affected flow path is not isolated to prevent uncontrolled depressurization of the RCS. The frequency of the initiating event was determined by fault tree analysis which is presented in Section 6.4.

A — Failure to deliver sufficient HPSI flow. See discussion for Branch Heading A given in Section 5.3.4.1.

Z_2 — Failure to deliver 5% main feedwater is defined as the inability of the MFW System to ramp back to provide 5% flow to both steam generators. Additional information on the Main Feedwater System is presented in Section 6.10.

G_1 — Failure to deliver auxiliary feedwater refers to the inability of the AFW System to provide flow for cooling either steam generator. Once 5% main feedwater, the preferred source becomes unavailable, the Auxiliary Feedwater System provides feedwater for cooling either steam generator so that shutdown cooling entry conditions can be achieved. The AFW System failure probability was determined by fault tree analysis. The fault tree model includes only the automatic actions needed to deliver auxiliary feedwater. Additional information on the AFW System and the fault tree results are given in Section 6.11.

C_2 Failure to open the turbine bypass valves refers to not opening at least one of the turbine bypass valves to relieve secondary steam. This system is used as the preferred system for removing secondary steam to enhance RCS cooldown. The system failure probability was determined by fault tree analysis. Additional system information and fault tree results are given in Section 6.6.

W_2 Failure to open the main steam safety valves refers to at least one of the nine safety valves in each bank not opening. If the turbine bypass valves are unavailable, the main steam safety valves would open and reclose to relieve secondary steam but prevent overcooling of the RCS. The failure probability for opening one of nine valves in each bank is presented in Section 6.9.

T Failure to open the atmospheric dump valves refers to not opening either atmospheric dump valve flow path to relieve secondary steam to the atmosphere. The atmospheric dump valves are used to dump secondary steam to the atmosphere when the turbine valves are unavailable. The system failure probability was determined by fault tree analysis with the results and additional system information presented in Section 6.8.

S_1 Failure to Provide Containment Cooling. See discussion for branch heading S_1 given in Section 5.3.4.1.

R Failure to Achieve High Pressure Recirculation. See discussion for branch heading R given in Section 5.3.4.1.

5.4 OTHER CORE MELT SEQUENCES

The NRC questions (see Appendix A) focused on the initiating events and subsequent event sequences that the staff considered to be most relevant to the PORV issue. These events are loss of heat sink, steam generator tube rupture and PORV LOCA. The questions additionally request that consideration be given to ATWS, PTS and other accident sequences for which PORVs may provide a benefit.

A qualitative discussion of ATWS and PTS appear in the main body of this report (28). In order to investigate the other accident sequences for which PORVs may provide a benefit, a survey method was used. Specifically, the preliminary results of the Calvert Cliffs Unit 1 IREP Study (29) were reviewed with the intention of identifying core melt sequences that could be mitigated or prevented by incorporating feed and bleed capability, and that are not covered in the event trees of Section 5.1, 5.2, and 5.3.

The conclusion of the IREP review is that of the eleven dominant sequences identified by IREP, seven are not relevant to the PORV issue (these involve large and small LOCA and small-small LOCA with failure to trip) and four are relevant to the PORV issue and are covered by the event trees of Sections 5.1, 5.2, and 5.3. No relevant dominant sequences were found to have been over-looked. Section 7.4 contains the detailed sequence descriptions.

6.0 SYSTEM ANALYSES

The following sections contain the results of all fault tree analyses and probabilistic evaluations that were used as input to the systemic event trees for Loss of Secondary Heat Sink, Steam Generator Tube Rupture and PORV LOCA. Efforts were made to maintain consistent levels of detail in the fault tree models. There was an attempt to keep failures modelled at the component level, however, occasionally it was required to expand the fault trees to sufficient levels of detail to include distinct failure modes for major components (e.g. HPSI pump fails to start and HPSI pump fails to operate) and to include auxiliary system failures. Specifically, the Electrical Distribution System, the Instrument Air System, and the Component Cooling Water System were addressed and included in a uniform manner throughout the system fault tree analyses.

In performing the fault tree analyses, a number of general groundrules were formulated to further standardize the models. The analyses did not consider the following:

1. Failures resulting from the environment created by the initiating events.

2. Common cause failures of more than one piece of equipment based on common location.

3. Failures caused by external events such as floods, lightning, tornadoes or earthquakes.

4. Spurious closure of normally open valves, unless they are fail-closed valves.

5. Spurious opening of normally closed valves, unless they are fail-open valves.

6. Sabotage.

Whenever possible, plant specific operating procedures were used to support development and construction of the fault tree logic diagrams.

All analyses are categorized by system for organizational efficiency, however, when applicable the sections include multiple fault trees developed at the system functional level for various modes of system operation. Also included in each systemic section is a system description and schematic, a support system dependency diagram, a list of assumptions specific to the fault tree models developed for the particular system, a table of results and a table of dominant cutsets for each fault tree model. The quantitative results of the fault tree analyses are presented as confidence distributions in terms of median values and error factors. Typically, the dominant mode of system failure was the unavailability (the probability that a system will not respond on demand). The unreliability of a system required to operate for a period of time following a transient is included in the results only if the unreliability was found to be a significant (>10%) contributor to the overall system failure probability.

It should be noted that the support system dependency diagrams presented in Sections 6.1 - 6.16 include onsite and offsite sources of non class 1E AC power as separate support systems in order to provide increased visibility of the support systems available for operation of both safety and normally operating plant systems. An arrow drawn from one source of AC power to the next represents the logical sequence of AC power available to the system. The arrow could also be interpreted as a logical AND gate, i.e., the power supplies connected by an arrow provide normal and backup AC power to the system and both sources must be unavailable to cause system failure. A terminated line drawn from a support system indicates that the particular support system is not a valid requirement of any of the operating modes of the specific plant system being addressed.

6.1 HIGH PRESSURE SAFETY INJECTION SYSTEM

Three distinct operating modes of the HPSI system were evaluated for input to one or more of the systemic/action level event trees discussed in Sections 5.1-5.3. The functions addressed were Fail to Deliver Sufficient

HPSI Flow (injection mode), Failure to Achieve High Pressure Recirculation and Fail to Throttle HPSI. The HPSI system also plays an important role in feed and bleed operation, however, the functional aspects of the HPSI system in relation to feed and bleed operation are addressed in Section 6.5, "Primary Feed and Bleed System". Fault tree logic diagrams were used to evaluate Fail to Deliver Sufficient HPSI Flow and Failure to Achieve HP Recirculation. A probability calculation based on operating experience was used to calculate the probability of failing to throttle HPSI flow. The results of the analyses are presented in Section 6.1.3.

6.1.1 System Description

Schematics of the SONGS HPSI System (Injection Mode and Recirculation Mode) are presented in Figures 6.1.1-1 and 6.1.1-2. The injection mode of operation is initiated upon receipt of a safety injection actuation signal (SIAS). A SIAS is produced upon any two coincident low pressurizer pressure (<1600 psia) or high containment pressure signals. The SIAS may also be initiated manually in the control room. Upon a SIAS, the HPSI pumps automatically start and the HPSI header isolation valves open. During injection mode, the minimum flow lines downstream of each pump are kept open to prevent possible dead head operation. The pumps take suction from two Refueling Water Tanks (RWTs) and discharge through the eight HPSI header isolation valves via two redundant HPSI headers. The safety injection water then flows to the reactor vessel through a safety injection nozzle on each of the four RCS cold leg pipes. If offsite power (normal AC) is unavailable, the ESF buses are connected to the diesel generators and safeguard loads (the HPSI System) are then started in a preprogrammed time sequence.

The recirculation mode is automatically initiated by the Recirculation Actuation Signal (RAS) upon low RWT level. The RAS opens the containment sump outlet valves. The operator closes the HPSI pump mini-flow line recirculation valves at 37% level in the RWT and closes the RWT isolation valves following RAS at 19% level in the RWT.

The High Pressure Safety Injection/Recirculation support system dependency diagram is provided in Figure 6.1.1-3.

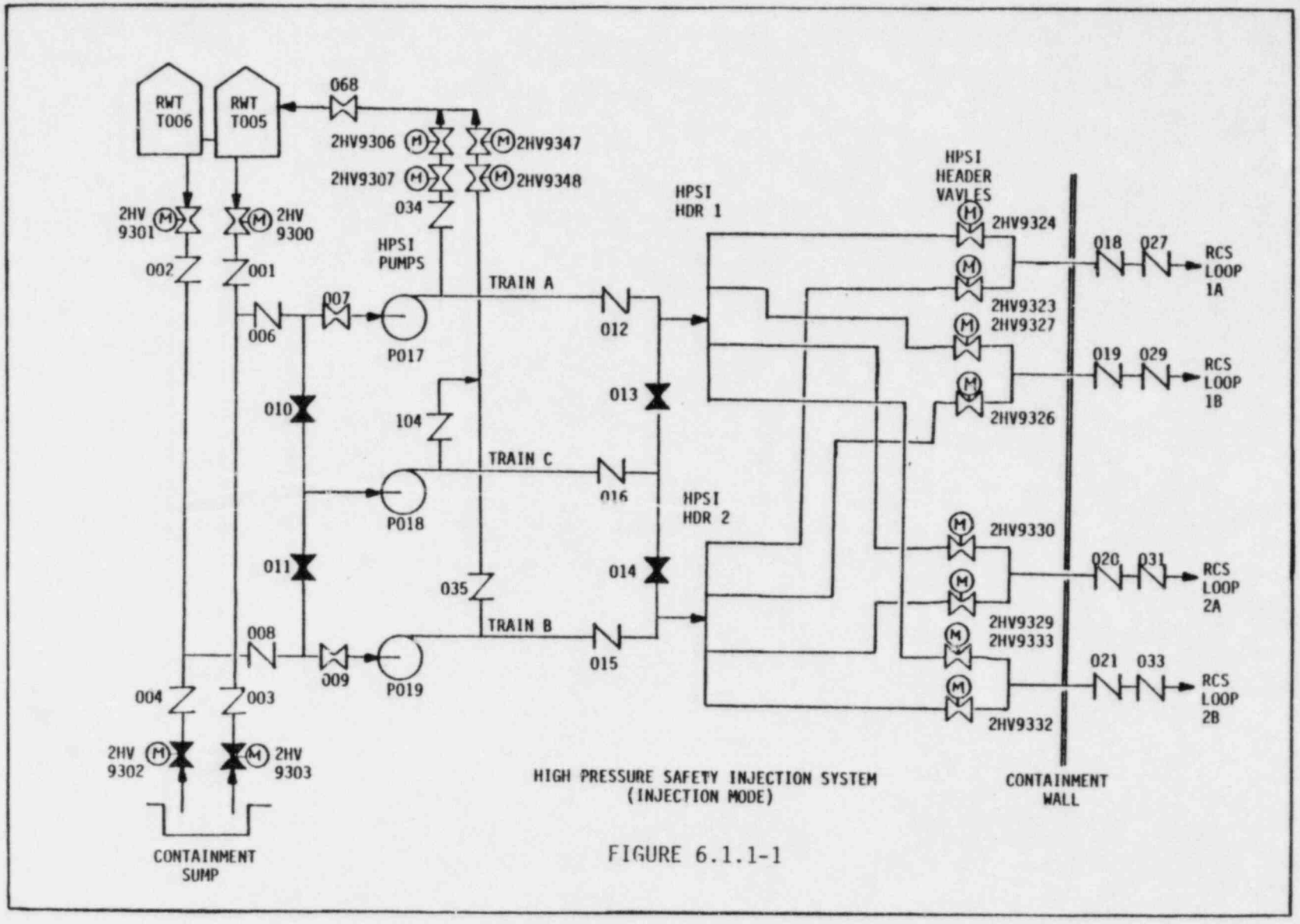

RWT T006
RWT T005
068
2HV9306
2HV9347
2HV9307
2HV9348
034
HPSI PUMPS
2HV 9301
2HV 9300
002
001
006
007
P017
TRAIN A
012
HPSI HDR 1
HPSI HEADER VAVLES
2HV9324
018
027
RCS LOOP 1A
2HV9323
2HV9327
019
029
RCS LOOP 1B
2HV9326
013
010
104
TRAIN C
016
P018
HPSI HDR 2
2HV9330
011
014
035
020
031
RCS LOOP 2A
2HV9329
2HV9333
008
009
P019
TRAIN B
015
021
033
RCS LOOP 2B
2HV9332
004
003
2HV 9302
2HV 9303
CONTAINMENT SUMP
HIGH PRESSURE SAFETY INJECTION SYSTEM (INJECTION MODE)
CONTAINMENT WALL

FIGURE 6.1.1-1

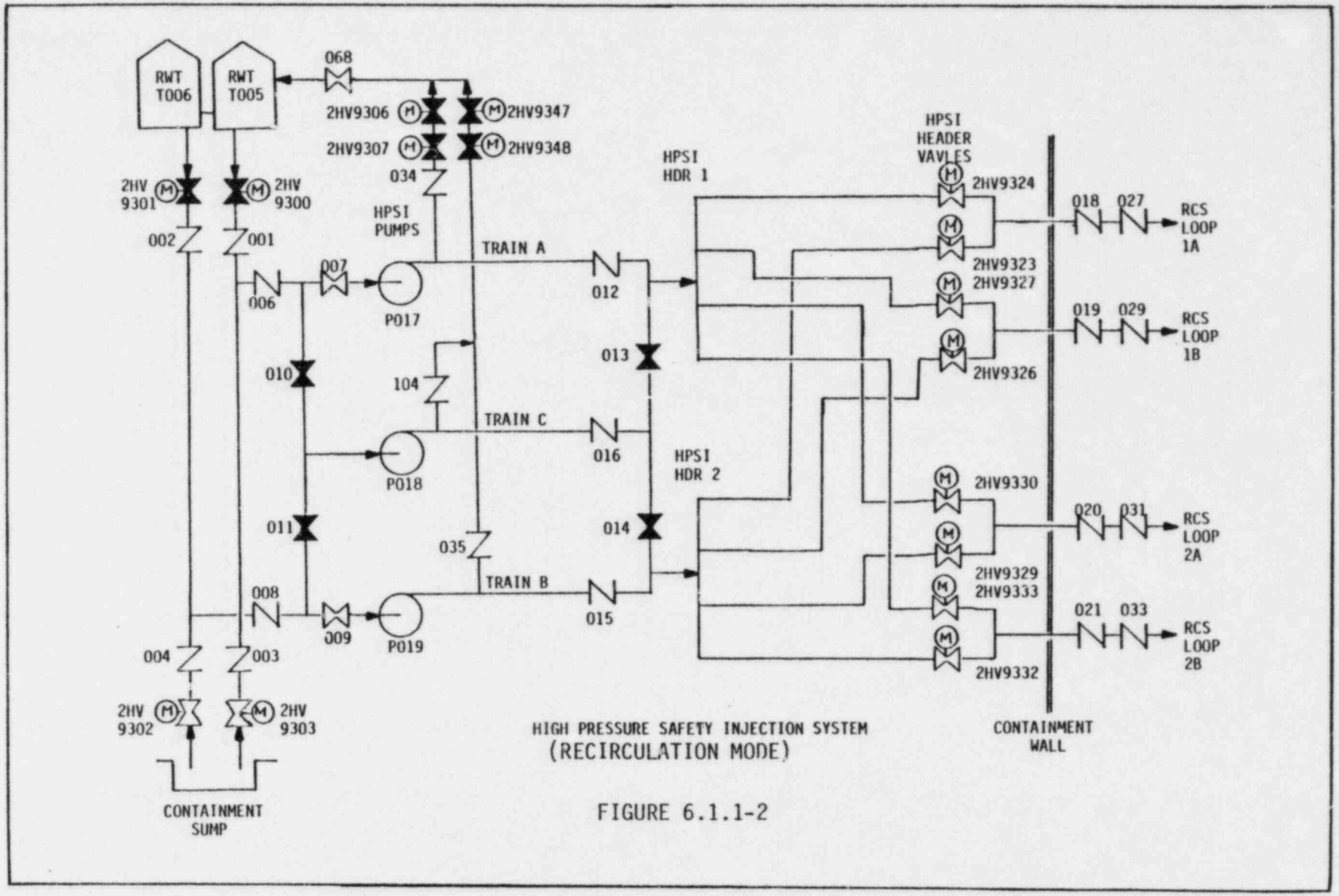
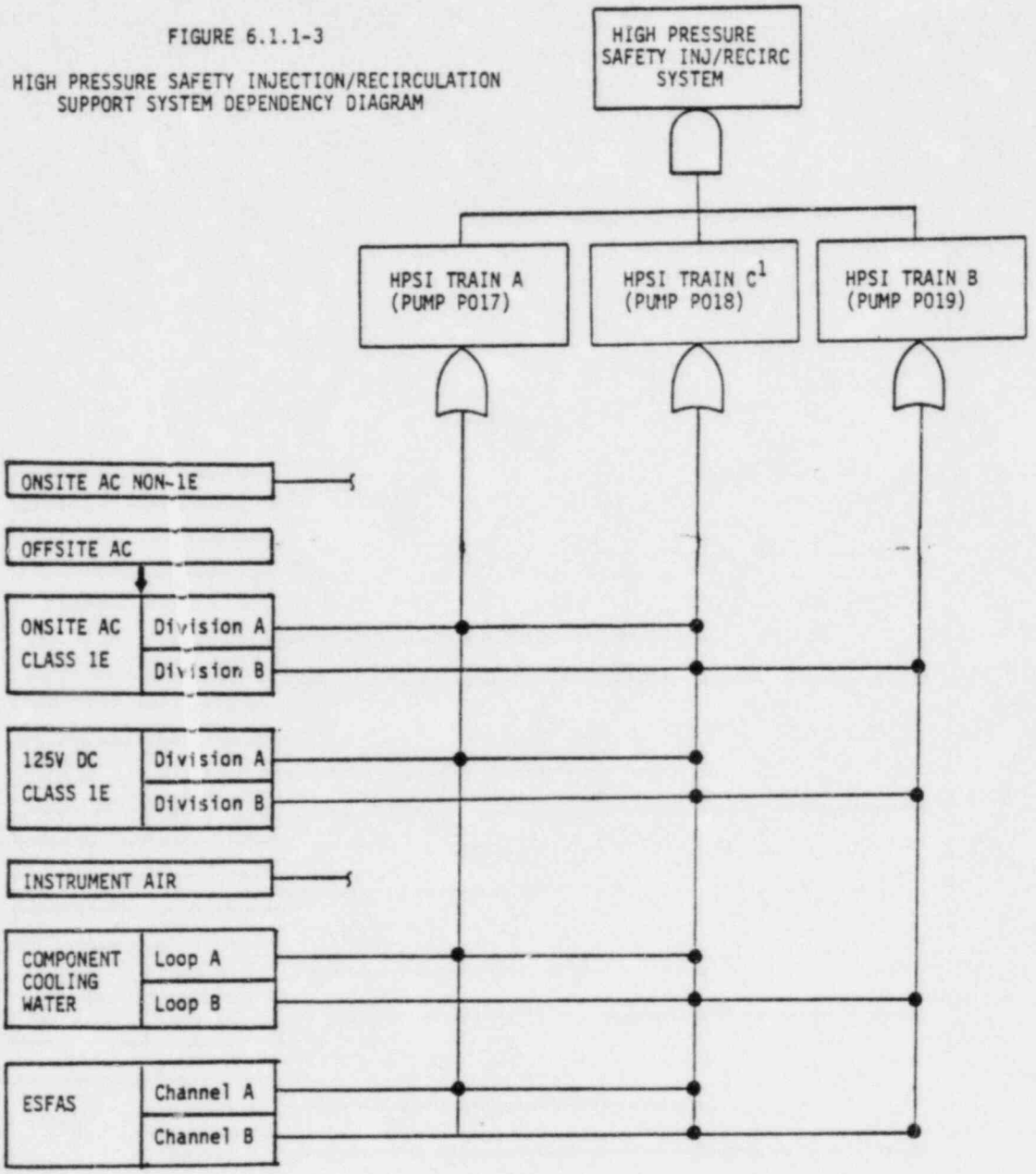

RWT T006
RWT T005
068
2HV9306
2HV9347
2HV9307
2HV9348
034
HPSI PUMPS
2HV 9301
2HV 9300
002
001
007
006
P017
TRAIN A
012
010
104
013
TRAIN C
016
P018
011
014
035
TRAIN B
008
009
P019
015
004
003
2HV 9302
2HV 9303
CONTAINMENT SUMP
HPSI HDR 1
HPSI HDR 2
HPSI HEADER VAVLES
2HV9324
2HV9323
2HV9327
2HV9326
2HV9330
2HV9329
2HV9333
2HV9332
018
027
019
029
020
031
021
033
RCS LOOP 1A
RCS LOOP 1B
RCS LOOP 2A
RCS LOOP 2B
CONTAINMENT WALL
HIGH PRESSURE SAFETY INJECTION SYSTEM
(RECIRCULATION MODE)

FIGURE 6.1.1-2

FIGURE 6.1.1-3

HIGH PRESSURE SAFETY INJECTION/RECIRCULATION SUPPORT SYSTEM DEPENDENCY DIAGRAM



[1]This pump is aligned for manual actuation, however, it has the capability to start automatically on either SIAS A or SIAS B.

6.1.2 Assumptions

The following assumptions were made in performing the fault tree analysis for Fail to Deliver Sufficient HPSI Flow:

1. System failure is defined as the inability to deliver sufficient HPSI flow to the reactor core. Sufficient HPSI flow is defined as one pump flow to two RCS loops. (Two flowpaths are required to deliver the flow from one pump.

2. Isolation of the pump mini-flow lines could result in dead head operation and damage to the pumps.

3. HPSI pumps P017 and P019 are available to start on SIAS. HPSI Pump P018 is on standby and operator action is required to establish flow.

4. The following operator actions were considered:

   - Manual backup of SIAS from the control room

   - Operator action to establish flow from standby HPSI Pump P018. This includes the operator actions required to:

     - unlock and open manual valves

013-C-075	258-D-387 (CCW)
014-C-075	259-D-387 (CCW)
010-C-212	231-D-387 (CCW)
011-C-212	

     - unlock and open check valve 104-C-329

     - start HPSI Pump P018

     The operator is allowed 30 minutes to backup the SIAS or to establish flow from the standby HPSI train.

5. HPSI PUMP P018 is normally aligned to receive power from 4.16 KV Bus 2A04. It can be manually transferred to 4.16 KV Bus 2A06.

6. The containment sump isolation valves are closed.

7. The HPSI system is tested at start-up and once every three months. If pump maintenance is required, manual valves 007-C-212 or 009-C-212 may be closed and inadvertently left in the wrong position. However, all other normally open valves are required to remain open during plant operation. If a valve was inadvertently in the wrong position, it would be discovered during the HPSI pump test. Therefore, the only failure mode considered for these valves is plugging.

8. Component Cooling Water (CCW) is required for successful HPSI pump operation.

The following assumptions were made in performing the fault tree analysis for Failure to Achieve HP Recirculation:

1. System failure is defined as the inability to recirculate sufficient coolant through the reactor core via the high pressure safety injection system.

2. Sufficient coolant is defined as the successful operation of one high pressure safety injection pump.

3. Successful operation of the HPSI system in the injection mode has been achieved. HPSI pumps P017 and P019 are assumed to be operating.

4. The operator is required to close the mini-flow line series isolation valves at 37% level in the RWT. Failure of these valves to close does not significantly impact HP recirculation flow; therefore, failure to isolate the mini-flow lines is not considered in the fault tree model.

5. The RWT isolation valves are manually closed following initiation of the recirculation mode. Failure of these valves to close does not impede recirculation flow; therefore, these valves are not included in the fault tree model.

The following assumptions were made for the probability calculation for Fail to Throttle HPSI:

1. This failure mode is applicable only to the SGTR event trees. Fail to Throttle HPSI refers to maintaining a high RCS pressure through continued delivery of safety injection near the shut off head. System failure is defined as the operator failing to take the appropriate actions to throttle HPSI flow.

2. There have been four events to date classified as SGTRs. (See Section 4.3.2). In one of the four events, the operator failed to adequately throttle HPSI flow.

6.1.3 Results

The quantitative results of the analyses are presented in Table 6.1.3-1. The confidence distributions of the failure probabilities are presented in terms of median values and error factors. The error factor is defined as the ratio of the 95 to 50 percentile.

For Fail to Deliver Sufficient HPSI Flow, a fault tree logic diagram was used to evaluate the specific cases required as input to various event trees. For the SGTR event trees where offsite power is available at the time of the initiating event, the fault tree model does not include grid collapse following turbine trip as a component failure, i.e. the probability of grid collapse on turbine trip is 0.0. For the SGTR with Coincident LOOP event trees, the fault tree model assumes the grid is lost on turbine trip, i.e., the probability of grid collapse on turbine trip is

1.0. For the PORV LOCA event trees, grid collapse following turbine trip is included as a valid failure mode with a probability of 10^{-3} (16). (10^{-3} is a generic value and for SONGS this number might be lower, i.e., the transmission system has a high transient stability limit due to high installed capacity and extensive grid interconnections with other utilities). It was noted that the unreliability of the HPSI system became a significant contributor (>10%) to the total system failure probability for the case where offsite power was given as unavailable. Therefore, a separate analysis was performed to determine the probability of failing to maintain HPSI flow for 8 hours following a SGTR with Coincident LOOP. These results are presented as Cases One through Four respectively in Table 6.1.3-1.

For Failure to Achieve HP Recirculation, a fault tree logic diagram was used to provide input to the Loss of Secondary Heat Sink (LOHS) and PORV LOCA event trees. For the PORV LOCA event trees, the probability of failing to achieve HP recirculation is provided as Case Five in Table 6.1.3-1. For the LOHS event trees the probability of failing to achieve HP recirculation is conditional on the loss of MFW and the loss of AFW. The dependencies which exist between these three systems have been incorporated into the HP Recirculation System failure probability. These results are presented as Case Six in Table 6.1.3-1.

The probability for Fail to Throttle HPSI is used only in the SGTR event trees. Operating experience was used to calculate a failure probability of .25 (1 failure in 4 SGTR events). An error factor of three was assumed.

Table 6.1.3-2 contains a list of the dominent cutsets for each case presented in Table 6.1.3-1. Included in the table is a brief description of each cutset as well as the percent contribution to the total failure probability. The percentage is based on a point estimate ratio.

TABLE 6.1.3-1

FAILURE PROBABILITIES FOR SONGS HPSI SYSTEM

Case Number	Description	Failure Probability (Median Value)	Error Factor
One	Fail to Deliver Sufficient HPSI Flow-System Unavailability given offsite power is available at the time of the initiating event	1.5E-4	4
Two	Fail to Deliver Sufficient HPSI Flow-System Unavailability given offsite power is unavailable at the time of the initiating event	7.7E-3	11
Three	Fail to Deliver Sufficient HPSI Flow-System Unavailability	1.8E-4	5
Four	Fail to Maintain Sufficient HPSI Flow-System Unreliability at 8 hours given offsite power is unavailable at the time of the initiating event	1.7E-3	16
Five	Failure to Achieve HP Recirculation-System Unavailability	2.6E-5	15
Six	Failure to Achieve HP Recirculation-System Unavail-ability given loss of MFW and loss of AFW	2.0E-3	8
Seven	Fail to Throttle HPSI	2.5E-1	3

TABLE 6.1.3-2

DOMINANT CUTSETS FOR SONGS HPSI SYSTEM

Case Number	Cutset		Description	% of Total Failure Probability
One	1.	HVNT0418	Mini-flow line manual valve 068-C-076 plugged	88%
	2.	FSSR0413 FSSR0422 HSS00414	SIASA not generated and SIASB not generated and Operator fails to generate SIAS from control room	2.8%
	3.	HVNX0454 HVNX0456 HPM00427	Disch. valve 228-D-387 not open Disch. valve 236-D-387 not open Operator fails to realign valves and start standby HPSI train	.3%
Two	1.	EDXJ0150 EDXJ0151	DG 2G002 Fails to start and DG 2G003 Fails to start	17%
	2.	EDXJ0150 ELBN0172	DG 2G002 Fails to start and 4.16KV Bus 2A06 Fails on LOOP	13%
	3.	EDXJ0151 ELBN0171	DG 2G003 Fails to start and 4.16KV Bus 2A04 Fails on LOOP	13%
Three	1.	HVNT0418	Mini-flow line manual valve 068-C-086 plugged	84%
	2.	FSSR0413 FSSR0422 HSS00414	SIASA not generated and SIASB not generated and Operator fails to generate SIAS from control room	2.7%
	3.	EBGP0161 EDXJ0150 EDXJ0151	Grid collapse following TT and DG 2G002 Fails to start and DG 2G003 Fails to start	.8%
Four	1.	EDXJ0150 EDXC0153	DG 2G002 Fails to start and DG 2G003 Fails to run	15%
	2.	EDXJ0151 EDXC0152	DG 2G003 Fails to start and DG 2G002 Fails to run	15%
	3.	ELBN0172 EDXC0152	4.16KV Bus 2A06 Fails on LOOP and DG 2G002 Fails to run	11%
	4.	ELBN0171 EDXC0153	4.16KV Bus 2A04 Fails on LOOP and DG 2G003 Fails to run	11%

TABLE 6.1.3-2
(continued)
DOMINANT CUTSETS FOR SONGS HPSI SYSTEM

Case Number	Cutset		Description	% of Total Failure Probability
Five	1.	FSRR0600	RASA not generated and	28%
		FSRR0596	RASB not generated and	
		HSR00603	Operator fails to generate RAS from control room	
	2.	HVMA0594	Sump valve 2HV-9303 mechanical malfunction and	8.7%
		HVMA0595	Sump valve 2HV-9302 mechanical malfunction	
	3.	EBGP0161	Grid collapse following TT and	7.8%
		EDXJ0150	DG 2G002 Fails to start and	
		EDXJ0151	DG 2G003 Fails to start	
Six	1.	EBGP0160	Spurious grid collapse	17%
		EDXC0152	DG 2G002 Fails to run	
		EDXC0153	DG 2G003 Fails to run	
	2.	EBGP0160	Spurious grid collapse	11%
		EDXJ0150	DG2G002 Fails to start	
		EDXC0153	DG2G003 Fails to run	
	3.	EBGP0160	Spurious grid collapse	11%
		EDXJ0151	DG 2G003 Fails to start	
		EDXC0152	DG 2G002 Fails to run	
Seven	1.	HZZ00539	Operator Fails to throttle HPSI	100%

6.2 AUXILIARY SPRAY SYSTEM

6.2.1 System Description

A schematic of the SONGS Auxiliary Spray System is presented in Figure 6.1.1-1. Auxiliary spray valve 2HV9201 is manually opened from the control room and provides the primary flowpath for auxiliary spray. As charging line valves 2HV-9202 and 2HV-9203 are throttled closed, flow is diverted through the auxiliary spray line to the main spray line and into the pressurizer. If spray valve 2HV-9201 is unavailable, manual spray valve 130-C-334 can be opened with a handwheel to provide a secondary flowpath for auxiliary spray. If charging flow cannot be diverted, the operator can close charging line stop valve 2HV-9200 from the control room or locally with a handwheel to terminate charging and divert flow through the secondary auxiliary spray flowpath. If offsite power is unavailable, charging line stop valve 2HV-9200 must be used to divert charging flow. (The charging line valves are fail as is on loss of offsite power). It should be noted that charging line stop valve 2HV-9200 fails open on loss of offsite power due to loss of instrument air, hence, the operator is required to manually close the valve. A schematic of the charging supply to the auxiliary spray flowpaths is presented in Figure 6.2.1-2.

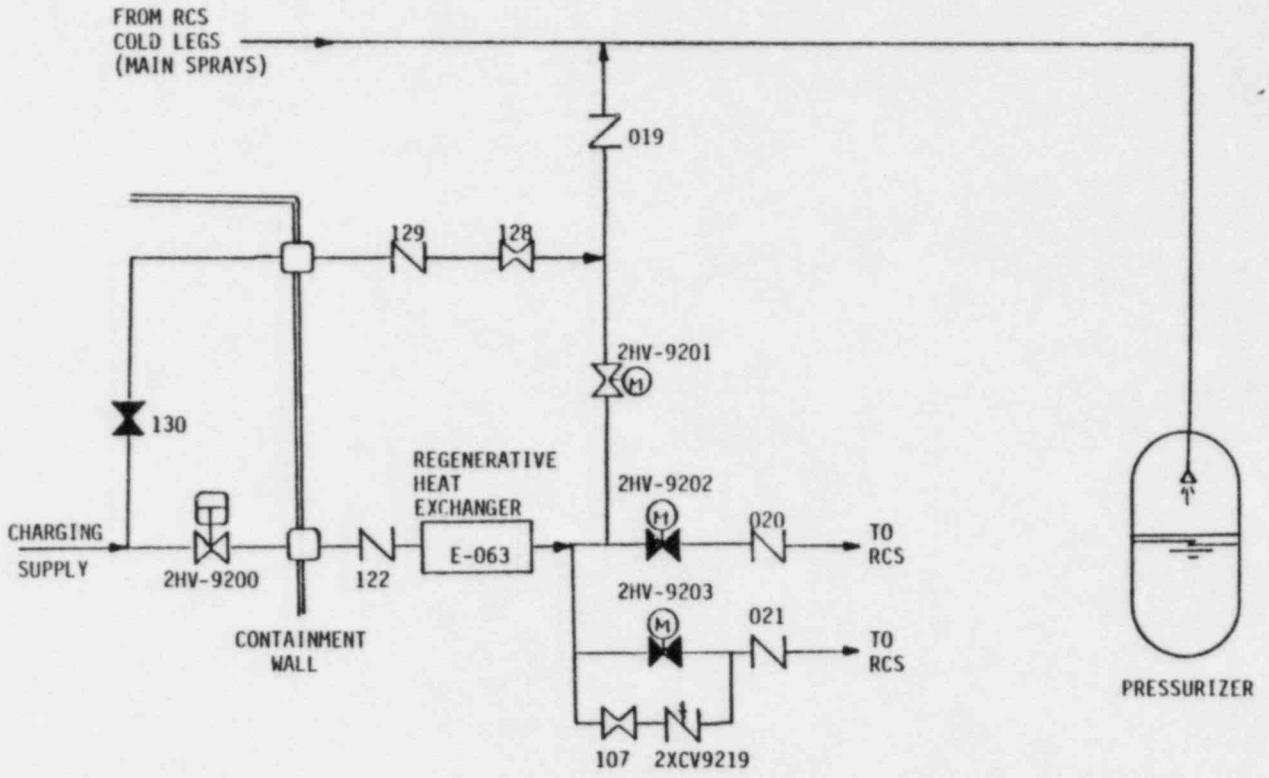
The Auxiliary Spray support system dependency diagram is provided in Figure 6.2.1-3.

6.2.2 Assumptions

The following assumptions were made in performing the fault tree analysis:

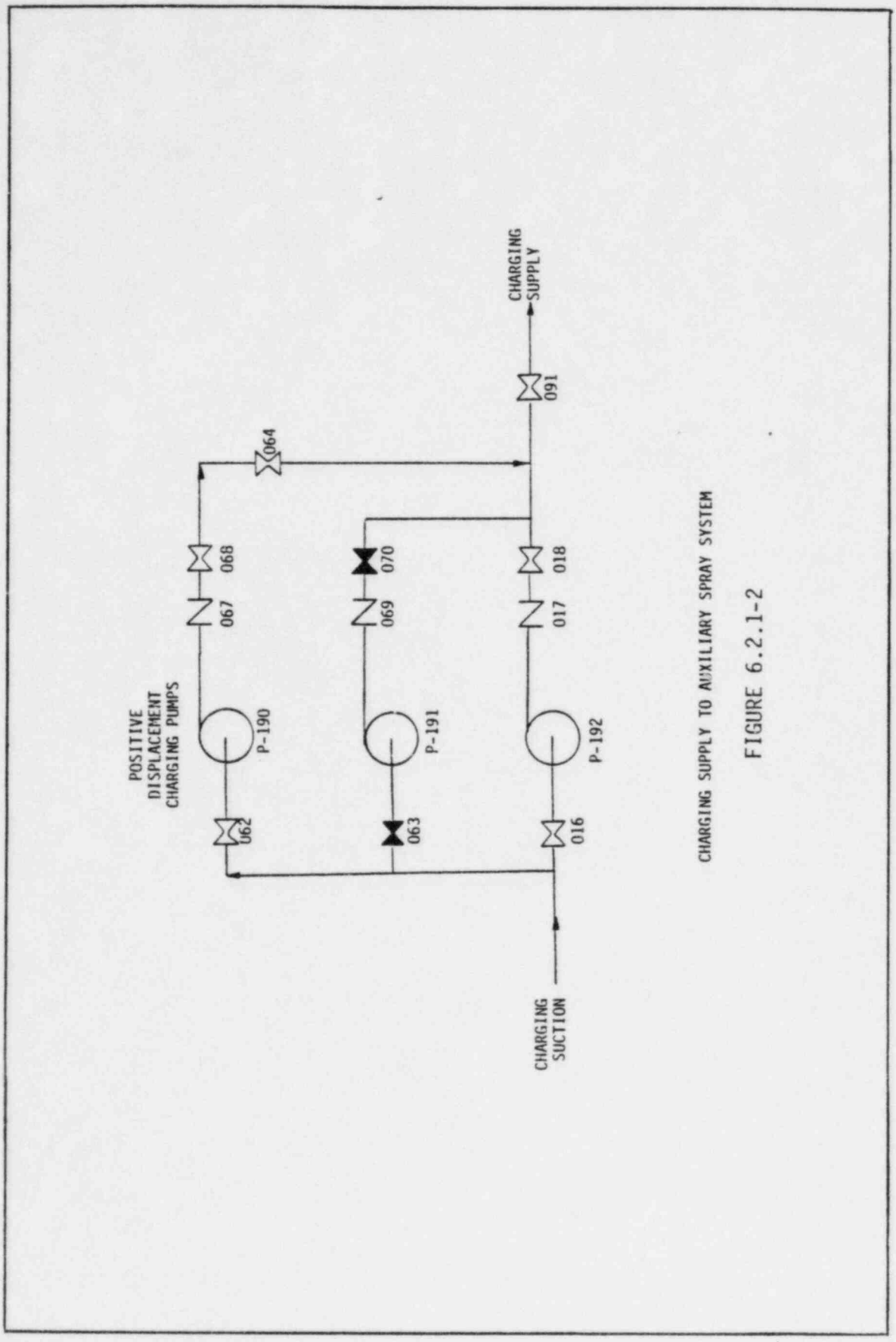
1. System failure is defined as the inability to deliver auxiliary spray flow to the pressurizer.

2. The pressurizer main spray valves are assumed to be closed for the following reasons:



AUXILIARY SPRAY SYSTEM

FIGURE 6.2.1-1

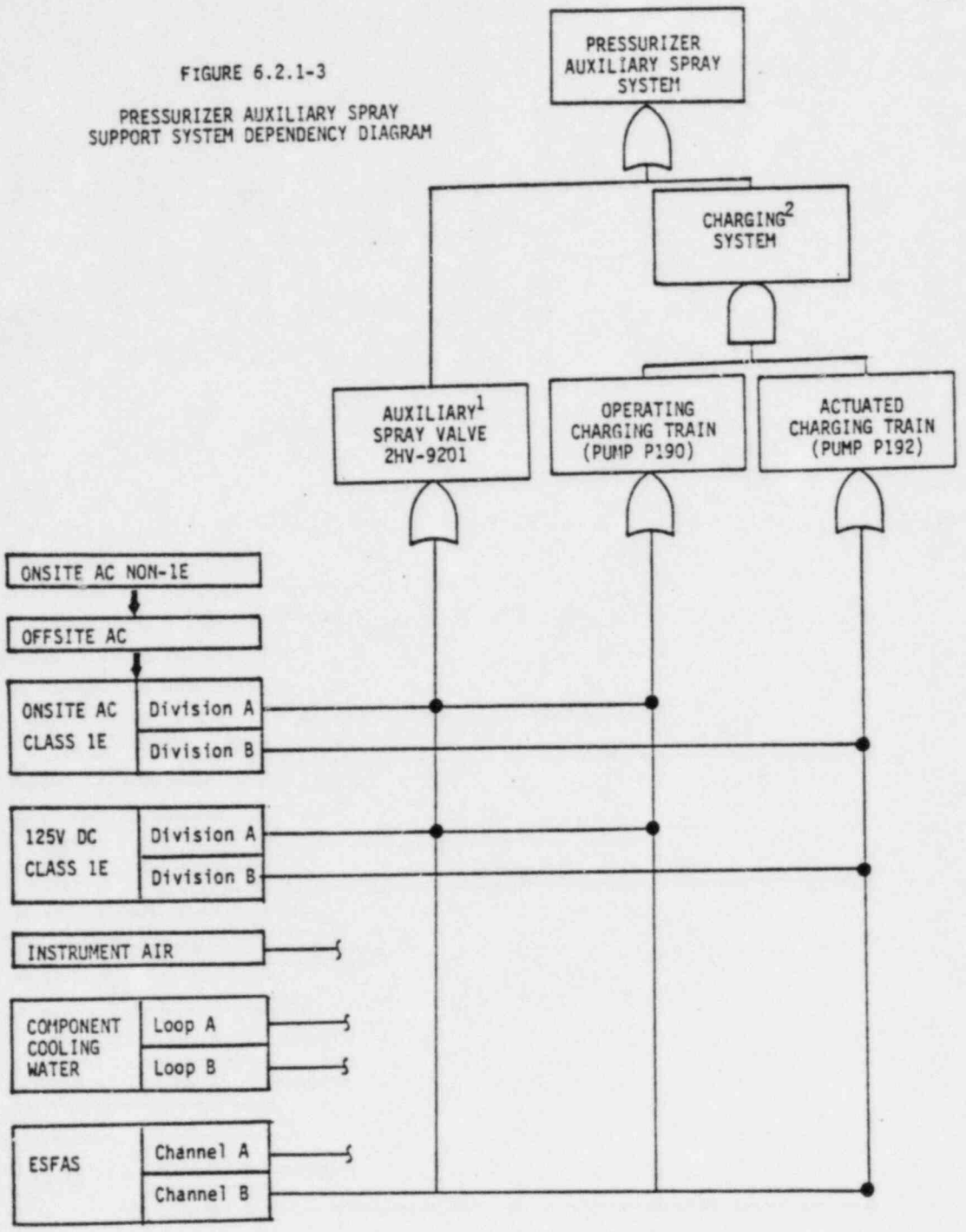


CHARGING SUPPLY TO AUXILIARY SPRAY SYSTEM

FIGURE 6.2.1-2

FIGURE 6.2.1-3

PRESSURIZER AUXILIARY SPRAY
SUPPORT SYSTEM DEPENDENCY DIAGRAM



[1]A manual auxiliary spray valve (operated with a handwheel) provides redundancy.

[2]Charging pump P191 is assumed to be down for maintenance.

- the valves are normally closed
- the valves are fail closed
- if the valves were open, they would be closed by the PPCS immediately following the SGTR
- operating procedures require the operator to insure the main spray valves are closed prior to initiating of auxiliary spray.

3. Spring loaded check valve 2XCV9219 is not in the failed open position at the time of the initiating event.

4. The following operator actions were considered:

   - Operator action to open auxiliary spray valve 2HV-9201 and throttle closed charging line valves 2HV-9202 and 2HV-9203 from the control room. (Referred to as "Operator fails to initiate Auxiliary Spray Flow").
   - Operator action to open manual valve 130-C-334 if 2HV-9201 fails to open and operator action to close charging line stop valve 2HV-9200 if normal charging flow is not terminated. (Referred to as "Operator fails to achieve Auxiliary Spray Flow"). It should be noted that the failure probability for this action is conditional on the availability of instrument air since charging line stop valve 2HV-9200 cannot be closed from the control room on loss of instrument air.

5. The operator is allowed 30 minutes to establish auxiliary spray flow from the time auxiliary spray flow is first desired.

6. The availability of charging flow is modelled by including CVCS components upstream of the secondary auxiliary spray flowpath to the suction side of the charging pumps. (See Figure 6.2.1-2). Suction flow is assumed to be available to the pumps due to the fact that modelling the redundant sources of CVCS inventory would unnecessarily complicate the fault tree without significantly contributing to the overall failure probability of the auxiliary spray system.

7. The operational status of the charging pumps is assumed to be as follows:

   - Charging pump P190 is operating at the time of SGTR.
   - Charging pump P191 is down for maintenance.
   - Charging pump P192 is required to start on a low pressurizer level signal from the Pressurizer Level Control System (PLCS) or on SIAS.

6.2.3 Results

The fault tree logic diagram for Fail to Deliver Auxiliary Spray Flow was used to evaluate the specific cases required as input to various event trees. For the SGTR event trees where offsite power is available at the time of the initiating event, the fault tree model does not include grid collapse following turbine trip as a component failure, i.e., the probability of grid collapse on turbine trip is 0.0. For the SGTR with Coincident LOOP event trees, the fault tree model assumes the grid is lost on turbine trip, i.e., the probability of grid collapse on turbine trip is 1.0. For the Loss of Secondary Heat Sink event tree the probability of failing to deliver auxiliary spray flow is conditional on the loss of MFW and the loss of AFW. The dependencies which exist between these three systems have been incorporated into the Auxiliary Spray System failure probability.

The quantitative results of the analyses are presented as Case One through Three respectively in Table 6.2.3-1. The confidence distributions of the failure probabilities are presented in terms of the median values and error factors. The error factor is defined as the ratio of the 95 to 50 percentile.

Table 6.2.3-2 contains a list of the dominant cutsets for each case presented in Table 6.2.3-1. Included in the table is a brief description of each cutset as well as the percent contribution to the total failure probability. The percentage is based on a point estimate ratio.

TABLE 6.2.3-1

FAILURE PROBABILITIES FOR SONGS AUXILIARY SPRAY SYSTEM

Case Number	Description	Failure Probability (Median Value)	Error Factor
One	Fail to Deliver Auxiliary Spray Flow-System Unavailability given offsite power is available at the time of the initiating event	2.1E-3	5
Two	Fail to Deliver Auxiliary Spray Flow-System Unavailability given offsite power is unavailable at the time of the initiating event	2.2E-2	5
Three	Fail to Deliver Auxiliary Spray Flow-System Unavailability given loss of MFW and Loss of AFW	6.2E-3	4

TABLE 6.2.3-2

DOMINANT CUTSETS FOR SONGS AUXILIARY SPRAY SYSTEM

Case Number	Cutset		Description	% of Total Failure Probability
One	1.	PVX00461	Operator fails to initiate auxiliary spray	96%
	2.	ELBN0167	4.16KV Bus 2A08 fails on TT and	.8%
		PVX00462	Operator fails to achieve auxiliary spray flow (through secondary flowpath)	
	3.	ELBN0178	4.16KV Bux 2A09 fails on TT and	.8%
		PVX00462	Operator fails to achieve auxiliary spray flow	
Two	1.	PVX00462	Operator fails to achieve auxiliary spray flow	49%
	2.	PVX00461	Operator fails to initiate auxiliary spray flow	11%
	3.	PVMB0465	Charging stop valve 2HV-9200 fails to close (mechanical malfunction)	6.2%
Three	1.	PVX00461	Operator fails to initiate auxiliary spray flow	63%
	2.	EBGP0160	Spurious grid collapse	11%
		PVX00462	Operator fails to achieve auxiliary spray flow	
	3.	EXUN0102	Reserve auxiliary transformer 2XR1 fails	5.6%
		PVX00462	Operator fails to achieve auxiliary spray flow	

6.3 CONTAINMENT HEAT REMOVAL SYSTEM

6.3.1 System Description

The objectives of the Containment Heat Removal System are to reduce the containment temperature and pressure following a Loss of Coolant Accident or Main Steam Line Break by removing thermal energy from the containment. These cooling systems also serve to limit offsite radiation levels by reducing the pressure differential between the containment atmosphere and the external environment. The containment heat removal systems include the Containment Spray System and the Emergency Containment Cooling System. Both the Containment Spray System and the Emergency Containment Cooling System consist of two completely redundant and independent trains. Each train of the Containment Spray System and the Emergency Containment Cooling System is designed for 50% of the required heat removal capacity. Thus, the following combinations constitute 100% of the required heat removal capacity.

1. Two-out-of-two Containment Spray System trains, or
2. Two-out-of-two Emergency Containment Cooling System Trains, or
3. One containment spray train and one emergency containment cooling train.

The Containment Spray System utilizes the refueling water tanks, the containment sump, two containment spray pumps, two shutdown cooling heat exchangers, two independent spray headers, and associated valves, piping, and instrumentation as shown in Figure 6.3.1-1. The spray system is actuated by the Containment Spray Actuation Signal (CSAS) and the Safety Injection Actuation Signal (SIAS). The SIAS starts the containment spray pumps in order to minimize spray delay time and the CSAS opens the spray control valves to the containment.

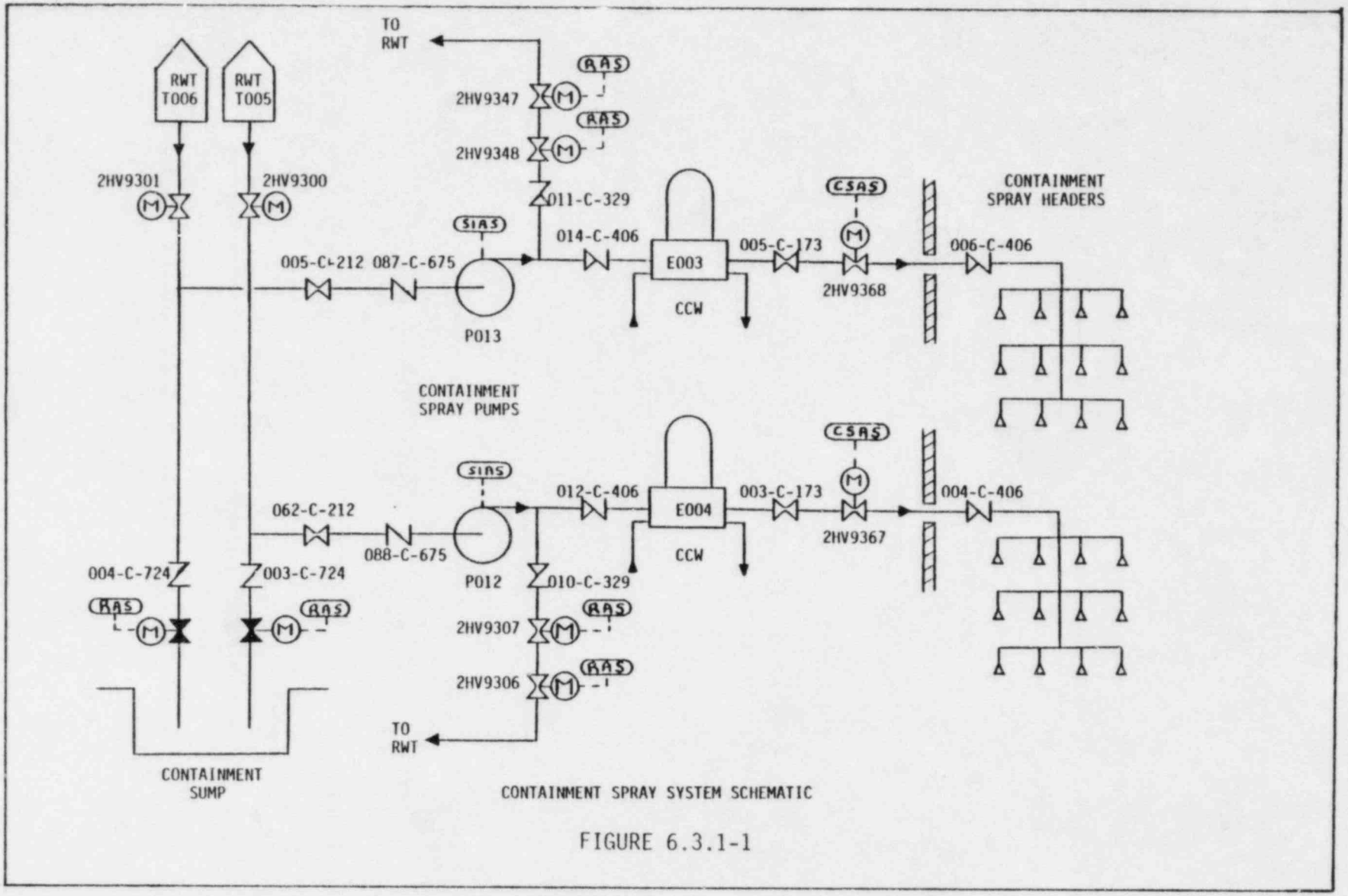

TO
RWT
RWT
T006
RWT
T005
RAS
2HV9347
RAS
2HV9348
2HV9301
2HV9300
011-C-329
SIAS
014-C-406
E003
005-C-173
CSAS
CONTAINMENT
SPRAY HEADERS
006-C-406
005-C-212
087-C-675
P013
CCW
2HV9368
CONTAINMENT
SPRAY PUMPS
SIAS
012-C-406
E004
003-C-173
CSAS
004-C-406
062-C-212
088-C-675
P012
CCW
2HV9367
004-C-724
003-C-724
010-C-329
RAS
RAS
2HV9307
RAS
2HV9306
TO
RWT
CONTAINMENT
SUMP
CONTAINMENT SPRAY SYSTEM SCHEMATIC

FIGURE 6.3.1-1

During the injection mode the actuated spray pumps take suction from the refueling water tanks and discharge to the containment headers. These headers contain spray nozzles that break the flow into small droplets which are then dispersed into the containment atmosphere to absorb heat. When the water droplets reach the containment floor, they drain to the containment sump where they remain until the recirculation mode begins.

When the refueling water tank inventory decreases to 19% of its minimum allowed volume, a recirculation actuation signal (RAS) is generated. Generation of RAS opens the containment sump isolation valves to allow automatic transfer of the containment spray pumps suction from the refueling water tanks to the containment sump. Transfer of pump suction ensures that containment cooling is maintained.

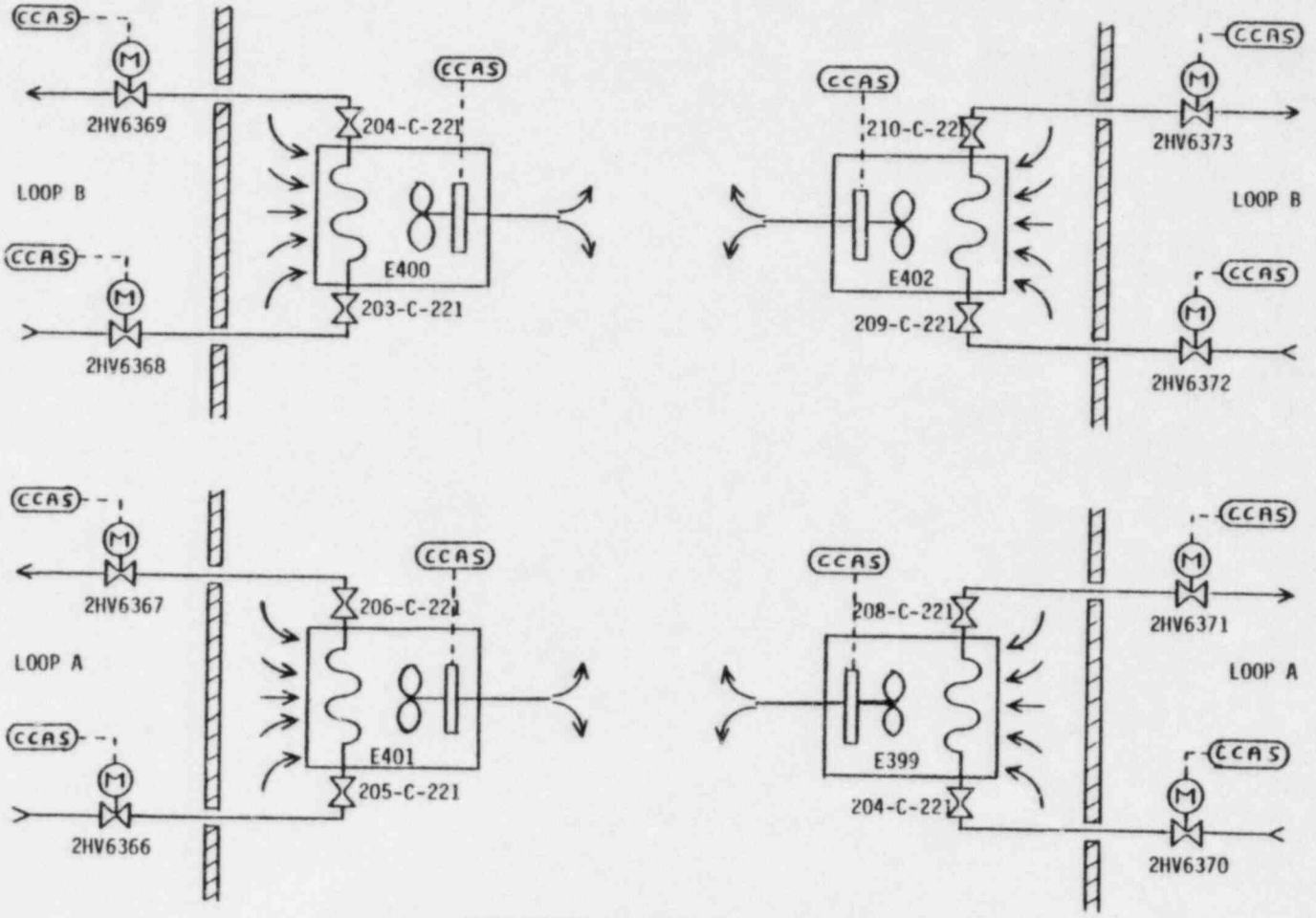
The Emergency Containment Cooling System consists of four separate fan cooler units (two per train) inside the containment as shown in Figure 6.3.1-2. The cooling system is actuated by a containment cooling actuation signal (CCAS). Upon receipt of a CCAS the component cooling water return line valves are opened and the fans start. Once the fans start, they continue to operate until the containment pressure decreases below 2 psig and CCAS is reset.

The containment heat removal support system dependency diagram is provided in Figure 6.3.1-3.

6.3.2 Assumptions

The following assumptions were made in performing the fault tree analysis:

1. Insufficient containment heat removal is defined as containment cooling which is less than 100% of the combined capacity of the Containment Spray and Emergency Containment Cooling Systems. Based on the definition, the bounding system failure combinations are:

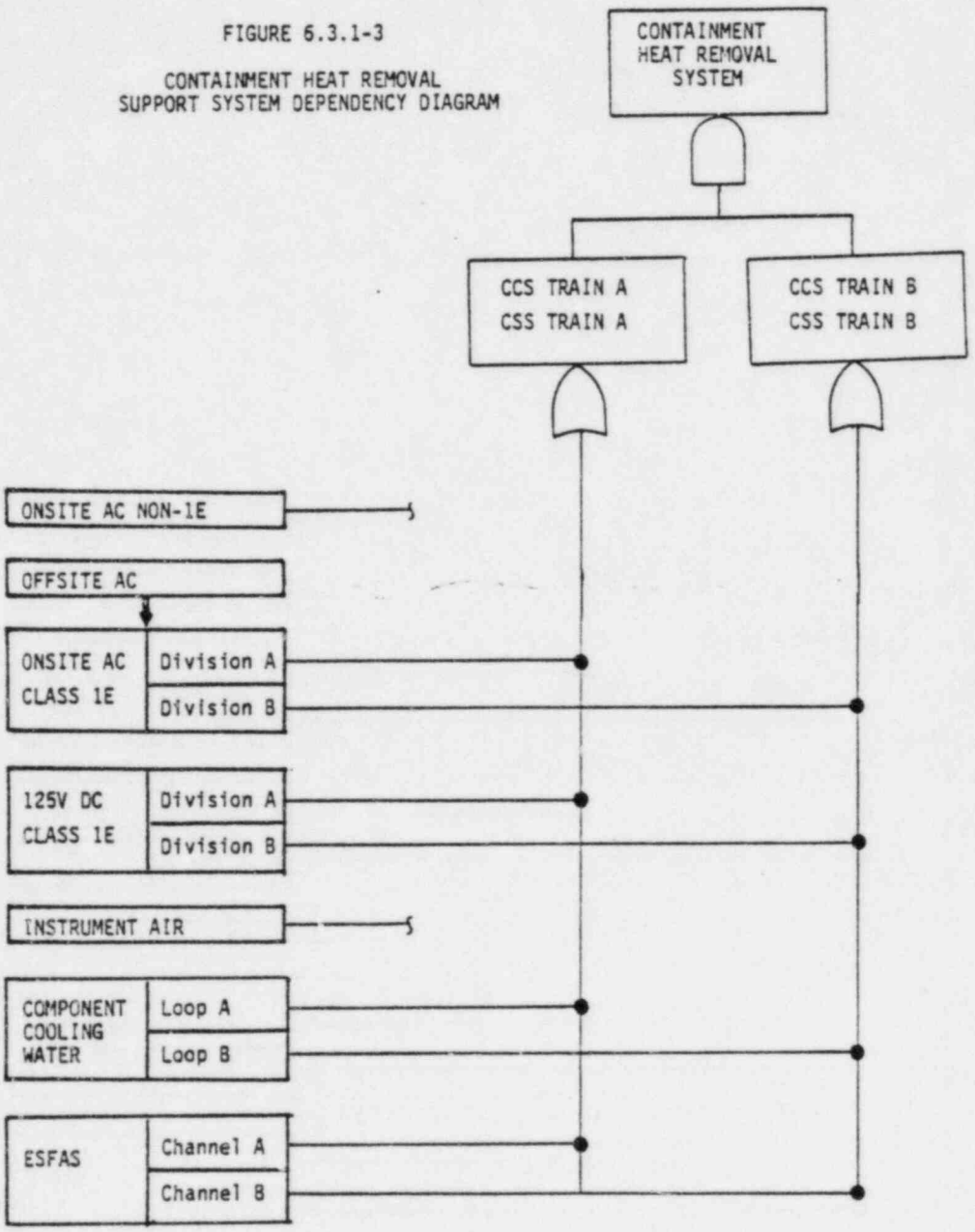


CONTAINMENT EMERGENCY FAN COOLERS

FIGURE 6.3.1-2

FIGURE 6.3.1-3

CONTAINMENT HEAT REMOVAL
SUPPORT SYSTEM DEPENDENCY DIAGRAM



a) Effective loss of one fan cooler and both containment spray system trains

b) Effective loss of three fan coolers and one containment spray system train.

2. The normal containment fan coolers are not credited for removing containment heat following Loss of Coolant Accident or Steam Line Break Events.

3. Isolation of the containment spray pump mini-flow lines could result in dead headed operation and damage to the pumps.

6.3.3 Results

The fault tree logic diagram for Fail to Provide Containment Cooling was used to evaluate the probability of failing to provide sufficient containment heat removal for the PORV LOCA event trees. Because the fan coolers are operating in a harsh environment, their associated component failure rates are greater than those for a normal operating environment. Therefore, the unreliability of the Containment Heat Removal System at eight hours into the event was found to be greater than the system unavailability. Separate analyses were used to determine both the system unavailability and the system unreliability. The results are presented as Case One and Case Two in Table 6.3.3-1. For the LOHS with Feed and Bleed Operation event tree, only the portion of the logic diagram including the Containment Spray System was used to generate a failure probability for Failure of Containment Sprays. As discussed in Section 5.1.4.2, failure of the Containment Spray System has an effect on the volume of RWT inventory available for feed and bleed operation. For this event tree, the probability of failing to actuate the containment sprays is conditional on the loss of MFW and the loss of AFW. The dependencies which exist between the MFW, AFW, and Containment Spray systems have been incorporated into the Containment Spray System failure probability. These results are presented as Case Three in Table 6.3.3-1.

For each case, the confidence distribution of the failure probabilities are presented in terms of the median values and error factors. The error factor is defined as the ratio of the 95 to 50 percentile.

Table 6.3.3-2 contains a list of the dominant cutsets for each case presented in Table 6.3.3-1. Included in the table is a brief description of each cutset as well as the percent contribution to the total failure probability. The percentage is based on a point estimate ratio.

TABLE 6.3.3-1

FAILURE PROBABILITIES FOR SONGS CONTAINMENT HEAT REMOVAL SYSTEM

Case Number	Description	Failure Probability (Median Value)	Error Factor
One	Fail to Provide Containment Cooling - System Unavailability	5.6E-5	7
Two	Fail to Provide Containment Cooling - System Unreliability at 8 hours	7.0E-5	9
Three	Failure of Containment Sprays - System Unavailability given loss of MFW and loss of AFW	1.3E-3	16

TABLE 6.3.3-2

DOMINANT CUTSETS FOR SONGS CONTAINMENT HEAT REMOVAL SYSTEM

Case Number	Cutset	Description	% of Total Failure Probability
One	1. FSSR0413 FSSR0422 HSS00414	SIASA not generated and SIASB not generated and Operator fails to generate SIAS from control room	13%
	2. GPMJ0721 CVXT0618	CS Pump P012 fails to start and CCW HX E-002 outlet valve 2HCV-6215 not open	4.4%
	3. GPMJ0736 CVXT0612	CS Pump P013 fails to start and CCW HX E-001 outlet valve 2HCV-6510 not open	4.4%
Two	1. GWFC0762 CVXT0618	Fan cooler E-401 fails to operate CCW HX E-002 outlet valve 2HCV-6215 not open	8.4%
	2. GWFC0749 CVXT0618	Fan cooler E-399 fails to operate CCW HX E-002 outlet valve 2HCV-6215 not open	8.4%
	3. GWFC0768 CVXT0612	Fan cooler E-402 fails to operate CCW HX E-001 outlet valve 2HCV-6510 not open	8.4%
	4. GWFC0756 CVXT0612	Fan cooler E-400 fails to operate CCW HX E-001 outlet valve 2HCV-6510 not open	8.4%
Three	1. HVNT0418	Miniflow line manual [illegible] 068-C-076 plugged	9.2%
	2. EBGP0160 EDXJ0150 EDXJ0151	Spurious grid collapse and DG 2G002 fails to start and DG 2G003 fails to start	4.9%
	3. EBGP0160 EDXJ0150 EDXC0153	Spurious grid collapse and DG 2G002 fails to start and DG 2G003 fails to run	3.9%
	4. EBGP0160 EDXC0152 EDXJ0151	Spurious grid collapse and DG 2G002 fails to run and DG 2G003 fails to start	3.9%

6.4 POWER OPERATED RELIEF VALVES (PORVs)

For the PORV LOCA event trees, fault tree analyses were performed to determine the occurrence frequencies of the following PORV LOCA initiating events:

- PORV LOCA Following Loss of Secondary Heat Sink. This type of PORV LOCA refers to manually opening the PORV flow paths. The steam generators are unavailable to remove RCS heat.

- PORV LOCA Following SGTR. This type of PORV LOCA refers to manually opening the PORV flowpaths following a tube rupture in one steam generator. The unaffected steam generator is available to remove RCS heat.

- Spurious PORV LOCA. This type of PORV LOCA includes error induced opening of either PORV flowpath. Both steam generators are available to remove RCS heat.

The frequencies for loss of secondary heat sink and tube rupture in one steam generator were incorporated into the fault trees to evaluate the occurrence frequencies for these types of PORV LOCA. Nuclear operating experience data (27) was used along with an assumed valve testing frequency that varies from two weeks to quarterly to evaluate the Spurious PORV LOCA occurrence frequency.

In order to evaluate the unavailability of the assumed PORV for back-up RCS depressurization capability should the Auxiliary Spray System be unavailable, a fault tree logic diagram was used to determine the probability of failing to establish flow through one PORV.

6.4.1 System Description

An assumed Powered Operated Relief Valve (PORV) design for SONGS is presented in Figure 6.4.1-1. The design features two 50% capacity flow paths. Each path contains a motor operated block valve and a PORV. During plant operations the motor operated block valves and the PORVs are closed. These valves are designed to be opened manually to reduce RCS pressure following a steam generator tube rupture event. The role of PORVs following a SGTR is discussed in Section 7.2.5. These valves are also opened manually to establish a means of alternate decay heat removal following a loss of the secondary heat sink. The role of PORVs following a loss of secondary heat sink is further discussed in Section 6.5, "Primary Feed and Bleed System". The PORVs are not opened by signals that are generated automatically, therefore, they do not prevent or minimize challenges to the primary safety valves. The PORV support system dependency diagram is provided in Figure 6.4.1-2.

6.4.2 Assumptions

The following assumptions were made in performing the frequency evaluations for PORV LOCA:

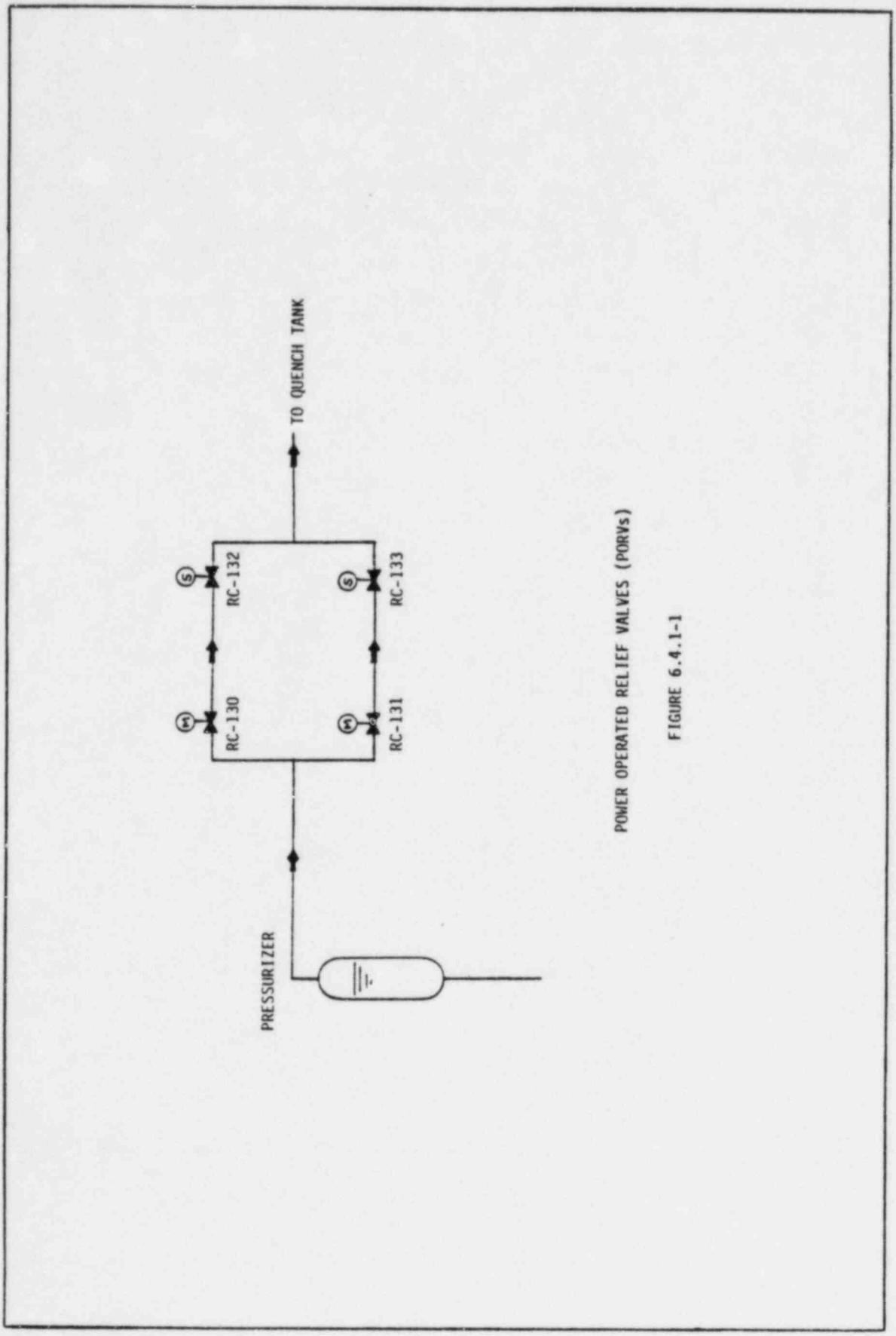
1. Both PORV flowpaths are required following a loss of secondary heat sink event.

2. At least one PORV flowpath is required following a SGTR.

3. Spurious PORV LOCA refers to error induced opening of either PORV flowpath.

4. The frequency for testing the valves varies from two weeks to quarterly.

5. Operator action is required to establish or terminate flow through the PORVs.

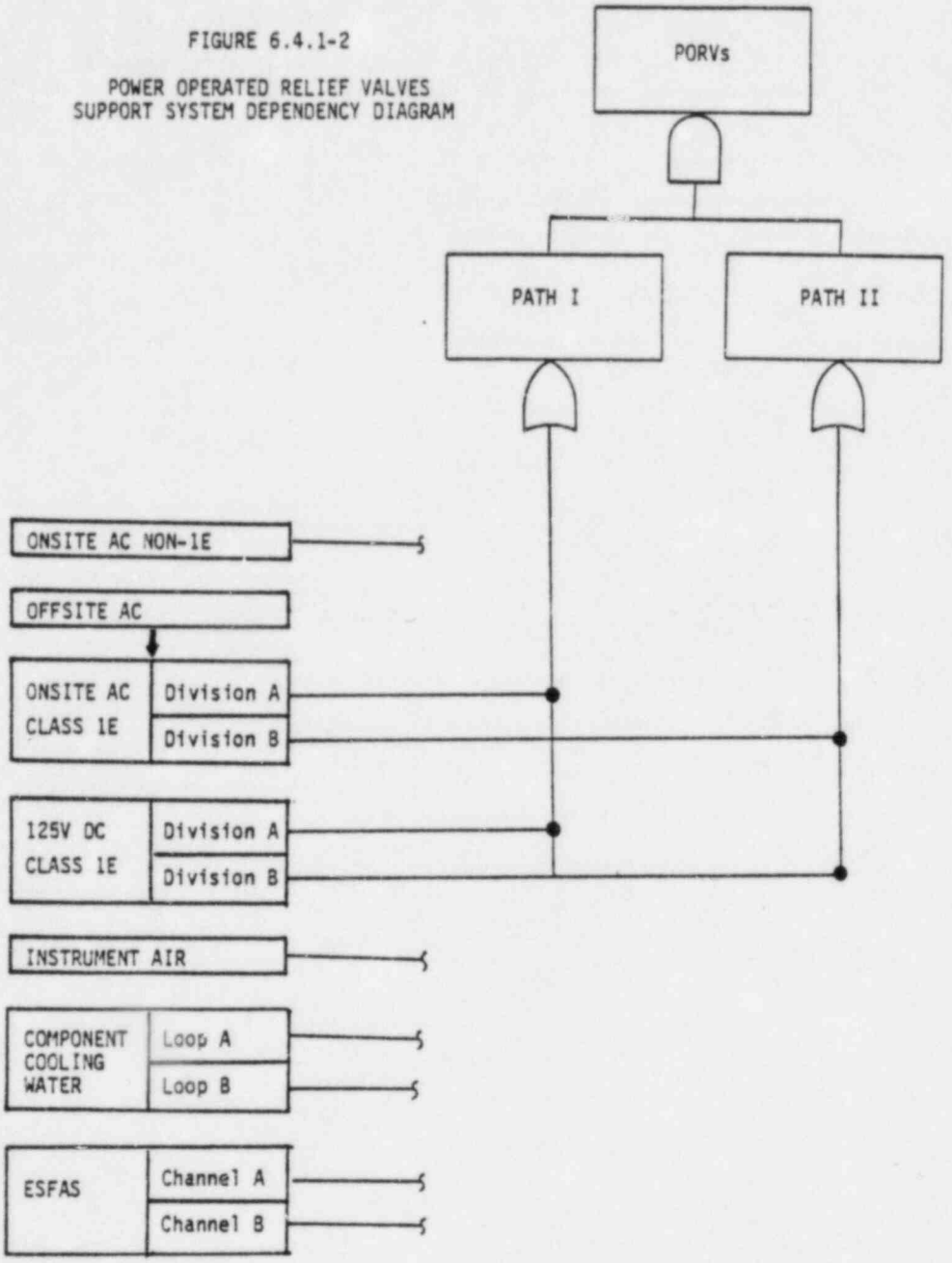


POWER OPERATED RELIEF VALVES (PORVs)

FIGURE 6.4.1-1

FIGURE 6.4.1-2

POWER OPERATED RELIEF VALVES
SUPPORT SYSTEM DEPENDENCY DIAGRAM



The following assumptions were made in performing the fault tree analysis for Failure to Establish Flow Through One PORV:

1. Failure to establish flow through the PORVs is defined as the inability to fully open one block valve and the associated PORV.

2. Motor operated block valves RC-130 and RC-131 are loaded on 480 VAC motor control centers 2BE and 2BJ respectively.

3. PORV RC-132 and RC-133 are loaded on 125 VDC buses 2D3 and 2D4 respectively.

4. Operator action is required to establish flow through the PORVs.

6.4.3 Results

For the PORV LOCA event trees, fault tree analysis was used to determine the following initiating event frequencies:

- PORV LOCA following loss of secondary heat sink.
- PORV LOCA following SGTR.
- Spurious PORV LOCA

In order to determine the unavailability of the PORVs, a fault tree logic diagram was used to evaluate the probability of failing to establish flow through one PORV. The model was used to evaluate the following cases:

- offsite power is assumed to be available at the time of the initiating event.

- offsite power is included as a component with a failure probability of 10^{-3} (16). (It should be noted that this is a generic value and for SONGS this number might be lower, i.e., the transmission system has a high transient stability limit due to high installed capacity and extensive grid interconnections with other utilities).

- offsite power is assumed to be unavailable at the time of the initiating event.

The quantitative results of the analyses are presented as Cases One through Six respectively in Table 6.4.3-1. The confidence distributions of the initiating event frequencies and failure probabilities are presented in terms of the median values and associated error factors. The error factor is defined as the ratio of the 95 to 50 percentile.

Table 6.4.3-2 contains a list of the dominant cutsets for each case presented in Table 6.4.3-1. Included in the table is a brief description of each cutset as well as the percent contribution to the total frequency or failure probability. The percentage is based on a point estimate ratio.

TABLE 6.4.3-1

INITIATING EVENT FREQUENCIES AND FAILURE PROBABILITIES FOR SONGS PORVs

Case Number	Description	Median Value	Error Factor
One	PORV LOCA Following LOHS - Initiating Event Frequency	1.5E-6 per year	29
Two	PORV LOCA Following SGTR - Initiating Event Frequency	1.3E-4 per year	7
Three	Spurious PORV LOCA - Initiating Event Frequency	3.2E-5 per year	16
Four	Failure to Establish Flow through One PORV - System Unavailability given offsite power is available at the time of the initiating event	1.0E-3	10
Five	Failure to Establish Flow through One PORV - System Unavailability	1.2E-3	9
Six	Failure to Establish Flow through One PORV - System Unavailability given offsite power is unavailable at the time of the initiating event	7.5E-3	9

TABLE 6.4.3-2

DOMINANT CUTSETS FOR SONGS PORVs

Case Number	Cutset	Description	% of Total Frequency/ Probability
One	1. ZZZZ0902	Loss of MFW and	99%
	ZZZZ0901	Loss of AFW and	
	VVX00487	Operator fails to isolate the PORV flow paths	
Two	1. ZZZZ0900	Tube rupture in one SG and	99%
	VVX00487	Operator fails to isolate the PORV flow paths	
Three	1. VVMV0483	Pre-existing error on valve RC-133 and	23%
	ZZZZ0910	Valve RC-131 opens for testing and	
	VVX00478	Operator fails to isolate the PORV flow path	
	2. VVMV0482	Pre-existing error on valve RC-131 and	23%
	ZZZZ0908	Valve RC-133 opens for testing and	
	VVX00478	Operator fails to isolate the PORV flow path	
	3. VVMV0477	Pre-existing error on valve RC-132 and	23%
	ZZZZ0906	Valve RC-130 opens for testing and	
	VVX00478	Operator fails to isolate the PORV flow path	
	4. VVMV0476	Pre-existing error on valve RC-130 and	23%
	ZZZZ0904	Valve RC-132 opens for testing and	
	VVX00478	Operator fails to isolate the PORV flow path	
Four	1. VVZ00593	Operator fails to open one PORV and the associated block valve	> 99%
Five	1. VVZ00593	Operator fails to open one PORV and the associated block valve	99%

TABLE 6.4.3-2
(continued)
DOMINANT CUTSETS FOR SONGS PORVs

Case Number	Cutset	Description	% of Total Frequency/ Probability
Six	1. VVZ00593	Operator fails to open one PORV and the associated block valve	24%
	2. EDXJ0150 EDXJ0151	DG 2G002 fails to start and DG 2G003 fails to start	22%
	3. ELBN0172 EDXJ0150	4.16 KV Bus 2A06 fails on LOOP and DG 2G002 fails to start	17%
	4. ELBN0171 EDXJ0151	4.16 KV Bus 2A04 fails on LOOP and DG 2G003 fails to start	17%
	5. ELBN0171 ELBN0172	4.16 KV Bus 2A04 fails on LOOP and 4.16 KV Bus 2A06 fails on LOOP	13%

6.5 PRIMARY FEED AND BLEED SYSTEM

6.5.1 System Description

A conceptual Primary Feed and Bleed System for SONGS consists of Power Operated Relief Valves (PORVs), the High Pressure Safety Injection System and the Charging System. A schematic of the PORV design is presented in Figure 6.5.1-2. The PORV design consists of two trains of a power-operated relief valve and a motor-operated block valve in series. The PORV trains are located off the pressurizer and exhaust to the pressurizer quench tank.

A schematic of the SONGS HPSI System (Injection Mode) is presented in Figure 6.5.1-1. During the injection mode, the minimum flowlines downstream of each pump are kept open to prevent possible dead head operation. The pumps take suction from two RWTs and discharge through the eight HPSI header isolation valves via two redundant HPSI headers. The safety injection water then flows to the reactor vessel through a safety injection nozzle on each of the four RCS cold leg pipes. The HPSI System is connected to the diesel generator power system in the event of a loss of normal offsite power.

A schematic for charging flow to the RCS loops is presented in Figure 6.5.1-3. The charging pumps, located in the radwaste building, take suction from the volume control tank and return the purification flow to the RCS during plant steady state operations. Normally one pump is operating. The second and third pumps are automatically started as pressurizer level decreases. The pumps are positive displacement type with an integral leakage collection system. An automatic system maintains the water level in the volume control tank. A volume control tank low level signal causes a preset solution of concentrated boric acid and reactor makeup water to be introduced into the volume control tank. A low-low suction level signal closes the outlet valve on the volume control tank and switches the charging pump suction to the refueling water storage tank.

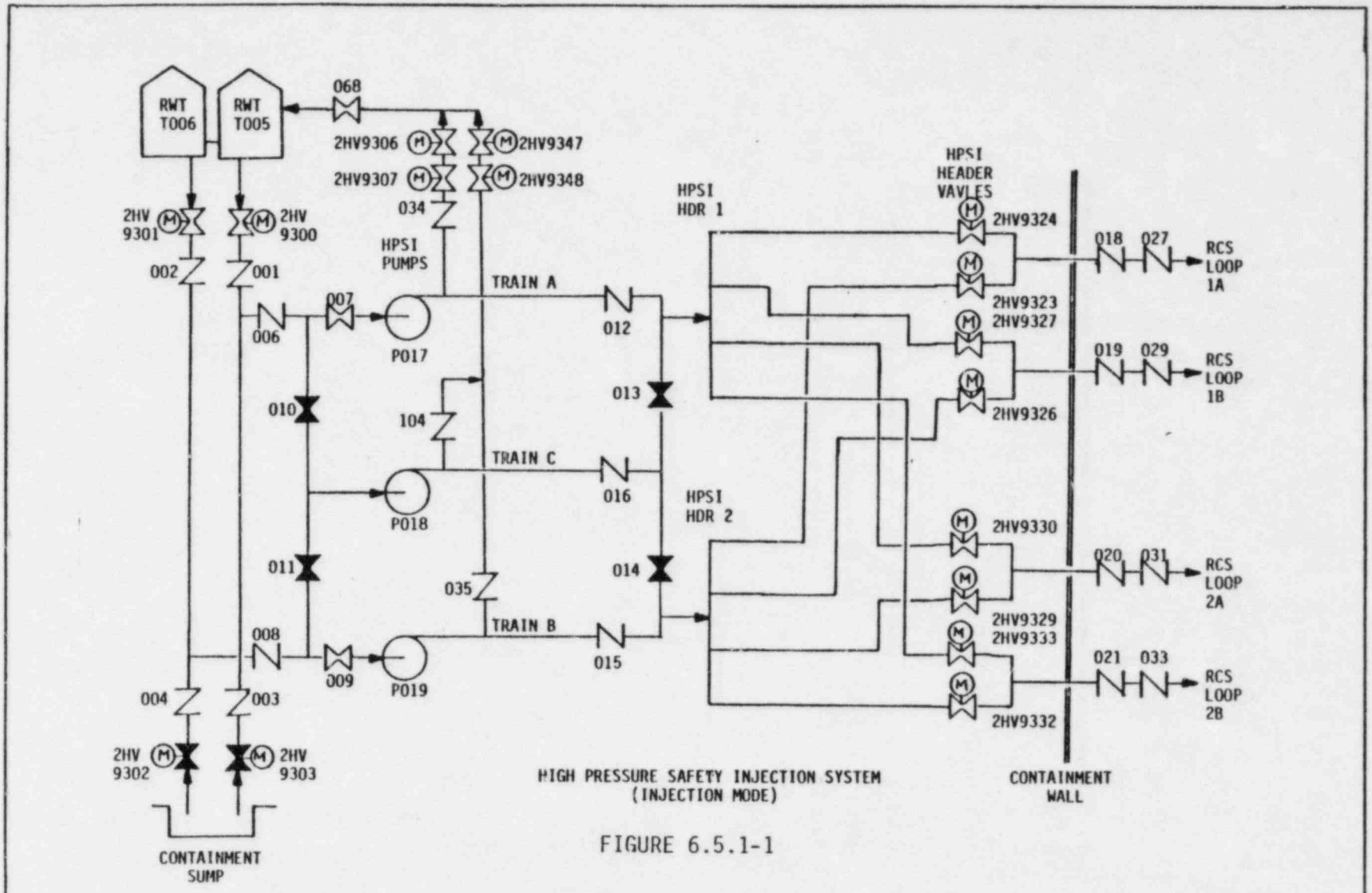
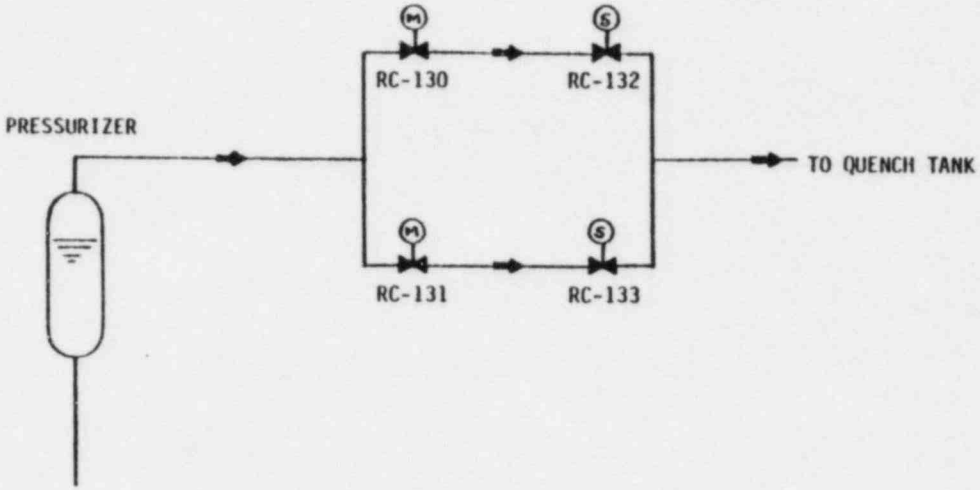
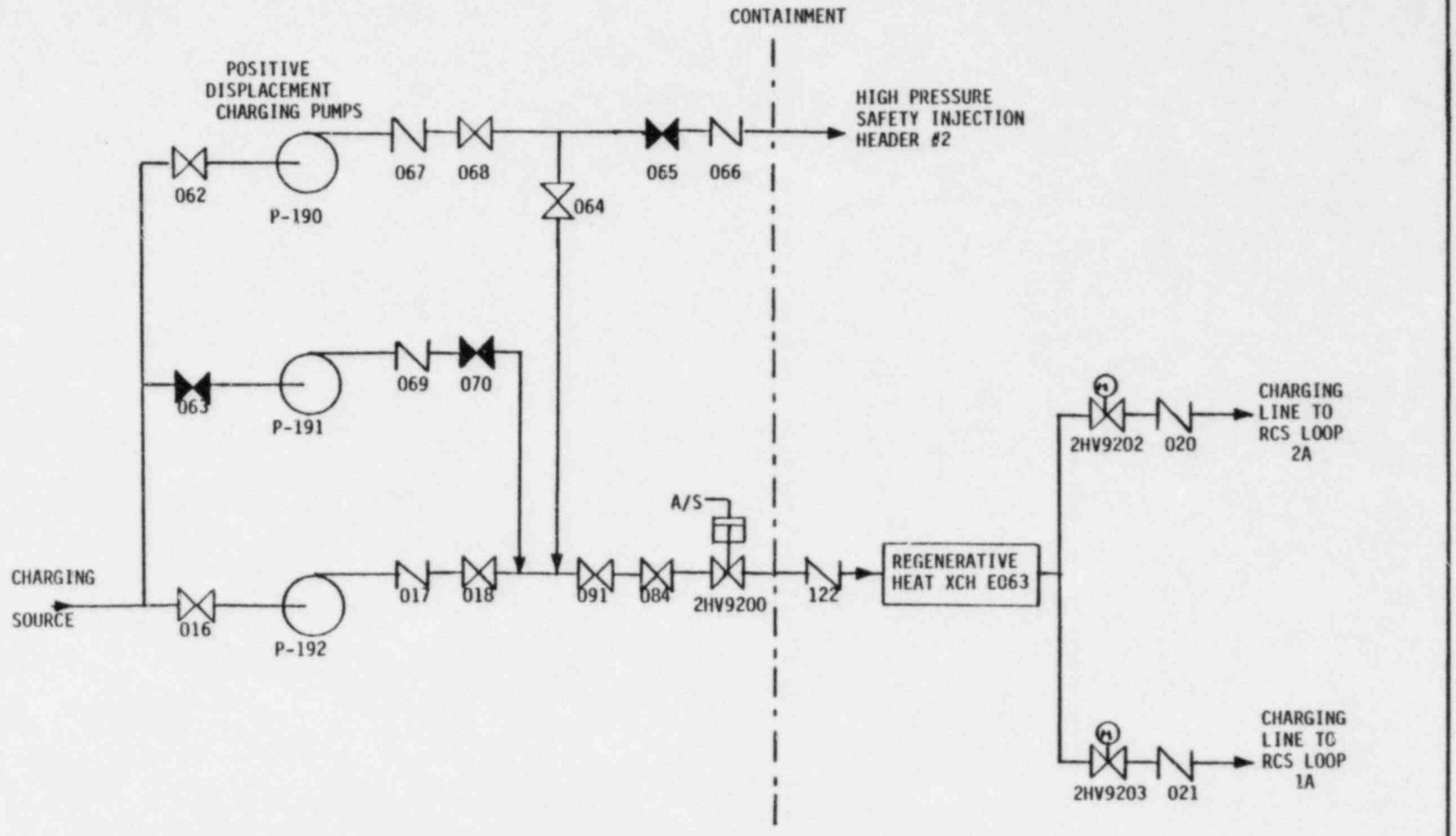

RWT T006
RWT T005
068
2HV9306
2HV9347
2HV9307
2HV9348
034
HPSI PUMPS
2HV 9301
2HV 9300
002
001
006
007
P017
TRAIN A
012
HPSI HDR 1
HPSI HEADER VAVLES
2HV9324
018
027
RCS LOOP 1A
2HV9323
2HV9327
019
029
RCS LOOP 1B
2HV9326
013
010
104
TRAIN C
016
P018
HPSI HDR 2
2HV9330
011
014
035
020
031
RCS LOOP 2A
2HV9329
2HV9333
TRAIN B
008
015
009
P019
021
033
RCS LOOP 2B
2HV9332
004
003
2HV 9302
2HV 9303
CONTAINMENT SUMP
HIGH PRESSURE SAFETY INJECTION SYSTEM (INJECTION MODE)
CONTAINMENT WALL

FIGURE 6.5.1-1



POWER OPERATED RELIEF VALVES (PORVs)

FIGURE 6.5.1-2



CHARGING SYSTEM

FIGURE 6.5.1-3

The Primary Feed and Bleed System is a manually actuated system. Following a loss of secondary heat sink (loss of main and auxiliary feedwater flow) the operator initiates feed and bleed by opening the PORVs and associated block valves. The injection mode of operation of the HPSI system is either manually initiated or automatically initiated following a SIAS. A SIAS is produced upon any two coincident low pressurizer pressure or high containment pressure signals. One charging pump is operating at time of initiating event. Primary pressure control and heat removal is accomplished by releasing steam through the PORVs and by providing primary inventory makeup from one HPSI pump and one Charging pump or two HPSI pumps until shutdown cooling entry conditions are achieved.

The Primary Feed and Bleed support system dependency diagram is provided in Figure 6.5.1-4.

6.5.2 Assumptions

The following assumptions were made in performing the fault tree analysis:

1. Failure of Feed and Bleed Operation is defined as the inability to establish flow through the PORVs and deliver sufficient HPSI and charging flow to the reactor core.

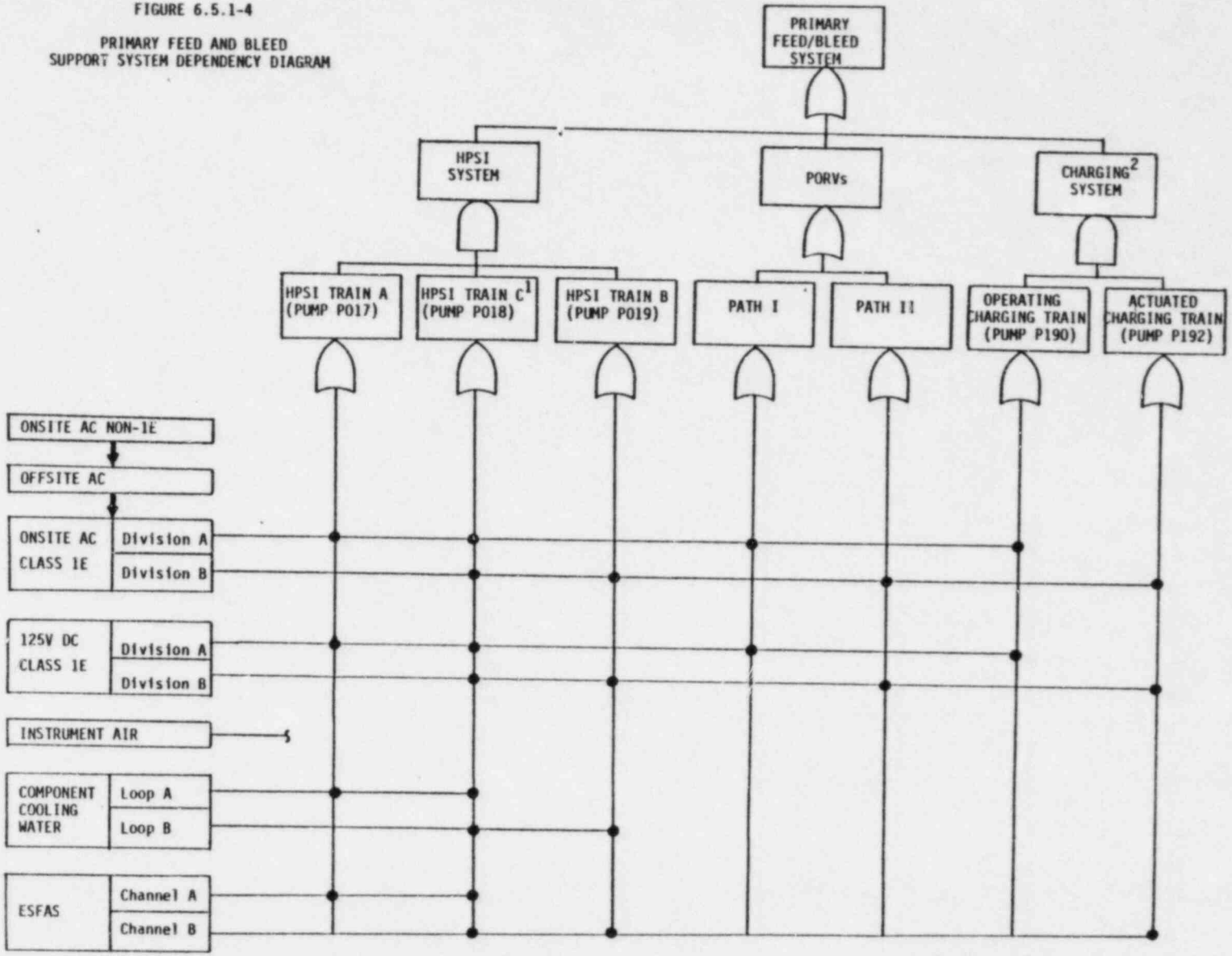
2. Operation of both PORV trains is required to establish sufficient flow through the PTRS.

3. Sufficient flow is defined as one HPSI pump flow delivered to two RCS loops, (two flow paths are required to deliver the flow from one pump), and one charging pump flow delivered to one RCS charging line or two HPSI pump flow delivered to two RCS loops.

4. Isolation of the HPSI pumps mini-flow lines could result in dead head operation and damage to the pumps.

FIGURE 6.5.1-4

PRIMARY FEED AND BLEED
SUPPORT SYSTEM DEPENDENCY DIAGRAM



[1]HPSI Pump P018 is aligned for manual actuation, however, it has the capability to start automatically on either SIAS A or SIAS B.

[2]Charging Pump P141 is assumed to be down for maintenance.

5. HPSI pumps P017 and P019 are available to start on SIAS. HPSI pump P018 is on standby and operator action is required to establish flow.

6. The following operator actions were considered:

   - Manual opening of the PORVs and block valves. (Human Error Probability of 0.025). The operator is allowed 20 minutes to open the PORVs and block valves.

   - Manual generation or backup of SIAS from the control room.

   - Operator action to establish flow from standby HPSI Pump P018. This includes the operator actions required to:

     - unlock and open manual valves

HPSI	013-C-075	CCW	258-D-387
	014-C-075		259-D-387
	010-C-212		231-D-387
	011-C-212		

     - unlock and open check vaAlve 104-C-329

     - start HPSI pump P018

7. HPSI Pump P018 is normally aligned to receive power from 4.16 KV Bus 2A04. It can be manually transferred to 4.16 KV Bus 2A06.

8. The containment sump isolation valves are closed.

9. Component Cooling Water (CCW) is required for successful HPSI pump operation.

10. The HPSI system is tested at startup and once every three months. If pump maintenance is required, manual valves 007-C-212 or 009-C-212 may be closed and inadvertently left in the wrong position. However, all other normally open valves will be assumed to remain open during plant operation. If a valve were inadvertently in the wrong position, it would be discovered during the tests. The only failure mode considered for these valves is plugging.

11. One charging pump, P190, is operating at the time of the initiating event; one charging pump is in maintenance (P191); the remaining pump is available to start on SIAS (P192).

12. The availability of charging flow is modelled by including CVCS components from the charging lines to the RCS loops, to the suction side of the charging pumps. Suction flow is assumed available to the pumps due to the fact that modelling the redundant sources of CVCS inventory would unnecessarily complicate the fault tree without significantly contributing to the overall failure probability of the Feed and Bleed System.

6.5.3 Results

The fault tree logic diagram for Failure of Feed and Bleed Operation was used to determine the probability of failing to achieve feed and bleed operation for the Loss of Secondary Heat Sink with Feed and Bleed Operation event tree. The model was used to evaluate the following cases:

- Failure of feed and bleed operation

- Failure of feed and bleed operation given loss of MFW and loss of AFW.

For Case Two the dependencies which exist between the three systems (Feed and Bleed, MFW and AFW) have been incorporated into the Feed and Bleed System failure probability. The quantitative results of the analyses are presented in Table 6.5.3-1. The confidence distributions of the failure probabilities are presented in terms of the median values and associated error factors. The error factor is defined as the ratio of the 95 to 50 percentile.

Table 6.5.3-2 contains a list of the dominant cutsets for each case presented in Table 6.5.3-1. Included in the table is a brief description of each cutset as well as the percent contribution to the total failure probability. The percentage is based on a point estimate ratio.

TABLE 6.5.3-1

FAILURE PROBABILITIES FOR SONGS PRIMARY FEED AND BLEED SYSTEM

Case Number	Description	Failure Probability (Median Value)	Error Factor
One	Failure of Feed and Bleed Operation - System Unavailability	3.7E-2	4
Two	Failure of Feed and Bleed Operation - System Unavailability given loss of MFW and loss of AFW	5.2E-2	4

TABLE 6.5.3.2

DOMINANT CUTSETS FOR SONGS FEED AND BLEED SYSTEM

Case Number	Cutset	Description	% of Total Failure Probability
One	1. VVZ00593	Operator fails to initiate feed and bleed operation	83%
	2. VVSA0590	PORV RC-133 fails to open	3.3%
	3. VVSA0589	PORV RC-132 fails to open	3.3%
	4. VVMA0587	Motor block valve RC-130 fails to open	3.3%
	5. VVMA0588	Motor block valve RC-131 fails to open	3.3%
Two	1. VVZ00593	Operator fails to initiate feed and bleed operation	62%
	2. EBGP0160 EDXJ0151	Spurious grid collapse and DG 2G003 fails to start	4.4%
	3. EBGP0160 EDXJ0150	Spurious grid collapse and DG 2G002 fails to start	4.4%
	4. EBGP0160 EDXC0153	Spurious grid collapse and DG2G003 fails to run	3.5%
	5. EBGP0160 EDXC0152	Spurious grid collapse and DG 2G002 fails to run	3.5%

6.6 TURBINE BYPASS SYSTEM AND TURBINE TRIP

Various functional modes of the Turbine Bypass System were evaluated for input to the systemic/action level event trees. For the SGTR event trees, fault tree logic diagrams were used to evaluate the following TBS functions:

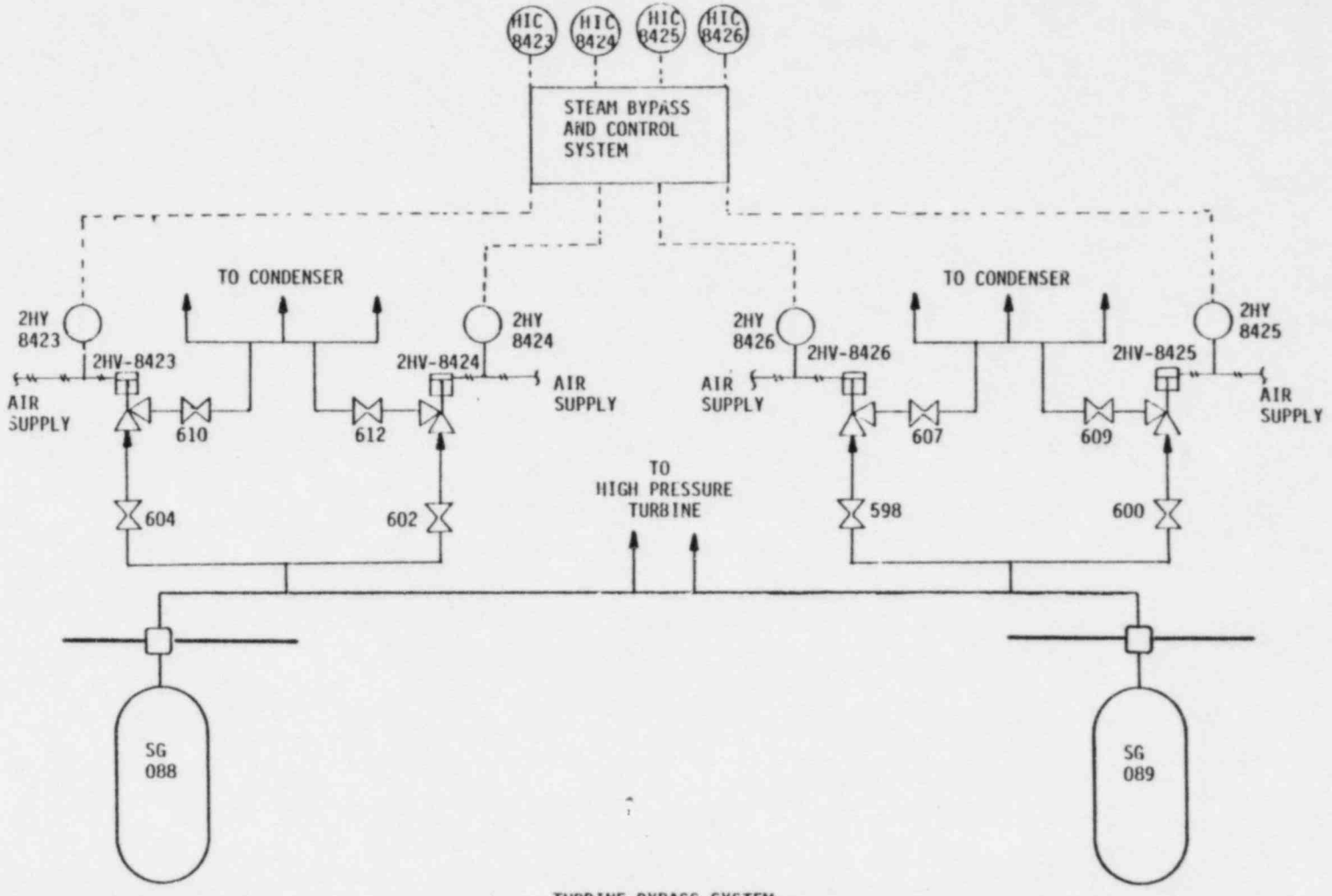
- Quick Open of TBVs following Turbine Trip
- Close all TBVs after Quick Open or during cooldown
- Maintain TBV flow prior to isolation of the affected (or most affected) SG
- Maintain TBV flow after isolation of the affected (or most affected SG

For the Spurious PORV LOCA event tree, a fault tree model was used to evaluate Failure to Open the TBVs (either automatically or manually during cooldown).

The probability of failing to trip the turbine was used in the SGTR event trees and is discussed in Section 6.4.

6.6.1 System Description

A schematic of the SONGS Turbine Bypass System is presented in Figure 6.6.1-1. The TBS takes steam from the main steam lines upstream of the turbine stop valves and discharges it directly to the main condenser. During normal operation, the TBVs are under control of the Steam Bypass and Control System (SBCS). The system is manually controlled when the power generated is less than 15%, or during hot-standby conditions. The operator observes main steam pressure and regulates the opening of the valves to keep main steam pressure under control. On high main steam pressure the SBCS opens the bypass valves to bypass steam to the condenser until main steam pressure is reduced. The opening of the TBVs is interlocked with the



TURBINE BYPASS SYSTEM

FIGURE 6.6.1-1

condenser vacuum to prevent the valves from opening when condenser vacuum is lost. In the event of a load rejection above 55%, the reactor trips and the TBS provides heat removal for the NSSS. If the TBS is not available, safe shutdown of the reactor is accomplished by manual operation of the atmospheric dump valves. The bypass valves fail closed on loss of instrument air.

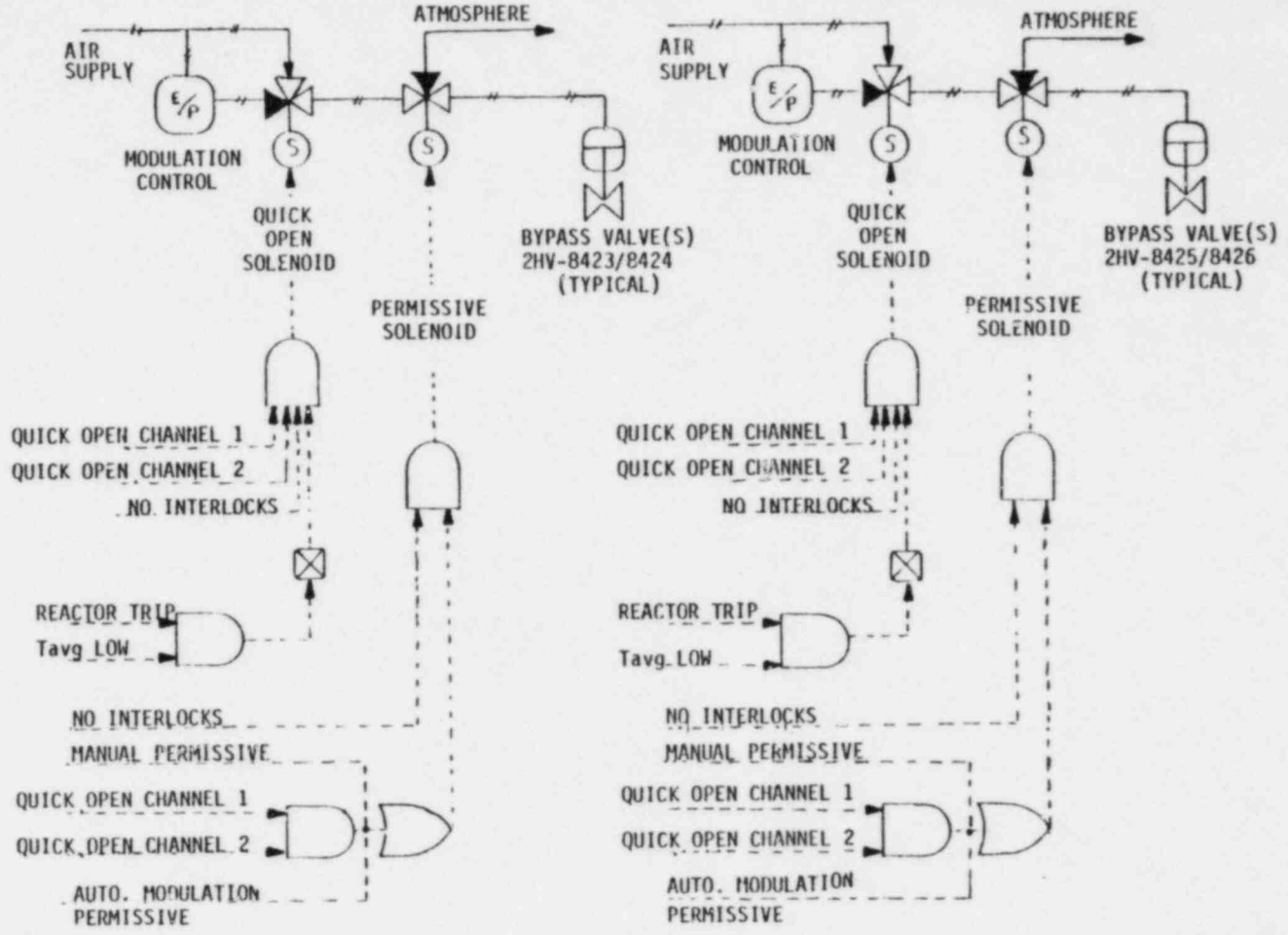
A simplified schematic of SBCS signals received by the bypass valves is presented in Figure 6.6.1-2. The SBCS continuously monitors changes in NSSS load. When a decrease in load is detected so large that it cannot be accommodated by the Modulation control of the valves because of their slow modulation speed, a "Valve Quick Opening" signal is generated which overrides the Modulation control and opens the valves in one second or less. To prevent a single component failure from opening more than one valve, the coincidence of two independently generated demand signals is made necessary for the quick opening of any one valve. For this, two parallel circuits (Channel 1 and Channel 2) are used to generate redundant "Quick Opening" signals. From these redundant signals a "Main Quick Opening Demand" and a "Permissive Quick Opening Demand" signal for each valve is derived and sent to the valves through independent channels. To carry the redundancy as far down as possible, as in the Modulation control case, the coincidence of these two signals is made to occur at the valves themselves.

The Turbine Bypass support system dependency diagram is provided in Figure 6.6.1-3.

6.6.2 Assumptions

The following assumptions were made in performing the fault tree analyses:

1. The Turbine Bypass System will be unavailable on Loss of Instrument Air, Loss of Condenser Vacuum or Loss of Offsite Power.

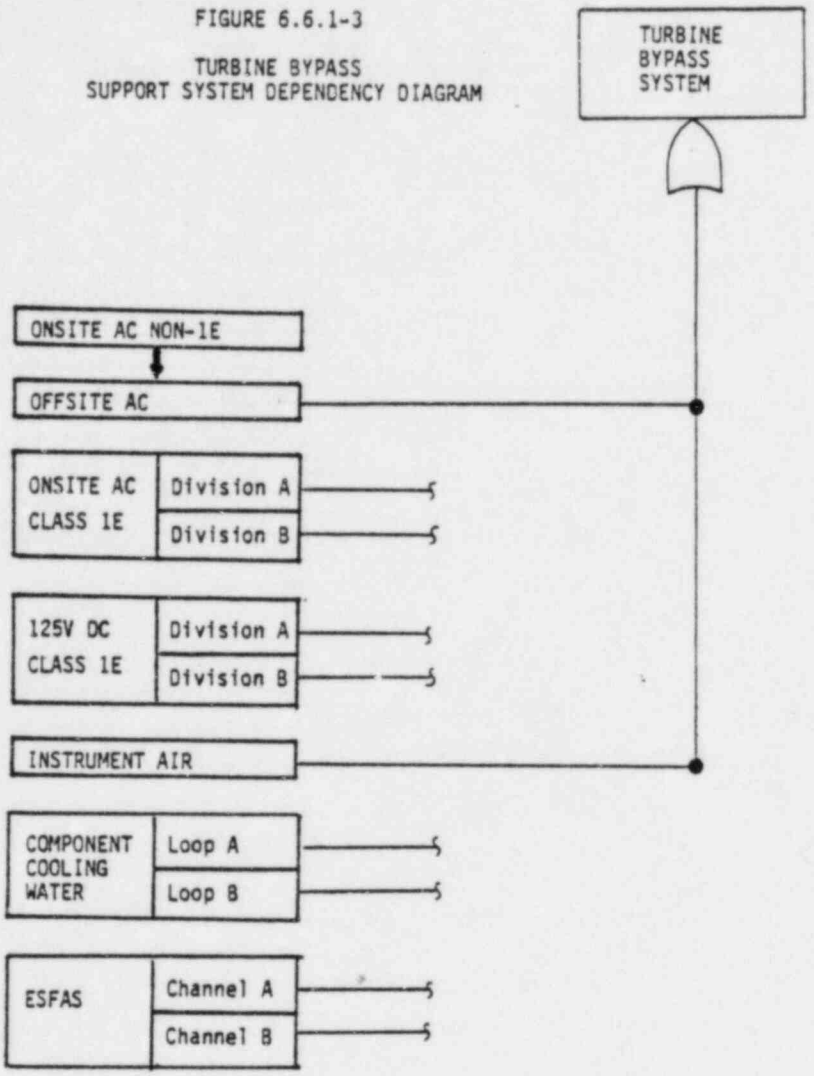


SIMPLIFIED SCHEMATIC OF SBCS SIGNALS

FIGURE 6.6.1-2

FIGURE 6.6.1-3

TURBINE BYPASS
SUPPORT SYSTEM DEPENDENCY DIAGRAM



2. Two redundant Quick Open Signals (Channel 1 and Channel 2) are required to open a bypass valve in the Quick Open mode of operation.

3. The SBCS receives power from 480V Motor Control Center 2BX.

4. For the case "Failure to Open the TBVs", the fault tree model includes both manual and automatic modes of system operation and refers to failing to open one of four TBVs.

5. For the case "1 of 4 TBVs Fails to Close After Quick Open or During Cooldown", the fault tree model includes both manual and automatic modes of system operation.

6. The fault tree "TBVs Fail to Quick Open" refers only to the Quick Open mode of operation. Given that instrument air and condenser vacuum are available at the time of the initiating event, the probability of losing the above before the TBV Quick Open Signal is generated is negligible. Therefore, instrument air and condenser vacuum are not modelled in the fault tree "TBVs Fail to Quick Open".

6.6.3 Results

For the SGTR event trees where offsite power is available at the time of the initiating event, fault tree logic diagrams were used to evaluate the following TBS failure modes:

- TBVs Fail to Quick Open (4 of 4 valves fail to quick open)
- 1 of 4 TBVs Fails to Reclose after Quick Open or During Cooldown
- Termination or Loss of TBV Flow prior to Isolation of the Affected SG
- Termination or loss of TBV Flow after Isolation of the Affected SG

The quantitative results of the analyses are presented as Cases One through Four respectively in Table 6.6.3-1. It should be noted that for SGTR with coincident LOOP, the TBS is not available.

For the Spurious PORV LOCA event tree, a fault tree model was used to determine the probability of failing to open the MBVs either automatically or manually during cooldown. The results are presented as Case Five in Table 6.6.3-1.

The confidence distributions of the above failure probabilities are presented in terms of the median values and associated error factors. The error factor is defined as the ratio of the 95 to 50 percentile.

Table 6.6.3-2 contains a list of the dominant cutsets for each case presented in Table 6.6.3-1. Included in the table is a brief description of each cutset as well as the percent contribution to the total failure probability. The percentage is based on a point estimate ratio.

TABLE 6.6.3-1

FAILURE PROBABILITIES FOR SONGS TURBINE BYPASS SYSTEM

Case Number	Description	Failure Probability (Median Value)	Error Factor
One	TBVs Fail to Quick Open - System Unavailability	7.8E-3	5
Two	1 of 4 TBVs Fails to Reclose after Quick Open or During Cooldown - System Unavailability	9.9E-3	5
Three	Loss of TBV Flow Prior to Isolation of the Affected (or Most Affected) SG - System Unavailability	1.1E-2	3
Four	Loss of TBV Flow After Isolation of the Affected (or Most Affected) SG - System Unavailability	5.2E-3	3
Five	Fail to Open TBVs - System Unavailability	6.0E-3	10

TABLE 6.6.3.2

DOMINANT CUTSETS FOR SONGS TURBINE BYPASS SYSTEM

Case Number	Cutset	Description	% of Total Failure Probability
One	1. ELBN0167	4.16 KV Bus 2A08 Fails on TT	60%
	2. EBFS0154	Bus 2A08 Breaker Fails	20%
Two	1. TVP00665	Operator Fails to Terminate TBV Flow During Cooldown	34%
	2. TVPB0685	TBV HV-8425 Fails to Close	12%
	3. TVPB0680	TBV HV-8426 Fails to Close	12%
	4. TVPB0673	TBV HV-8424 Fails to Close	12%
	5. TVPB0666	TBV HV-8423 Fails to Close	12%
Three	1. THS00690	Early SG Isolation	100%
Four	1. TSM00675	Operator Fails to Lower MSIS Setpoint	81%
	2. ZZZZ0025	Loss of Condenser Vacuum	9.0%
Five	1. ELBN0167	4.16 KV Bus 2A08 Fails on TT	47%
	2. EBGP0161	Grid Collapse Following TT	16%
	3. EBFS0154	Bus 2A08 Breaker Fails	16%

6.6.4 Turbine Trip

The probability of failing to trip the turbine was determined based on an earlier analysis performed for St. Lucie 2. The high pressure turbines for St. Lucie 2 and SONGS plants have four steam inlet paths. Each path contains a stop/emergency valve and a throttle valve, in series, which are controlled by individual E/H actuators. The dominant contributors to the failure to trip turbine are the mechanical malfunction of these valves and their actuators. Because of similarity between the valve arrangements and their actuators, the results of the St. Lucie 2 analysis are concluded to be applicable to this analysis.

The following assumptions are applicable to the SGTR event tree branch heading "Turbine Fails to Trip on Reactor Trip":

1. Failure to trip the turbine is defined as the inability to completely terminate steam flow to the high pressure turbine.

2. The stop, intercept, and throttle valves are initially fully open.

3. The reactor trip signal is generated.

4. An operator action from the control room is included as a backup in case the turbine fails to trip automatically.

5. The turbine valves are tested bi-monthly.

The median failure probability for "Turbine Fails to Trip on Reactor Trip" used in the event tree analysis is 7.1E-6 with an associated error factor of 11.

6.7 MAIN STEAM ISOLATION

6.7.1 System Description

A schematic of the SONGS Main Steam Isolation Valves (MSIVs) is presented in Figure 6.7.1-1. The MSIVs are held in the open position by a hydraulic system which exerts pressure on the bottom of a piston actuator. Nitrogen pressure on top of the piston actuator acts as the driving force for valve closure. Redundant actuation solenoids, powered from separate IE power sources, open nitrogen pressure operated dump valves which dump hydraulic oil from the bottom of the piston actuator through two separate dump lines.

Once an MSIS signal is generated, the MSIVs close and cannot be opened until plant conditions permit manual reset of the MSIS. These valves are located outside the containment downstream of the safety valves.

The MSIVs are designed such that they will provide positive shutoff of steam flowing from either direction within 5 seconds after receipt of a manual or automatic signal.

The Main Steam Isolation support system dependency diagram is provided in Figure 6.7.1-2.

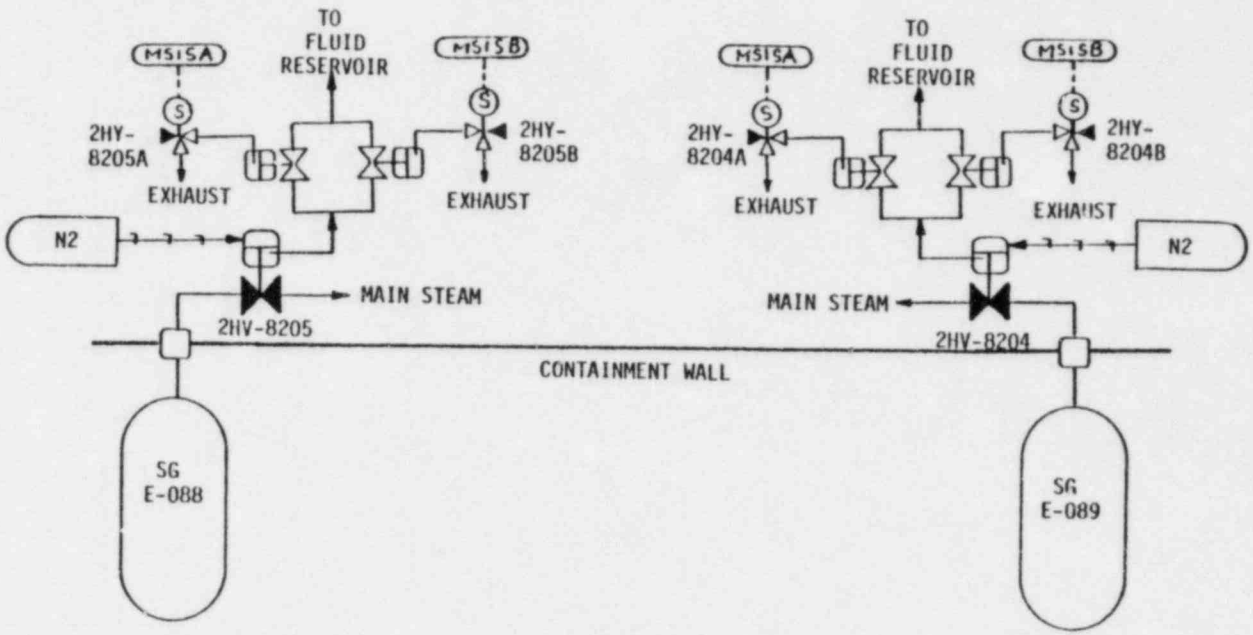
6.7.2 Assumptions

The following assumptions were made in performing the fault tree analyses:

1. Each MSIV receives both MSIS signals (MSISA and MSISB), however, only one signal is required for valve closure.

2. The MSIVs fail closed on loss of Class 1E 125V DC power.

3. The MSIVs fail closed on loss of nitrogen pressure to the pressure operated dump valves.

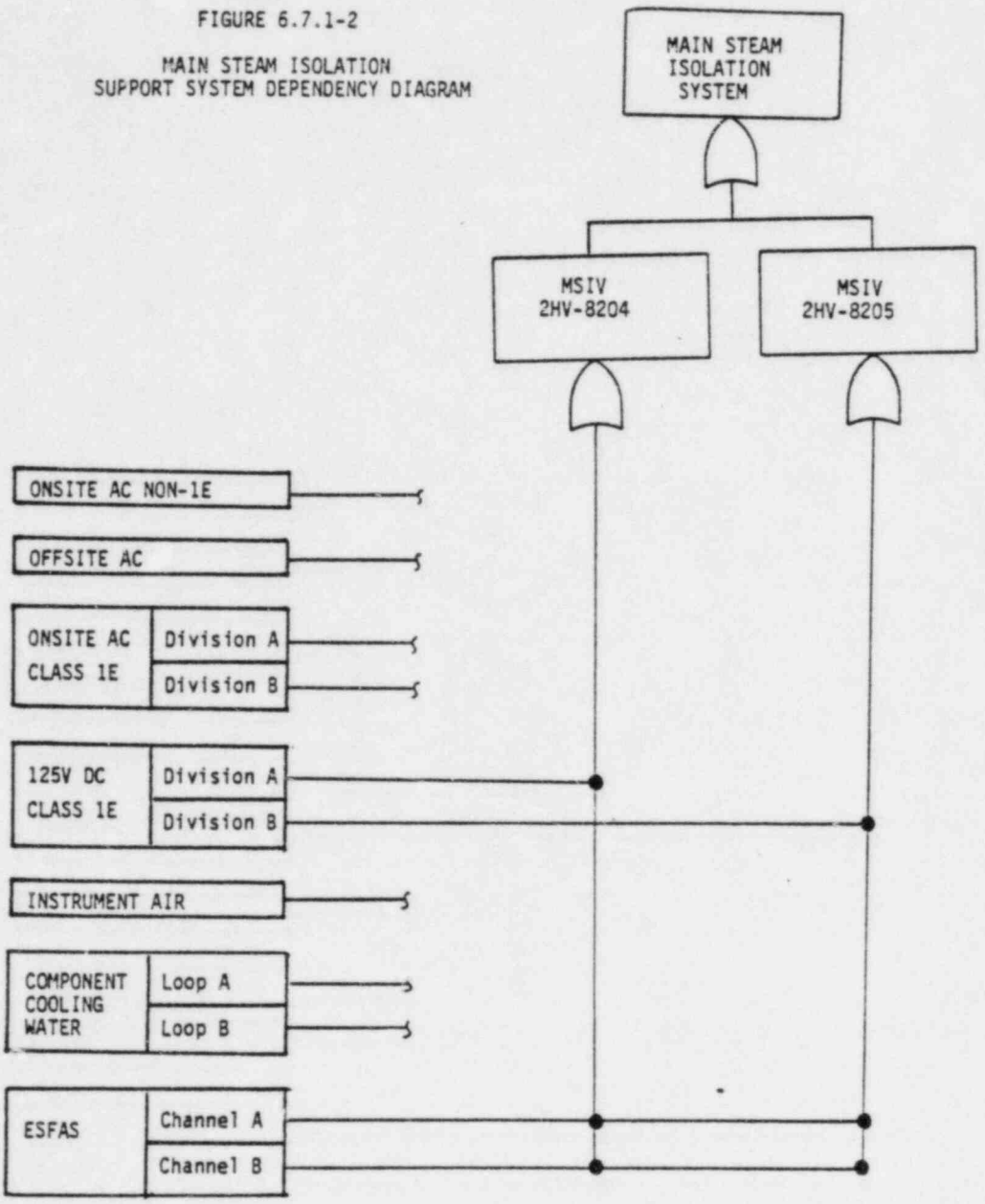


MAIN STEAM ISOLATION VALVES

FIGURE 6.7.1-1

FIGURE 6.7.1-2

MAIN STEAM ISOLATION
SUPPORT SYSTEM DEPENDENCY DIAGRAM



4. The MSIVs will fail to close on loss of nitrogen pressure to the top of the piston actuator.

5. The only operator action addressed in the model is a manual backup of the MSIS from the control room. Manual closure of an MSIV with a handwheel is not considered.

6.7.3 Results

Fault tree logic diagrams were used to evaluate the probability of failing to close MSIV HV-8204 and failing to close MSIV HV-8205. It should be noted that the unavailability of the MSIVs is not a function of the availability of offsite power.

The quantitative results of the analyses are presented as Cases One and Two in Table 6.7.3-1. The confidence distributions of the failure probabilities are presented in terms of the median values and associated error factors. The error factor is defined as the ratio of the 95 to 50 percentile.

Table 6.7.3-2 contains a list of the dominant cutsets for each case presented in Table 6.7.3-1. Included in the table is a brief description of each cutset as well as the percent contribution to the total failure probability. The percentage is based on a point estimate ratio.

TABLE 6.7.3-1

FAILURE PROBABILITIES FOR SONGS MSIVs

Case Number	Description	Failure Probability (Median Value)	Error Factor
One	HV-8204 Fails to Close - System Unavailability	9.0E-4	3
Two	HV-8205 Fails to Close - System Unavailability	9.0E-4	3

TABLE 6.7.3.2

DOMINANT CUTSETS FOR SONGS MSIVs

Case Number	Cutset	Description	% of Total Failure Probability
One	1. DVEB0522	MSIV HV-8204 Mechanical Malfunction	99%
	2. FSMR0525 FSMR0529 DSM00526	MSISA Not Generated and MSISB Not Generated and Operator fails to generate MSIS	.4%
Two	1. DVEB0531	MSIV HV-8205 Mechanical Malfunction	99%
	2. FSMR0525 FSMR0529 DSM00526	MSISA Not Generated and MSISB Not Generated and Operator fails to generate MSIS	.4%

6.8 ATMOSPHERIC DUMP SYSTEM

Various functional modes of the Atmospheric Dump System were evaluated for input to the systemic/action level event trees. For the SGTR event trees, fault tree logic diagrams were used to evaluate the following ADS functions:

- Open ADV HV-8419 on Steam Generator E-088
- Open ADV HV-8421 on Steam Generator E-089
- Terminate flow through ADV HV-8419 on Steam Generator E-088
- Terminate flow through ADV HV-8421 on Steam Generator E-089

For the spurious PORV LOCA event tree, a fault tree model was used to evaluate Failure to Open One of Two ADVs.

6.8.1 System Description

The SONGS Atmospheric Dump System is controlled manually by means of indicating controllers from the control room. A schematic of the ADS is presented in Figure 6.8.1-1.

The ADS consists of two Atmospheric Dump Valves (ADVs) and four solenoid operators. The actuator assembly is pneumatically operated via manual control signals from the control room.

In the "open" mode, the air solenoid valves align to supply air to the underside of the actuator piston and vent air from the upper side. Valve position is then controlled by the elecrtro-pneumatic controller which receives an electrical control signal from HIC-8419A1 or 8421A2 located on control room panel CR52. The HIC sends an electrical control signal to the electro-pneumatic controller which varies its air output signal to the steam dump actuator piston. The air pressure under the actuator piston opposes the spring tension above the piston. An increased air pressure under the piston allows the actuator piston to move upward, raising the plug, and increasing flow through the steam dump.

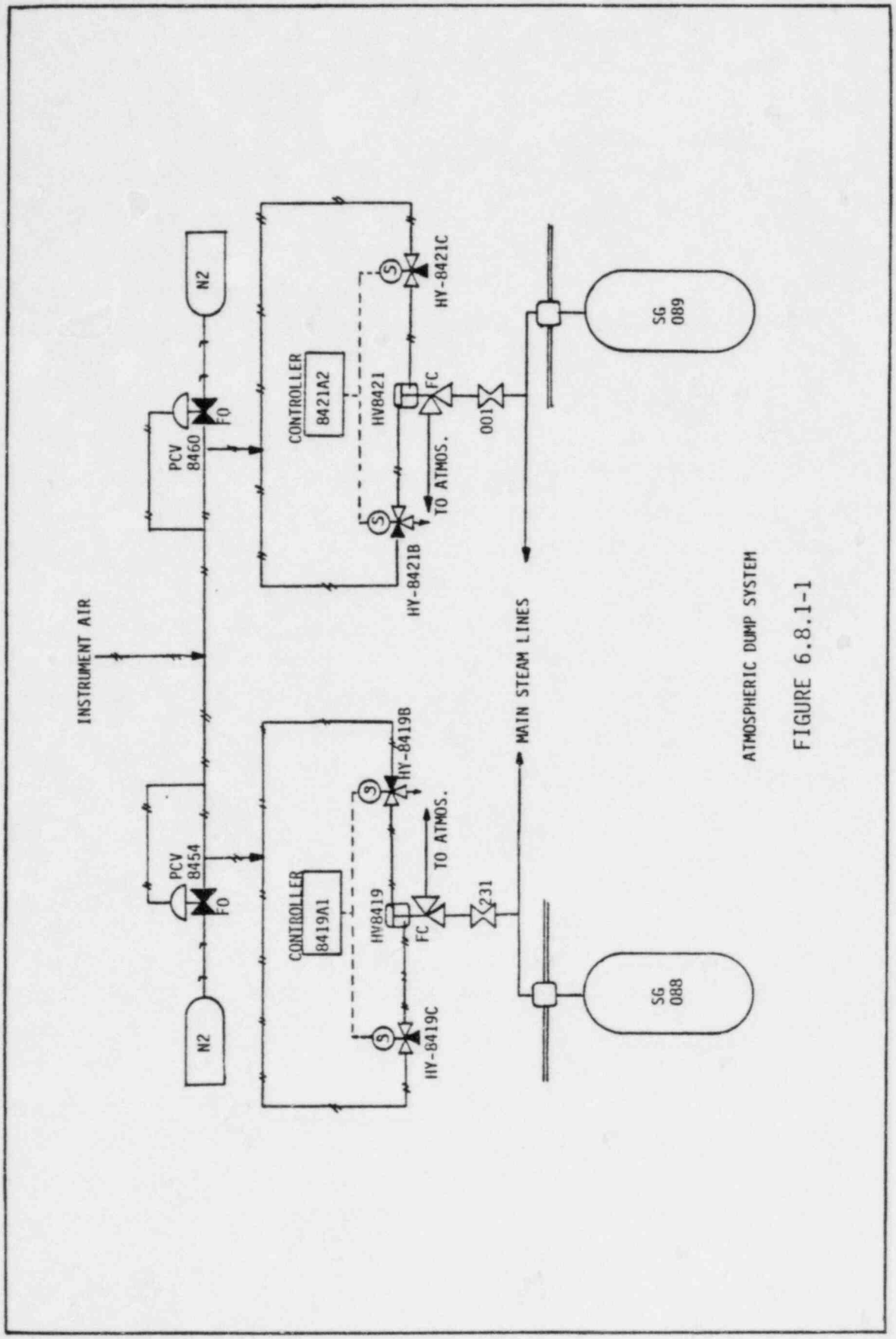

INSTRUMENT AIR
N2
PCV 8460
F0
CONTROLLER 8421A2
HV8421
FC
HY-8421C
HY-8421B
TO ATMOS.
001
SG 089
MAIN STEAM LINES
N2
PCV 8454
F0
CONTROLLER 8419A1
HV8419
FC
HY-8419B
HY-8419C
TO ATMOS.
231
SG 088
ATMOSPHERIC DUMP SYSTEM

FIGURE 6.8.1-1

In the "close" mode, the solenoid valves are positioned to vent the underside of the actuator piston and to supply air to the top side. The air pressure on top of the piston aids in shutting the steam dump and also ensures that the valve will be tightly seated.

The Class 1E 125VDC onsite power system provides power to control the ADVs. The steam dumps are designed to fail closed on a loss of electrical power. They will also close on a MSIS, but are provided with an override mode which will allow them to be reopened. Air supply to the steam dumps is provided by the turbine building instrument air header. Should instrument air be lost, a bottled nitrogen backup is supplied automatically. Both air and nitrogen headers are equipped with low pressure alarms. Cooldown can also be accomplished through manual operation of the atmospheric dump valves. Each valve has a handwheel that can be operated locally to override the actuator spring. In the event of a stuck open ADV, a manual valve upstream of each ADV can be closed to isolate steam flow.

The Atmospheric Dump support system dependency diagram is provided in Figure 6.8.1-2.

6.8.2 Assumptions

The following assumptions were made in performing the fault tree analyses:

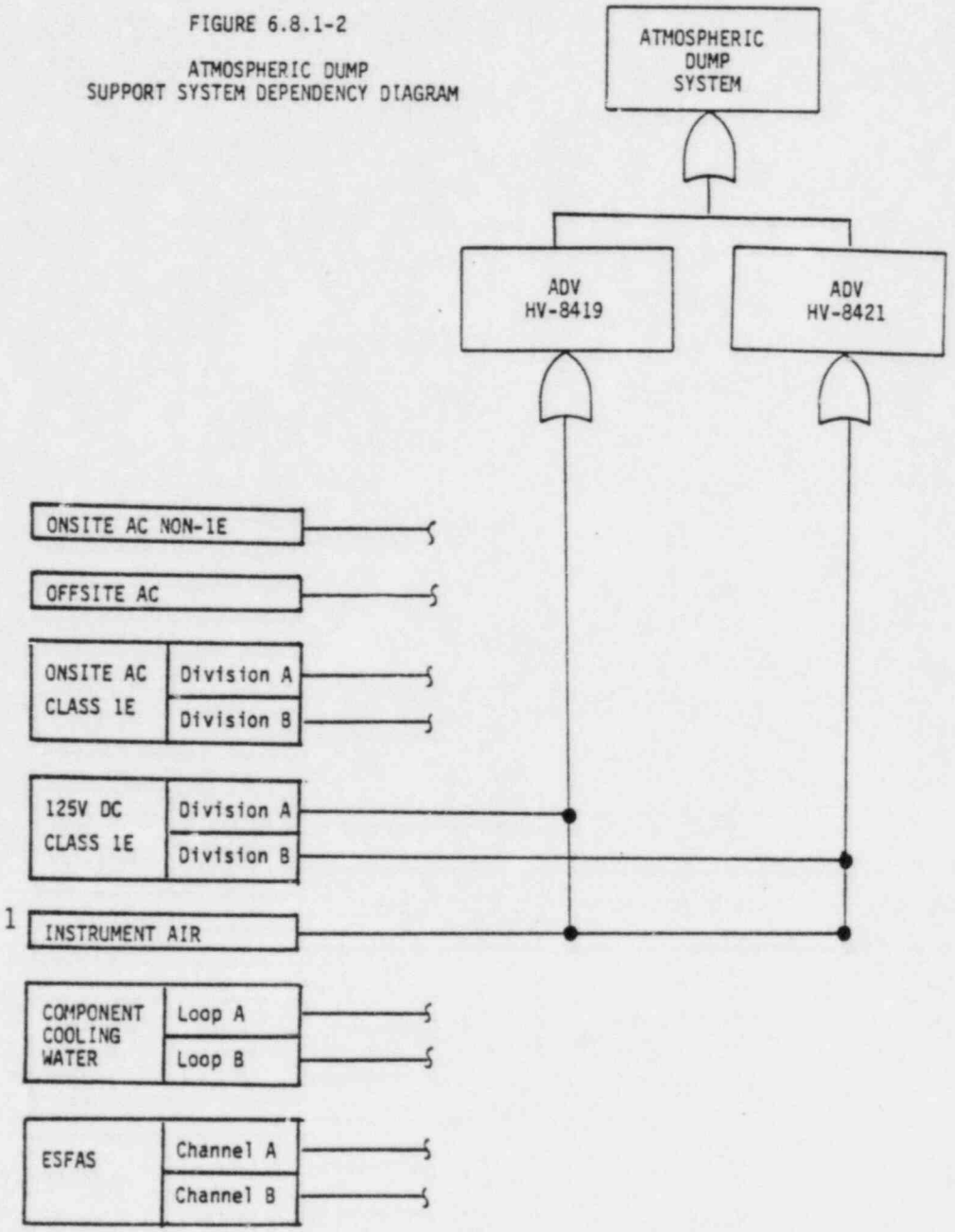
1. The manual isolation valves upstream of the ADVs can be manually opened or closed with a handwheel.

2. ADV HV-8419 and solenoid valves HV8419B and HV8419C are powered by 125V DC Bus 2D1. ADV HV-8421 and solenoid valves HB8421B and HV8421C are powered by 125VDC Bus 2D2.

3. Nitrogen bottle isolation valves PCV-8454 and PCV-8460 fail open on loss of instrument air.

FIGURE 6.8.1-2

ATMOSPHERIC DUMP
SUPPORT SYSTEM DEPENDENCY DIAGRAM



[1]For this system, Istrument Air supply includes a nitrogen backup.

4. The ADVs fail closed on loss of power or loss of instrument air and the nitrogen back-up.

5. Solenoid operators HV-8419C and HV-8421C fail open on loss of power, thereby preventing air or nitrogen pressure from opening the ADVs.

6. The spring tension above the ADV piston is sufficient to close the ADV if opening pressure is absent from the bottom of the piston.

6.8.3 Results

For the SGTR event trees where offsite power is available at the time of the initiating event, fault tree logic diagrams were used to evaluate the following ADS failure modes:

- Failure to open ADV HV-8419 on SG-088
- Failure to open ADV HV-8421 on SG-089
- Failure to terminate flow through ADV HV-8419 on SG-088
- Failure to terminate flow through ADV HV-8421 on SG-089

For the SGTR event trees where offsite power is unavailable at the time of the initiating event, the first two failure modes were re-evaluated.

For the Spurious PORV LOCA event tree, a fault tree model was used to determine the probability of failing to open one of two ADVs.

The quantitative results of the analyses are presented as Cases One through Five respectively in Table 6.8.3-1. The confidence distributions of the failure probabilities are presented in terms of the median values and associated error factors. The error factor is defined as the ratio of the 95 to 50 percentile.

Table 6.8.3-2 contains a list of the dominant cutsets for each case presented in Table 6.8.3-1. Included in the table is a brief description of each cutset as well as the percent contribution to the total failure probability. The percentage is based on a point estimate ratio.

TABLE 6.8.3-1

FAILURE PROBABILITIES FOR SONGS ATMOSPHERIC DUMP SYSTEM

Case Number	Description	Failure Probability (Median Value)	Error Factor
One	Failure to open ADV HV-8419 on SG-088 - System Unavailability given offsite power is available	2.3E-2	3
Two	Failure to open ADV HV-8421 on SG-089 - System Unavailability given offsite power is available	2.3E-2	3
Three	Failure to open ADV HV-8419 on SG-088 - System Unavailability given offsite power is unavailable	2.5E-2	3
Four	Failure to open ADV HV-8421 on SG-089 - System Unavailability given offsite power is unavailable	2.5E-2	3
Five	Failure to terminate flow through ADV HV-8419 on SG-088 - System Unavailability	8.7E-5	16
Six	Failure to terminate flow through ADV HV-8421 on SG-089 - System Unavailability	8.7E-5	16
Seven	Failure to open one of two ADVs - System Unavailabilty	1.6E-2	4

TABLE 6.8.3.2

DOMINANT CUTSETS FOR SONGS ATMOSPHERIC DUMP SYSTEM

Case Number	Cutset	Description	% of Total Failure Probability
One	1. D1X00547	Operator fails to generate open signal	77%
	2. DVNX0541	Manual valve 231-C-129 not open	5.7%
Two	1. D1X00556	Operator fails to generate open signal	77%
	2. DVNX0550	Manual valve 001-C-129 not open	5.7%
Three	1. D1X00547	Operator fails to generate open signal	73%
	2. DVNX0541	Manual valve 231-C-129 not open	5.4%
Four	1. D1X00556	Operator fails to generate open signal	73%
	2. DVNX0550	Manual valve 001-C-129 not open	5.4%
Five	1. DVPB0560	ADV HV-8419 Mechanical Malfunction (FTC)	49%
	DVNX0559	Manual valve 231-C-129 not closed	
	2. DIX00564	Operator fails to generate close signal	49%
	DVNX0559	Manual valve 231-C-129 not closed	
Six	1. DVPB0566	ADV-8421 Mechanical Malfunction (FTC)	49%
	DVNX0565	Manual valve 001-C-129 not closed	
	2. DIX00570	Operator fails to generate close signal	
	DVNX0565	Manual valve 001-C-129 not closed	49%
Seven	1. D1X00547	Operator fails to generate open signal	> 99%

6.9 MAIN STEAM SAFETY VALVES

The MSSVs are included in various manners as branches in the systemic/action level event trees. For the Loss of Heat Sink event trees, the probability of failing to provide sufficient heat removal with the MSSVs is included in the branch titled "Failure to Remove Secondary Steam". Following a reactor/turbine trip, RCS heat is removed from the steam generators by operation of the TBVs, ADVs or MSSVs respectively. Cooldown can be initiated using one SG. Failure of the TBVs and ADVs to remove secondary steam results in a demand for the MSSVs to open. The probability of failing to remove secondary steam is conservatively defined as the probability of failing to remove secondary steam with the MSSVs.

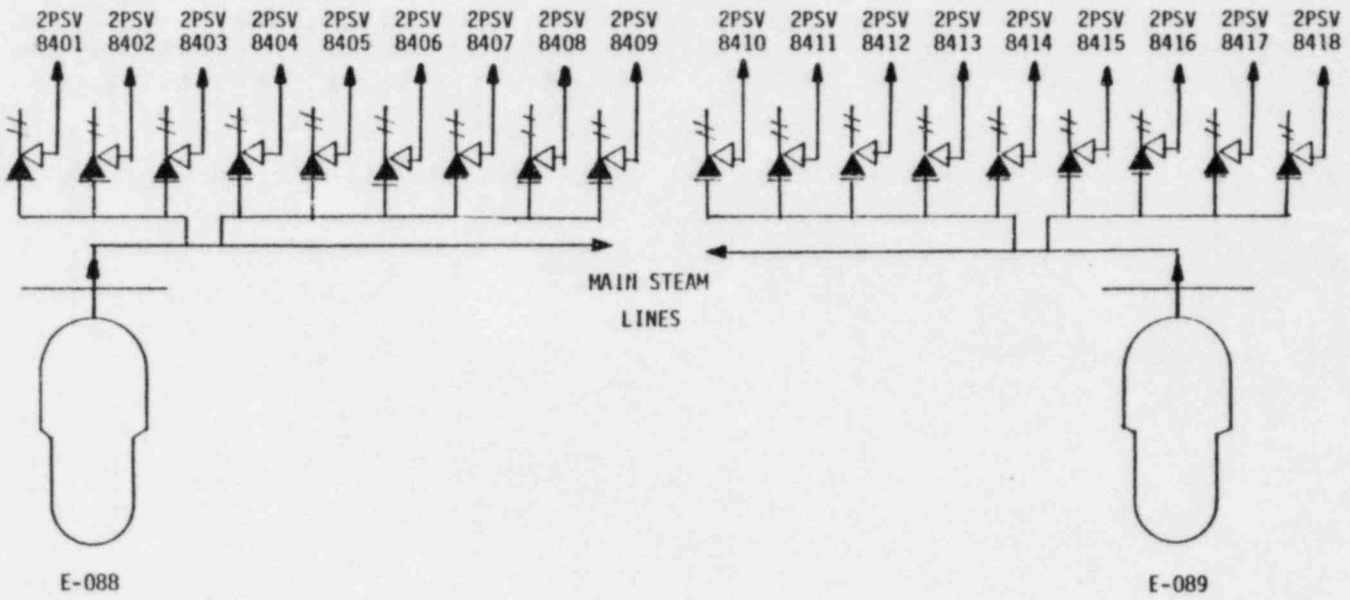
The MSSVs are modelled in the Spurious PORV LOCA event tree as the branch "Failure to Open MSSVs".

For the SGTR event trees, fault tree logic diagrams were used to evaluate the probability of failing to reclose one MSSV given:

- one MSSV opens on the affected (or most or least affected) SG
- five MSSVs open on the affected (or most or least affected) SG

6.9.1 System Description

A schematic of the SONGS MSSVs is presented in Figure 6.9.1-1. The spring-loaded MSSVs provide over pressure protection for the secondary side of the steam generator and the main steam piping. There are nine spring-loaded safety valves installed in each of the two 40-inch main steam lines. The total relieving capacity of the safety valves is 7.55×10^6 lb./hr. per steam generator. The valve setpoints are as follows:



MAIN STEAM SAFETY VALVES

FIGURE 6.9.1-1

SG-088	SG-089	Lift Setting
2PSV-8401	2PSV-8410	1100 psia
2PSV-8402	2PSV-8411	1107 psia
2PSV-8403	2PSV-8412	1114 psia
2PSV-8404	2PSV-8413	1121 psia
2PSV-8405	2PSV-8414	1128 psia
2PSV-8406	2PSV-8415	1135 psia
2PSV-8407	2PSV-8416	1142 psia
2PSV-8408	2PSV-8417	1149 psia
2PSV-8409	2PSV-8418	1155 psia

Successful operation of a MSSV requires the valve to open at the proper pressure setpoint and to reclose upon decreased pressure.

6.9.2 Assumptions

For the Loss of Secondary Heat Sink event trees and the spurious PORV LOCA event tree the following assumptions were made in performing the reliability analyses:

1. Failure to Remove Secondary Steam and Failure to Open MSSVs are defined as the failure to open one of nine MSSVs.

2. The nine main steam safety valves on one main steam line are independent of the main steam safety valves on the other main steam line.

3. Failure of a MSSV is defined as failure to open when the pressure in the associated steam generator equals or exceeds the setpoint pressure of the valve.

For the SGTR event trees, the following assumptions were made in performing the fault tree analyses:

1. One MSSV Fails to Reclose is defined as one MSSV failing to terminate steam flow after secondary pressure has decreased below the valve lift setting.

2. If the TBS is unavailable following turbine trip, five MSSVs per SG will open.

6.9.3 Results

For the Loss of Secondary Heat Sink event trees and Spurious PORV LOCA event tree, the probability of failing to open 1 of 9 MSSVs was determined to be 1.0E-9. Therefore, a probability of 1.0E-9 with an associated error factor of 10 was assumed.

For the SGTR event trees, fault tree logic diagrams were used to evaluate the following failure probabilities:

- One MSSV on the affected or most affected SG fails to reclose (MSSV 2PSV-8401 on SG-088)

- One MSSV on the unaffected or least affected SG fails to reclose (MSSV 2PSV-8410 on SG-089)

- One MSSV on the affected or most affected SG fails to reclose given the TBS is unavailable following turbine trip. (Four valves on SG-088 are assumed to open).

- One MSSV on the unaffected or least affected SG fails to reclose given the TBS is unavailable following turbine trip. (Five valves on SG-089 are assumed to open).

The quantitative results of the analyses are presented as Cases One through Six respectively in Table 6.9.3-1. The confidence distributions of the failure probabilities are presented in terms of the median values and associated error factors. The error factor is defined as the ratio of the 95 to 50 percentile.

TABLE 6.9.3-1

FAILURE PROBABILITIES FOR SONGS MSSVs

Case Number	Description	Failure Probability (Median Value)	Error Factor
One	Failure to Remove Secondary Steam - System Unavailability	1.0E-9	10
Two	Fail to Open MSSVs - System Unavailability	1.0E-9	10
Three	One MSSV on SG-088 fails to reclose - System Unavailability	1.0E-2	3
Four	One MSSV on SG-089 fails to reclose - System Unavailability	1.0E-2	3
Five	One MSSV on SG-088 fails to reclose given TBS is unavailable following turbine trip - System Unavailability	5.1E-2	3
Six	One MSSV on SG-089 fails to reclose given TBS is unavailable turbine trip - System Unavailability	5.1E-2	3

6.10 MAIN FEEDWATER SYSTEM

For the loss of Secondary Heat Sink event trees, an analysis was performed to determine the frequency of loss of main feedwater events. The analysis includes a review of initiating events which result in a reactor/plant trip condition and a fault tree analysis to determine the probability of loss of the post-trip 5% bypass MFW flow.

The frequency of Loss of Main Feedwater Events is defined as the frequency of automatic plant/reactor trip events and the probability of loss of post-trip 5% Bypass Main Feedwater Flow. Included in this definition are plant trips that are a result of perturbations in the main feedwater system or its support systems as well as malfunctions in other plant systems. The resulting frequency represents the frequency of total loss of Main Feedwater events.

System perturbations or malfunctions that result in reactor/plant trip events were determined based on Reference (15) and operating experience. Reference (15) provides a list of PWR initiating events, their frequency of occurrence and the associated error factors. These initiating events were divided into three categories based on their subsequent impact on main feedwater system operation (Table 6.10-1).

Initiating events which have a direct impact on the probability of the main feedwater system providing 5% bypass flow comprise Category 1 initiating events. This includes failures within the main feedwater system, electrical power distribution system, condenser and circulating water system.

To account for the SONGS-specific feedwater system design, the main feedwater system and electrical power distribution have been modeled at the component level in the fault tree logic diagram. Therefore, system/component failures which result in a trip condition and impact the operation of 5% bypass flow are treated directly in the fault tree logic diagram.

TABLE 6.10-1

LOSS OF MAIN FEEDWATER

PLANT TRIP EVENTS

Category 1:

Loss or reduction of feedwater flow (1 loop)
Total loss of feedwater flow (all loops)
Loss of condensate pump (1 loop)
Loss of condensate pumps (all loops)
Loss of condenser vacuum
Condenser leakage
Loss of power to necessary plant systems
Increase in feedwater flow (1 loop)
Increase in feedwater flow (all loops)
Feedwater flow instability, misc. mechanical causes
Loss of circulating water
Loss of offsite power

Category 2:

Generator trip or generator caused faults
Loss of 125 vdc Class 1E Bus
Full or partial closure of MSIV (1 loop)
Closure of all MSIV
Sudden opening of steam relief valves
Loss of component cooling
Loss of service water system
Turbine trip, throttle valve closure, EHC problems
Loss of RCS flow
Total loss of RCS flow

Category 3:

Spurious trip, cause unknown
Auto trip, no transient condition
Pressurizer spray failure
CEDM problems/rod drop
Leakage from control rods
Low pressurizer pressure
High pressurizer pressure
Inadvertent safety injection signal
Containment pressure problems
Pressure/temperature/power imbalance - rod position error
Pressurizer leakage
Misc. leakage in secondary system

Category 2 initiating events include those events which have a potential interaction with systems modeled in the Loss of Secondary Heat Sink event trees. This category of events includes failures of secondary or primary systems that influence the establishment of a secondary heat sink. Category 2 events are modeled as separate events in the fault tree logic diagram.

The initiating events in Category 3 are those events which do not have a direct impact on the main feedwater system or the Loss of Secondary Heat Sink event trees. These events do, however, result in a reactor trip and require a secondary heat sink to prevent core damage. Category 3 events have been combined and are represented in the fault tree logic diagram as "Additional Trip Events."

Several initiating events are outside the scope of the main feedwater analysis and are not addressed here (Table 6.10-2). Steam Generator Tube Rupture is addressed in a separate analysis. The plant is assumed to be operating in the automatic mode at the time of the initiating event. Therefore, manual trips and operator error feedwater instability are not addressed.

TABLE 6.10-2

PLANT TRIP EVENTS EXCLUDED FROM LOSS OF MAIN FEEDWATER ANALYSIS

Loss of coolant accidents
Uncontrolled rod withdrawal
Leakage in primary system
CVCS malfunction - boron dilution
Startup of inactive coolant pump
Feedwater flow instability - operator error
Steam generator leakage
Manual trip - no transient condition

For the Spurious PORV LOCA event tree, a fault tree logic diagram was used to evaluate the probability of failing to deliver 5% MFW flow to both steam generators. For the PORV LOCA with Coincident SGTR event tree, a fault tree model was used to determine the probability of failing to deliver 5% MFW flow to the unaffected steam generator.

6.10.1 System Description

A schematic of the SONGS Main Feedwater System is presented in Figure 6.10.1-1. The condensate and feedwater system consists of condensate pumps, low pressure feedwater heaters, heater drain tanks and pumps, feedwater pumps and drive turbines, and high pressure feedwater heaters. Four one-third capacity, condensate pumps are provided each taking suction from a separate condenser hotwell. The condensate pumps discharge into a common line that conducts the feedwater to the low-pressure feedwater train. The system is designed to permit continued full-load operation of the plant with one condensate pump or one heater drain pump unavailable.

From the low-pressure heaters the feedwater is pumped, by two half-capacity turbine-driven main feedwater pumps, to the high pressure feedwater heaters. The main feedwater pumps are single-stage, horizontal, centrifugal pumps capable of variable speed and parallel operation. The feedwater pump speed is controlled by the three-element control system that regulates the feedwater flow to each steam generator.

The feedwater pumps discharge through two parallel heaters into a common line. From the common line, the feedwater flow again divides into two parallel lines, each feeding a single steam generator. The feedwater control valves and containment isolation valves are located outside the containment. In order to facilitate balance flow between the two trains, crossties are provided at the discharge of the condensate pumps, heater drain pumps and the feedwater pumps.

The Main Feedwater support system dependency diagram is provided in Figure 6.10.1-2.

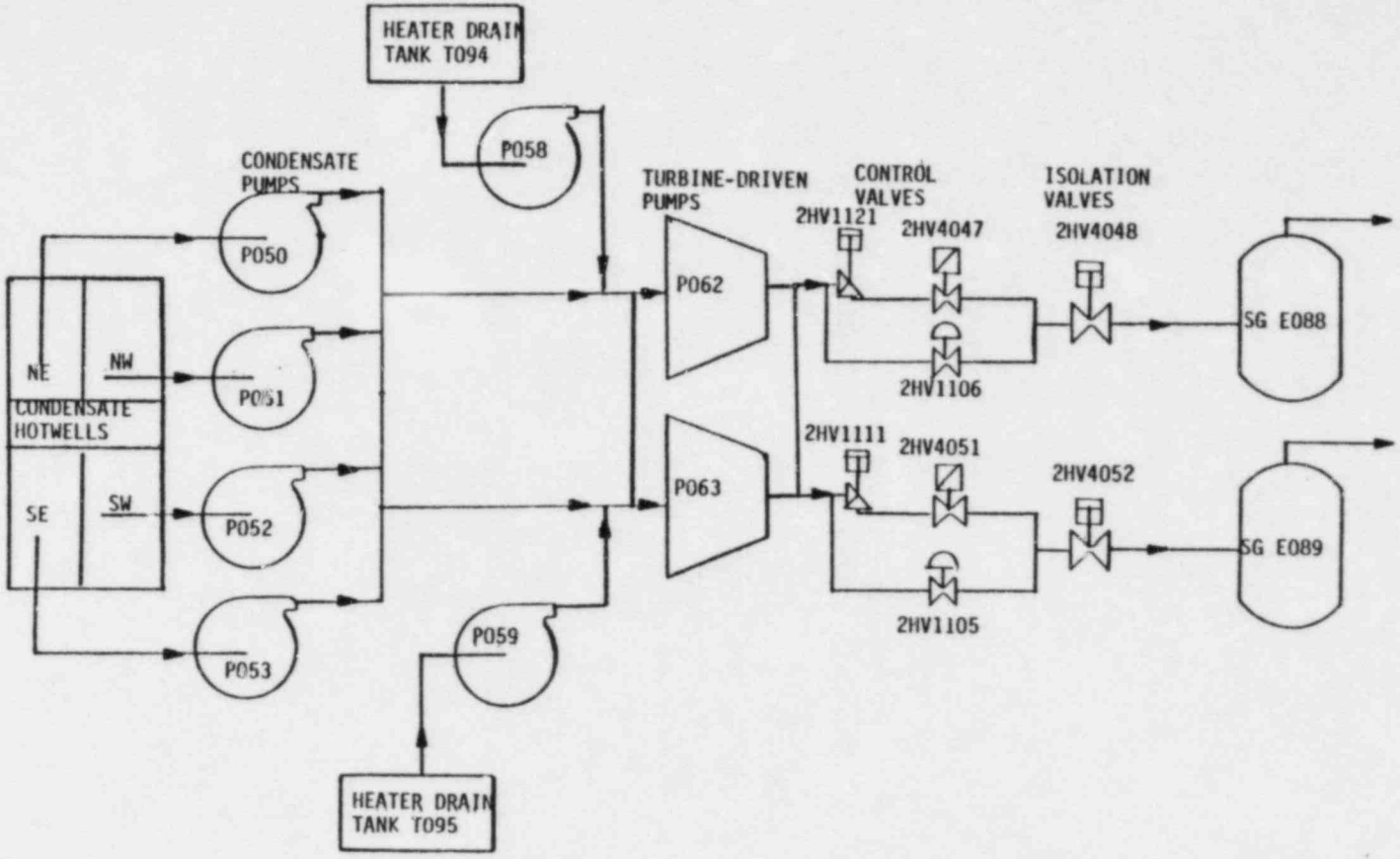
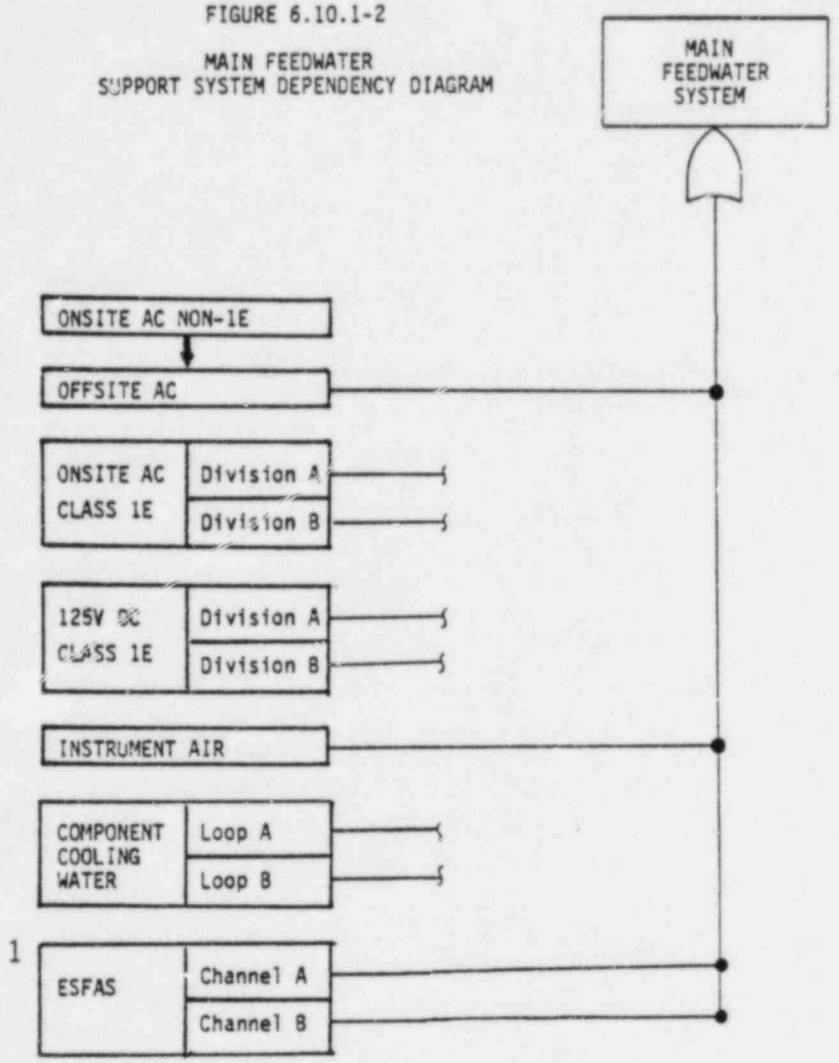


FIGURE 6.10.1-1

MAIN FEEDWATER SYSTEM

FIGURE 6.10.1-2

MAIN FEEDWATER
SUPPORT SYSTEM DEPENDENCY DIAGRAM



[1]The MFIVs are assumed to close on spurious MSIS or CIAS

6.10.2 Assumptions

The following assumptions were made in performing the frequency evaluation for the Loss of Secondary Heat Sink event trees and the fault tree analysis for the PORV LOCA event trees:

1. For the Loss of Secondary Heat Sink event trees, Loss of Main Feedwater is defined as the occurrence of an automatic plant/reactor trip event and the loss of post-trip 5% bypass main feedwater flow to both steam generators.

2. For the Spurious PORV LOCA event tree, Failure to Deliver 5% MFW is defined as failing to deliver 5% MFW flow to at least one steam generator.

3. For the PORV LOCA with Coincident SGTR event tree, Failure to Deliver 5% MFW to One SG is defined as failing to deliver 5% MFW flow to the unaffected SG.

4. The minimum equipment required to maintain main feedwater operating flow for 50 - 100% power operation includes:

   2 Main Feedwater Pumps
   3 Condensate Pumps
   2 Heater Drain Pumps
   4 Circulating Water Pumps
   Condenser

5. The minimum equipment required to provide 5% bypass MFW flow to 1 SG includes:

   1 Main Feedwater Pump
   1 Condensate Pump
   1 Bypass Control Valve
   1 Condensate Hotwell
   Condensate Water Storage Tank T120

6. The Feedwater System and support systems are in the normal, automatic mode of operation at the time of the initiating event.

7. The plant is operating at 50 - 100% power at the time of the initiating event.

8. One condensate pump (P050) is unavailable due to maintenance.

9. No operator action to restore main feedwater system is taken.

10. Condensate Storage Tank T120 contains an adequate supply of condensate to maintain 5% bypass flow for length of event.

11. Main Feedwater Pumps trip on

    High pump discharge pressure
    Low pump suction pressure
    Low pump lube oil pressure
    Pump turbine driver overspeed
    Turbine driver exhaust low vacuum
    Turbine thrust bearing wear excessive
    Low bearing lube oil pressure.

12. Class Non-1E DC Power is available before and after reactor-turbine trip.

13. Condensate pumps will trip on low hotwell level.

14. Failure of the low pressure and high pressure feedwater heaters does not prevent delivery of feedwater flow.

6.10.3 Results

For the Loss of Secondary Heat Sink event trees, a fault tree logic diagram was used to determine the frequency of Loss of Main Feedwater.

For the PORV LOCA event trees, fault tree logic diagrams were used to evaluate the probability of failing to deliver 5% MFW flow to a single SG and to one of two steam generators.

The quantitative results of the analyses are presented as Cases One through Three respectively in Table 6.10.3-1. The confidence distributions of the initiating event frequency and failure probabiities are presented in terms of the median values and associated error factors. The error factor is defined as the ratio of the 95 to 50 percentile.

Table 6.10.3-2 contains a list of the dominant cutsets for each case presented in Table 6.10.3-1. Included in the table is a brief description of each cutset as well as the percent contribution to the total frequency or failure probability. The percentage is based on a point estimate ratio.

TABLE 6.10.3-1

INITIATING EVENT FREQUENCY AND FAILURE PROBABILITIES FOR
SONGS MAIN FEEDWATER SYSTEM

Case Number	Description	Median Value	Error Factor
One	Loss of Main Feedwater Initiating Event Frequency	1.23 per year	3
Two	Fail to deliver 5% MFW to the unaffected SG given PORV LOCA following SGTR - System Unavailability	2.1E-2	5
Three	Fail to deliver 5% MFW to at least one of two SGs given spurious PORV LOCA - System Unavailability	1.4E-2	5

TABLE 6.10.3-2

DOMINANT CUTSETS FOR SONGS MAIN FEEDWATER SYSTEM

Case Number	Cutset	Description	% of Total Frequency/ Probability
One	1. MPMC0309	Condensate pump P053 fails to operate	13%
	2. MPMC0308	Condensate pump P052 fails to operate	13%
	3. MPMC0307	Condensate pump P051 fails to operate	13%
	4. MPMC0305	Heater drain pump P058 fails to operate	13%
	5. MPMC0306	Heater drain pump P059 fails to operate	13%
Two	1. EBGP0161	Grid collapse following turbine trip	65%
	2. IXXP0316	Loss of Instrument Air	8.7%
Three	1. EBGP0161	Grid collapse following turbine trip	70%
	2. IXXP0316	Loss of Instrument Air	9.3%

6.11 AUXILIARY FEEDWATER SYSTEM

Various functional modes of the Auxiliary Feedwater System were evaluated for input to the system/action level event trees. For the Loss of Secondary Heat Sink and PORV LOCA event trees, a fault tree logic diagram was used to determine the following failure probabilities:

- Failure to deliver AFW to at least one SG
- Failure to deliver AFW to at least one SG given loss of MFW as the initiating event
- Failure to deliver AFW to at least one SG given a spurious PORV LOCA as the initiating event and conditional on loss of 5% MFW flow to both SGs
- Failure to deliver AFW to the unaffected SG given a PORV LOCA with coincident SGTR as the initiating event and conditional on loss of 5% MFW flow to the unaffected SG.

For the SGTR event trees, fault tree logic diagrams were used to determine the following probabilities:

- Excess AFW flow to the affected or most affected SG
- Excess AFW or MFW flow to the least affected SG given offsite power is available at the time of the initiating event
- Excess AFW flow to the least affected SG given offsite power is unavailable at the time of the initiating event

The fault tree logic diagram for Failure to Deliver AFW models the AFW System from the condensate water sources to the steam generators including pumps, valves, the electrical power distribution system, the turbine driver and control systems. Not modeled are drain lines, drain valves, piping, miniflow lines, and connection lines which are small in size. Failure of these components has little impact on the total system failure probability.

The fault tree logic diagram incorporates the contribution to system failure from random system failures, test and maintenance, human error and common cause failures. Random system failures reflect the system malfunctions that occur as a result of random component failures. The contribution to system failure from test and maintenance is addressed by considering the associated system unavailability. The plant technical specifications limit the amount of time an auxiliary feedwater pump or associated train may be out of service to 72 hours while at power operations. All system components were reviewed for possible contribution to maintenance unavailability.

AFWS control or isolation valves which require full AFWS shutdown in order for repair also require plant shutdown (per technical specifications). These valves do not contribute to the maintenance unavailability of the AFWS.

Pump maintenance consists of a range of actions from major disassembly to packing adjustment. For the AFW pumps, most maintenance performed requires isolation of the pump from the system and, therefore, contributes to the maintenance unavailability of the pump train.

Because of the lack of operating history for SONGS, the maintenance unavailability of the different pump trains was determined based on generic values from WASH-1400 (16). From WASH-1400, the expected frequency of pump maintenance is one act every 4.5 months. This maintenance is assumed to include the pump, the driver (turbine or motor), and associated

control circuits. The maintenance duration is limited to 72 hours by technical specifications. The lognormal mean maintenance duration is 19 hours. Based upon these assumptions, maintenance unavailability contributions for the AFW pump trains was determined.

Testing of the AFWS consists primarily of surveillance testing to satisfy the plant technical specifications and ASME requirements. Monthly testing is performed on each AFW pump. For each test, pump discharge control valves are closed and the pump is manually started. Successful completion of the test requires that the AFW pump develop a minimum flow and differential pressure on recirculation flow line. The pump tests are performed sequentially. During the test, if the AFWS is required to operate, the operator may align the train to provide AFW flow.

The Auxiliary Feedwater control and isolation valves are tested quarterly with a 92-day test interval. The test involves the operator depressing each valve switch individually and observing the valve position indicator. The valve is then closed by the operator in the same manner. Testing of the control or isolation valves does not contribute to AFWS unavailability since the valve is capable of responding to an EFAS or providing AFW flow to the SG.

Monthly testing is also assumed to be performed separately on the EFAS and AFRS. (The AFRS is expected to be installed at the first refueling outage. System operation was included in the analysis). For each system, the actuation or control logic matrix and circuitry are tested. Assuming that, for the EFAS and AFRS respectively, the test places one train of the two train system unavailable and the test lasts for one hour, the unavailability contribution of testing was calculated.

Human interaction with the AFWS that results in system unavailability has also been considered. Human error resulting in the misalignment of the AFWS pumps manual valves (suction and discharge) is included directly in the fault tree analysis. The AFWS manual valves are locked open valves.

The AFWS is subjected to a monthly walk-through inspection. Per SONG's procedures (11), the operator uses a checklist and is backed up by a checker. It should be noted that the monthly flow test on the AFWS pumps provides indication of the suction manual valves position.

Operator action to restore AFWS as a response to system failure on demand is not included. Restoration of auxiliary feedwater is addressed in a separate task analysis. The restoration analysis is presented in Section 6.17.

The method used to perform the common cause failure analysis is based on the system logic model. The fault tree logic diagram was used to determine the failure characteristics of the system. A search was then performed to identify potential common failure causes for the dominant failure characteristics of the system.

Common cause contribution to system unavailability was found to be primarily due to common human failures. Human failure resulting in misalignment of manual valves has been addressed in the maintenance contribution. In addition, there is a potential for common miscalibration errors to be applied to all instruments of a particular set. The EFAS and AFRS were reviewed for possible miscalibration errors.

During periodic calibrations, a single technician or group of technicians performs the tests necessary to ensure instrument accuracy. These tests are usually performed sequentially among identical channels. This leads to a close coupling between acts. However, most calibration errors do not result in an instrument that fails to provide the proper signal due to system diversity and redundancy. The SONGS EFAS and AFRS are both two train systems with multiple channels.

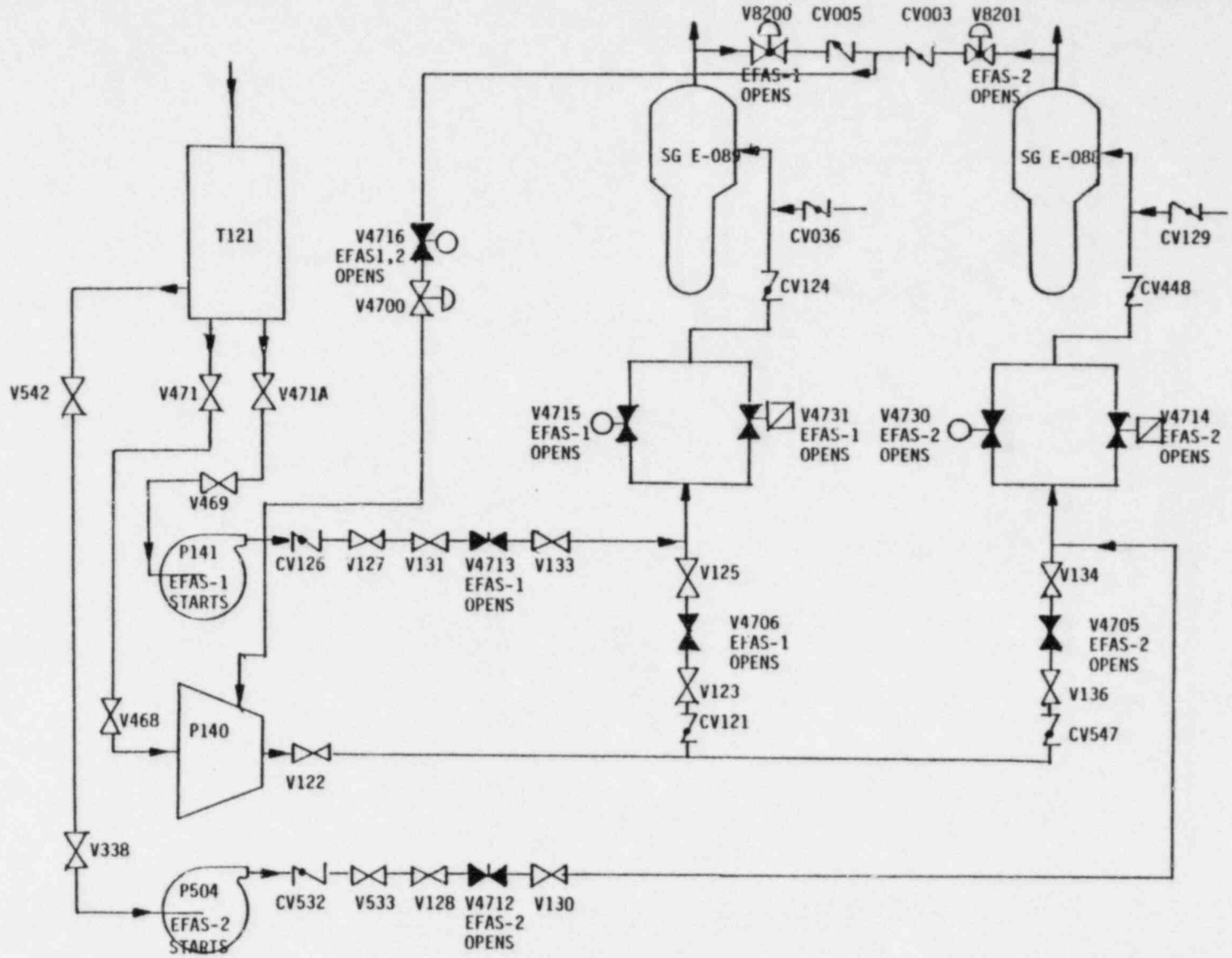
Human reliability analysis based on methodology in Reference (14) was employed to determine the probability of a common cause miscalibration error for the AFRS and the EFAS. It was assumed that the technician uses a written procedure for calibration and a checker inspects the setting. Deviation of the error instrument may also be detected by the operator by comparative scans with similar instruments.

6.11.1 System Description

A schematic of the SONGS Auxiliary Feedwater System is presented in Figure 6.11.1-1. The AFWS is designed to supply an assured source of water to the steam generators during normal plant startup and shutdown in the event of loss of main feedwater supply. The AFWS will start automatically on actuation of an emergency feedwater actuation signal (EFAS). The AFWS automatically regulated by the Auxiliary Feedwater Regulating System (AFRS) after the system's actuation. (The AFRS is expected to be installed at the first refueling outage. System operation was included in the analysis).

The AFWS design includes one 100 percent capacity steam turbine driven pump and two 100 percent capacity motor driven pumps. Each motor driven pump train, including the pump motor and associated control valves, will be powered by a separate emergency diesel generator in the event of loss of offsite power. The turbine driven pump receives steam from the main steam lines upstream of the main steam line isolation valves and exhausts to the atmosphere. The three AFW pumps take suction from Condensate Storage Tank T121 through separate lines.

The Auxiliary Feedwater support system dependency diagram is provided in Figure 6.11.1-2.

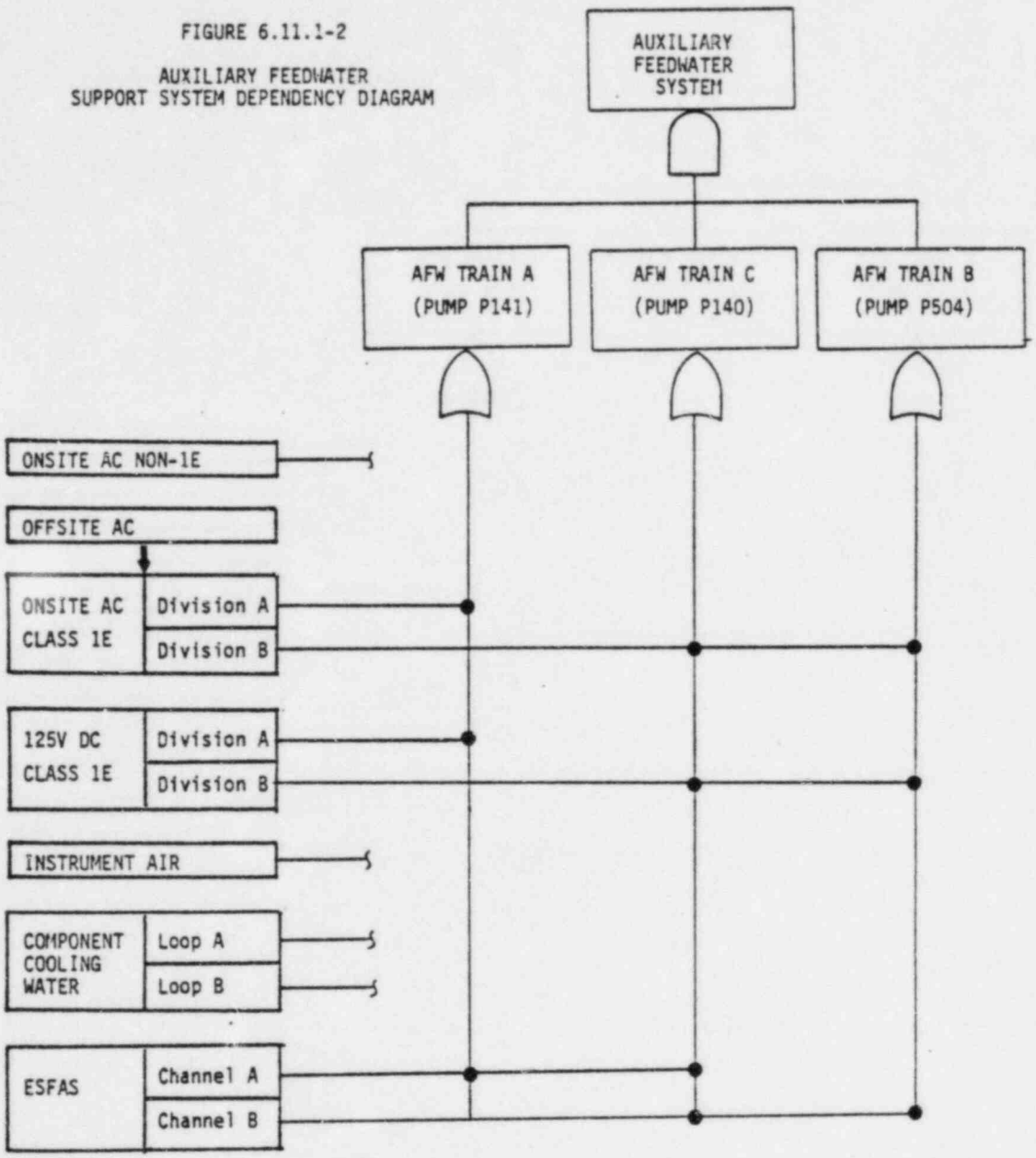


AUXILIARY FEEDWATER SYSTEM

FIGURE 6.11.1-1

FIGURE 6.11.1-2

AUXILIARY FEEDWATER
SUPPORT SYSTEM DEPENDENCY DIAGRAM



6.11.2 Assumptions

The following assumptions were made in performing the fault tree analyses for the Loss of Secondary Heat Sink event trees and the PORV LOCA event trees:

1. For the Loss of Secondary Heat Sink and Spurious PORV LOCA event trees, Failure to Deliver AFW is defined as failing to deliver sufficient AFW flow to at least one SG.

2. For the PORV LOCA with Coincident SGTR event tree, Failure to Deliver AFW to One SG is defined as failing to deliver sufficient AFW flow to the unaffected SG.

3. Passive failures (breach of pressure boundary events) of the AFWS are not considered. Pipe rupture and missile evaluations are not within the scope of work.

4. Operator action to manually actuate the AFWS or to re-establish AFW flow are not considered. Recovery of AFWS will be addressed in a separate analysis. (Section 6.17).

5. Crossties between AFW pumps have minimal effect on system performance in the emergency mode. Their failure would not be a significant contributor to system unavailability and are not modelled.

6. The temporary suction strainers located in the suction line of each AFW pump have been removed.

7. System boundaries are defined to be the SG inlet nozzles to the condensate water storage tanks.

8. The proposed AFRS design consists of a two train system. EFAS1, 2 has priority over AFRS operation. The AFRS bypass control valves and lines are assumed to be not sized to provide sufficient AFW flow.

9. For the SGTR event trees, Excess Feedwater flow is defined as continued undesired feedwater delivery to the affected (or most or least affected) SG.

6.11.3 Results

The fault tree logic diagram for Failure to Deliver AFW was used to determine the probability of failing to deliver sufficient AFW flow to at least one SG. For the Loss of Secondary Heat Sink event trees, the probability of failing to deliver AFW is conditional on the initiating event, Loss of Main Feedwater, i.e., the dependencies which exist between the MFW System and AFW System have been incorporated into the AFW System failure probability. For the Spurious PORV LOCA event tree, the probability of failing to deliver AFW is conditional on the loss of 5% MFW flow to both steam generators. For the PORV LOCA with Coincident SGTR event tree, only the portion of the logic diagram including flow to one SG was used to generate a failure probability for Failure to Deliver AFW to the unaffected SG. For this event tree, the probability of failing to deliver AFW to the unaffected SG is conditional on the loss of 5% MFW flow to the unaffected SG and the dependencies which exist between the two systems have been incorporated into the AFW System failure probability. It should be noted that the results of the above analyses do not include operator action to initiate or restore AFW flow.

For the SGTR event trees, fault tree logic diagrams were used to determine the following probabilities:

- Excess AFW flow to the affected or most affected SG
- Excess AFW or MFW flow to the least affected SG given offsite power is available at the time of the initiating event
- Excess AFW flow to the least affected SG given offsite power is unavailable at the time of the initiating event.

The quantitative results of the analyses are presented as Cases One through Seven respectively in Table 6.11.3-1. The confidence distributions of the failure probabilities are presented in terms of the median values and associated error factors. The error factor is defined as the ratio of the 95 to 50 percentile.

Table 6.11.3-2 contains a list of the dominant cutsets for each case presented in Table 6.11.3-1. Included in the table is a brief description of each cutset as well as the percent contribution to the total failure probability. The percentage is based on a point estimate ratio.

TABLE 6.11.3-1

FAILURE PROBABILITIES FOR SONGS AUXILIARY FEEDWATER SYSTEM

Case Number	Description	Failure Probability (Median Value)	Error Factor
One	Failure to deliver AFW to at least one SG - System Unavailability	1.1E-4[1]	15
Two	Failure to deliver AFW to at least one SG given loss of MFW - System Unavailability	1.1E-4[1]	15
Three	Failure to deliver AFW to at least one SG given a loss of 5% MFW to both SGs - System Unavailability	1.1E-4[1]	15
Four	Failure to deliver AFW to the unaffected SG given PORV LOCA following SGTR and loss of 5% MFW to the unaffected SG - System Unavailability	1.6E-3	6
Five	Excess AFW to the affected or most affected SG given a SGTR - System Unavailability	2.8E-4	14
Six	Excess AFW or MFW to the least affected SG given offsite power is available at the time of the initiating event (SGTR) - System Unavailability	3.0E-4	16
Seven	Excess AFW to the least affected SG given offsite power is unavailable at the time of the initiating event (SGTR) - System Unavailability	2.8E-4	14

1 These values do not include operator action to initiate or restore AFW flow. See Section 6.17 for restoration analysis.

TABLE 6.11.3-2

DOMINANT CUTSETS FOR SONGS AUXILIARY FEEDWATER SYSTEM

Case Number	Cutset	Description	% of Total Failure Probability
One	1. FSER0244	Failure of EFAS-1 and	68%
	FSER0245	Failure of EFAS-2	
	2. FSER0244	Failure of EFAS-1 and	14%
	FSEX0295	EFAS-2 in testing	
	3. FSEX0294	EFAS-1 and	14%
	FSER0245	Failure of EFAS-2	
Two	1. FSER0244	Failure of EFAS-1 and	68%
	FSER0245	Failure of EFAS-2	
	2. FSER0244	Failure of EFAS-1 and	14%
	FSEX0295	EFAS-2 in testing	
	3. FSEX0294	EFAS-1 in testing and	14%
	FSER0245	Failure of EFAS-2	
Three	1. FSER0244	Failure of EFAS-1 and	68%
	FSER0245	Failure of EFAS-2	
	2. FSER0244	Failure of EFAS-1 and	14%
	FSEX0295	EFAS-2 in testing	
	3. FSEX0294	EFAS-1 in testing and	14%
	FSER0245	Failure of EFAS-2	
Four	1. EBGP0161	Grid collapse on TT and	25%
	EDXJ0151	DG2G003 fails to start and	
	APTA0239	Turbine pump fails to start	
	2. EBGP0161	Grid collapse on TT and	18%
	ELBN0172	4.16KV Bus 2A06 fails on LOOP and	
	APTA0239	Turbine pump fails to start	
	3. EBGP0161	Grid collapse on TT and	16%
	EDXJ0151	DG2G003 fails to start and	
	APTV0276	Turbine pump in maintenance	
Five	1. AICP0821	Failure of AFRS-2 and	100%
	AZZ00822	Operator fails to take action	
Six	1. AICP0823	Failure of AFRS-1 and	97%
	AZZ00824	Operator fails to take action	
	2. MICP0825	FWCS 21049 malfunction and	3%
	MZZ00826	Operator fails to take action	
Seven	1. AICP0823	Failure of AFRS-1 and	100%
	AZZ00824	Operator fails to take action	

6.12 BLOWDOWN PROCESSING SYSTEM

Fault tree logic diagrams were used to calculate various Blowdown Processing System failure probabilities that were used as input to the SGTR event trees. The following fault tree models were developed for evaluation:

- Failure to Initiate Blowdown from the Affected SG (SG-088)
- Failure to Open Blowdown Isolation Valve on SG-088 (most affected SG)
- Failure to Open Blowdown Isolation Valve on SG-089 (least affected SG)
- Failure to Initiate Blowdown from Both Steam Generators (least affected and most affected SGs)

It should be noted that for SGTR with coincident LOOP, the BPS is unavailable.

6.12.1 System Description

The Blowdown Processing System (BPS) processes water from the tube bundle area of the steam generators. The blowdown water is filtered and purified to remove any impurities. Then, if meeting appropriate specifications, it is returned to the Condensate System for reuse. The processed blowdown can be directed to the Circulating Water System outfall piping or the Radwaste System in the event that demineralized effluent chemistry exceeds specifications. A schematic of the Blowdown Processing System is presented in Figures 6.12.1-1 and 6.12.1-2.

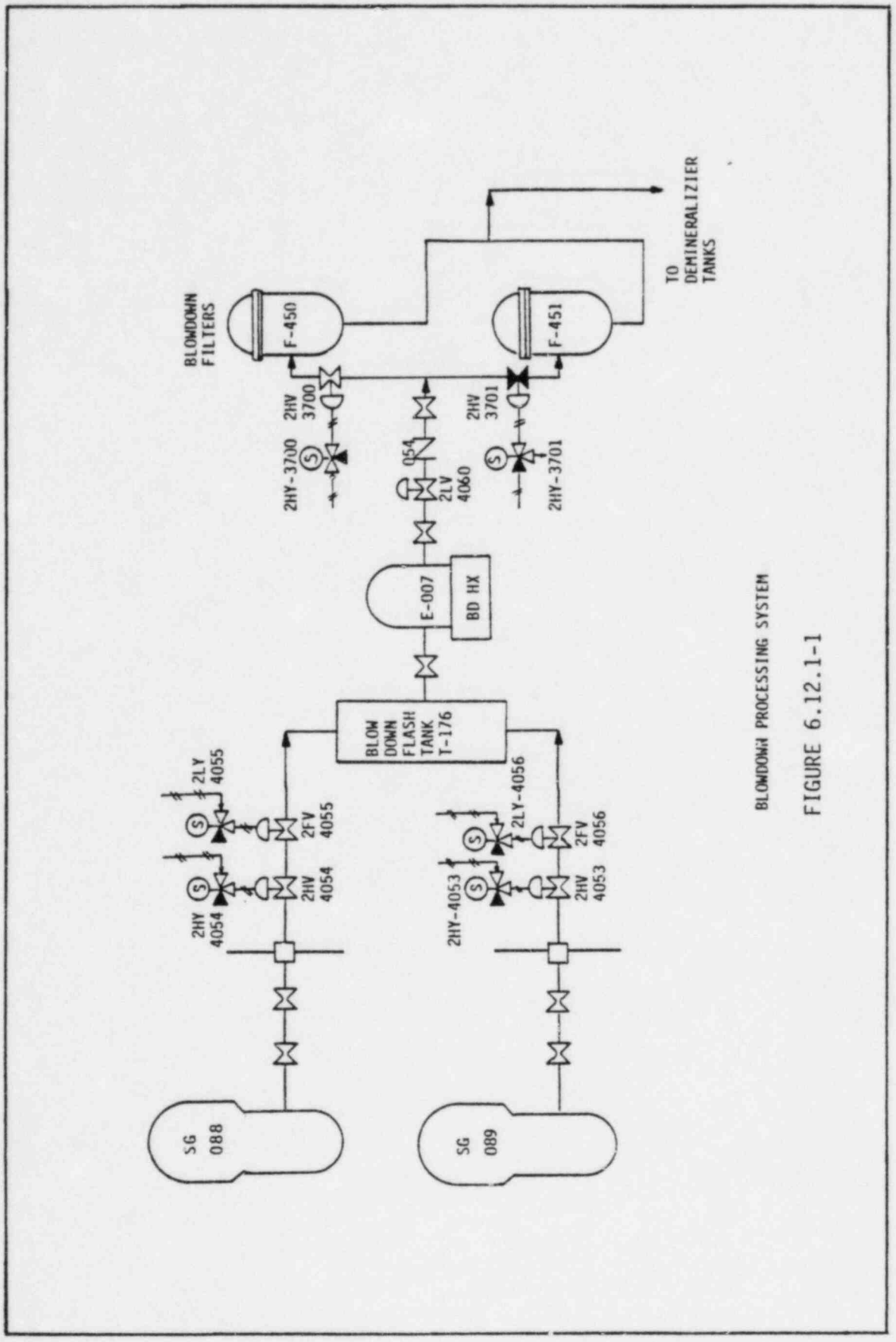


FIGURE 6.12.1-1

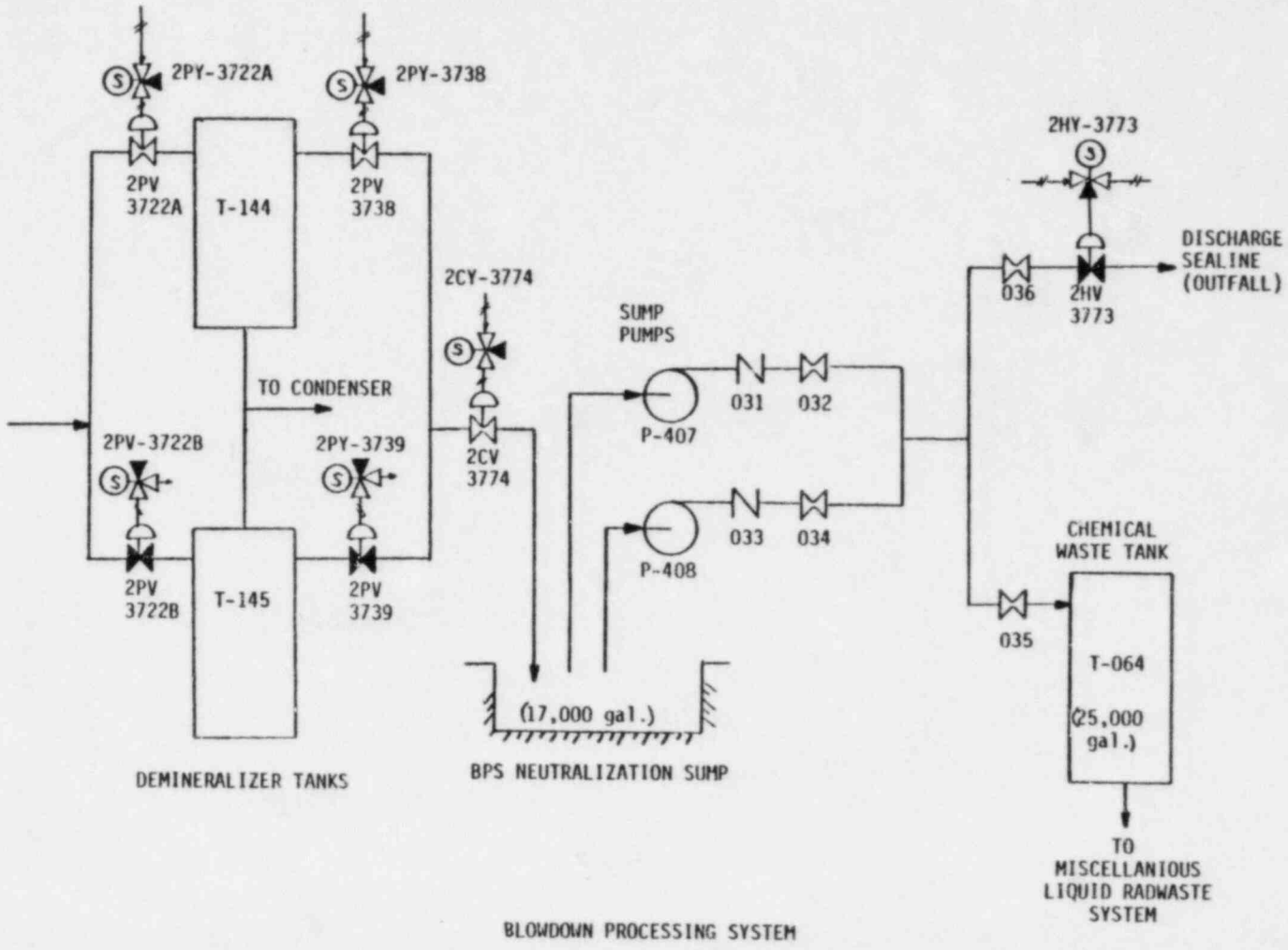


FIGURE 6.12.1-2

Steam generator blowdown flows from separate lines from each SG through the containment to the blowdown isolation valves, HV-4053 and HV-4054. The blowdown lines then traverse the safety equipment building to the turbine building and discharge through flow control valves into the blowdown flash tank T-188.

The blowdown flash tank, T-188, and blowdown heat exchanger, E-007, are located on the 30' and 6' levels, respectively, of the turbine building. These components cool SG blowdown to 120°F for processing by the blowdown filters and demineralizers. The blowdown liquid is cooled by condensate taken from the discharge of the condensate pumps.

The blowdown filters, demineralizers and Regeneration System are located on the 6' level of the turbine building. Filters F-450 and F-451 remove the suspended solid content from SG blowdown. Demineralization is performed by ion exchange in blowdown demineralizers T-144 and T-145.

Upon leaving the demineralizers, the processed blowdown is directed to one of three flow paths, depending on effluent water quality:

- Condenser hotwell - effluent chemistry within specification
- Circulating water outfall - effluent chemistry out of specification
- Chemical waste tank - detectable radioactivity

Two electric motor-driven, vertical, submerged sump pumps are used to pump the neutralization sump contents to either the chemical waste tank T-064 or to outfall. The pumps displace 400 gpm. Service water is utilized to seal, cool and lubricate the pump shaft. Incorporated into the discharge piping of pumps P-407 and P-408 is a radiation detector and a pH meter. Assuming no measurable radioactivity is present and the pH is within the proper range the neutralized water is pumped to outfall.

If a primary to secondary leak develops during normal operation, the Steam Generator Blowdown Processing System is initially isolated to help the operator in determining which steam generator is affected. Once this determination has been made, the BPS is lined up to the affected steam generator.

In the event that blowdown flow to the outfall is automatically isolated on detectable radiation, neutralization sump discharge must be manually aligned to the chemical waste tank.

The Blowdown support system dependency diagram is provided in Figure 6.12.1-3.

6.12.2 Assumptions

The following assumptions were made in performing the fault tree analyses:

1. System failure is defined as the inability to initiate and maintain blowdown flow from the affected (or most or least affected) steam generator following a SGTR.

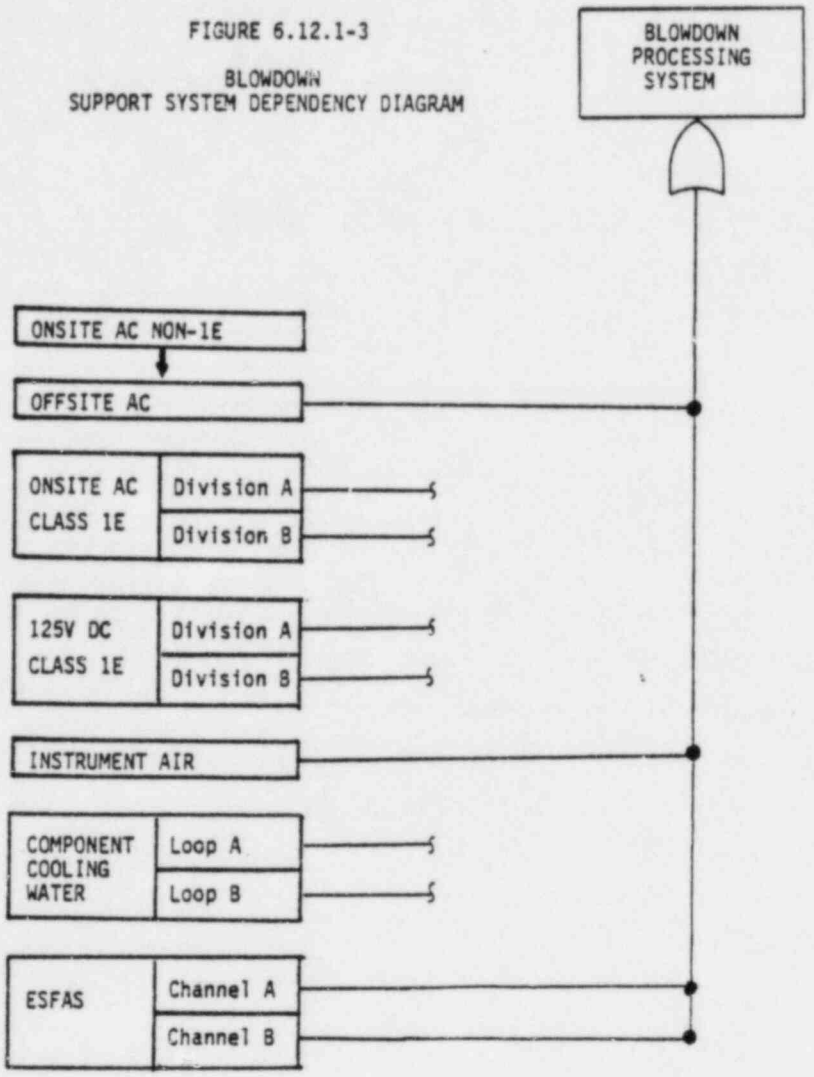
2. In the event of SGTR, BPS system boundaries are assumed to include flow to the chemical waste tank. Flow from the chemical waste tank to the various areas of the radwaste system is not modelled in the fault tree. The radwaste system is assumed to have sufficient capacity to store the desired quantity of blowdown inventory for subsequent processing.

3. Since blowdown flow from the affected SG will include relatively low temperature safety injection inventory, the blowdown heat exchanger is not considered to be a required component for successful BPS operation.

4. The blowdown flowpath shown in Figures 6.12.1-1 and 6.12.1-2 is inferred from information available in References (7) and (30).

FIGURE 6.12.1-3

BLOWDOWN
SUPPORT SYSTEM DEPENDENCY DIAGRAM



5. Service water to the sump pumps is assumed to be available prior to the SGTR and the probability of losing service water during the event is considered to be negligible. It was felt that including the service water system in the fault tree model would unnecessarily complicate the fault without having a significant impact on overall blowdown system reliability.

6. The flowpaths to the condenser and the outfall have been isolated prior to initiation of flow to the chemical waste tank, i.e., there will be no flow diversion to these areas.

7. The sump pump handsiwtch must be switched from the "outfall" position to the "radwaste" prior to starting the pumps. One pump is required and must be manually actuated.

8. Demineralizer control panel L-239 is powered by 480VAC MCC BM.

6.12.3 Results

Fault tree logic diagrams were used to evaluate the following probabilities for input to the SGTR event trees where offsite power is available at the time of the initiating event:

- The probability of failing to initiate and maintain blowdown flow from Steam Generator E-088. This model is applicable for tube rupture(s) in one SG. (Assumed to be SG-088).

- The probability of failing to initiate blowdown flow from Steam Generator E-088. This fault tree refers only to opening the blowdown isolation valve on the most affected SG (SG-088) assuming tube ruptures have occurred in two steam generators.

- The probability of failing to initiate blowdown flow from Steam Generator E-089. This fault tree refers only to opening the blowdown isolation valve on the least affected SG (SG-089) assuming tube ruptures have occurred in two steam generators.

- The probability of failing to initiate and maintain blowdown flow from both steam generators. This model includes failures which would simultaneously prevent blowdown initiation from both steam generators assuming tube ruptures have occurred in both steam generators.

The quantitative results of the analyses are presented as Cases One through Four respectively in Table 6.12.3-1. The confidence distributions of the failure probabilities are presented in terms of the median values and associated error factors. The error factor is defined as the ratio of the 95 to 50 percentile.

Table 6.12.3-2 contains a list of the dominant cutsets for each case presented in Table 6.12.3-1. Included in the table is a brief description of each cutset as well as the percent contribution to the total failure probability. The percentage is based on a point estimate ratio.

TABLE 6.12.3-1

FAILURE PROBABILITIES FOR SONGS BLOWDOWN PROCESSING SYSTEM

Case Number	Description	Failure Probability (Median Value)	Error Factor
One	Failure to Initiate Blowdown from SG-088 - System Unavailability	9.1E-2	3
Two	Failure to Open Blowdown Isolation Valve on SG-088 - System Unavailability	1.2E-2	4
Three	Failure to Open Blowdown Isolation Valve on SG-089 - System Unavailability	1.2E-2	4
Four	Failure to initiate Blowdown from Both Steam Generators - System Unavailability	7.3E-2	3

TABLE 6.12.3-2

DOMINANT CUTSETS FOR SONGS BLOWDOWN PROCESSING SYSTEM

Case Number	Cutset	Description	% of Total Failure Probability
One	1. BVN00797	Operator fails to open manual valve 035-R-221	57%
	2. BPM00809	Operator fails to start sump pumps	27%
Two	1. BVD00794	Operator fails to open isolation valve from control room	89%
	2. BVDA0793	Isolation valve HV-4054 fails to open	10%
Three	1. BVD00814	Operator fails to open isolation valve from control room	89%
	2. BVDA0813	Isolation valve HV-4053 fails to open	10%
Four	1. BVN00797	Operator fails to open manual valve 035-R-221	57%
	2. BPM00809	Operator fails to start sump pumps	27%

6.13 ALTERNATE SECONDARY HEAT REMOVAL CAPABILITY

6.13.1 System Description

A conceptual low pressure secondary feedwater system design is presented in Figure 6.13.1-1. This capability is available to supplement the Auxiliary Feedwater System following a loss of main feedwater event. In the unlikely event of a loss of the safety grade three train AFWS, there are several sources of low pressure water available for use as makeup to the steam generators. The preferred source is the condensate system of the affected unit. The four condensate pumps (head of 500-600 psig) can use water from multiple sources (hotwell, condensate storage tanks) and through use of the feed pump bypass line, deliver makeup directly to each steam generator. Each condensate pump has a capacity of 7750 gpm. The normal condensate makeup sources (hotwell and condensate storage tanks) contain 746,600 gallons. If additional makeup is required, there are several alternate means to refill the storage tanks.

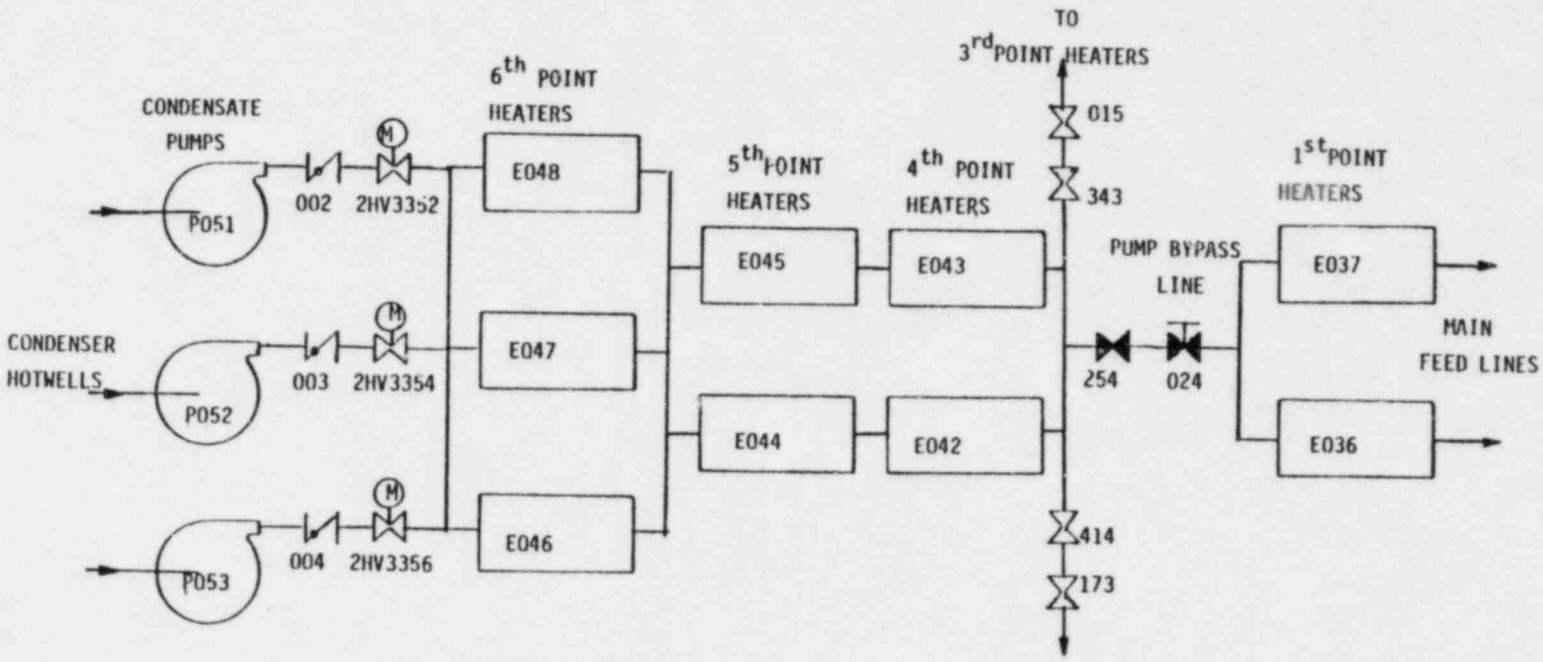
Additional alternate sources of makeup flow include the condensate transfer pump. Another source of high pressure but low flow makeup is available from the chemical additional tanks. For the purpose of the analysis, however, the alternate secondary heat removal capability will be defined as use of a condensate pump from the affected unit.

The condensate support system dependency diagram is provided in Figure 6.13.1-2.

6.13.2 Assumptions

The following assumptions were made in performing the fault tree analysis:

1. System failure is defined as failure to achieve sufficient secondary flow using the condensate system.



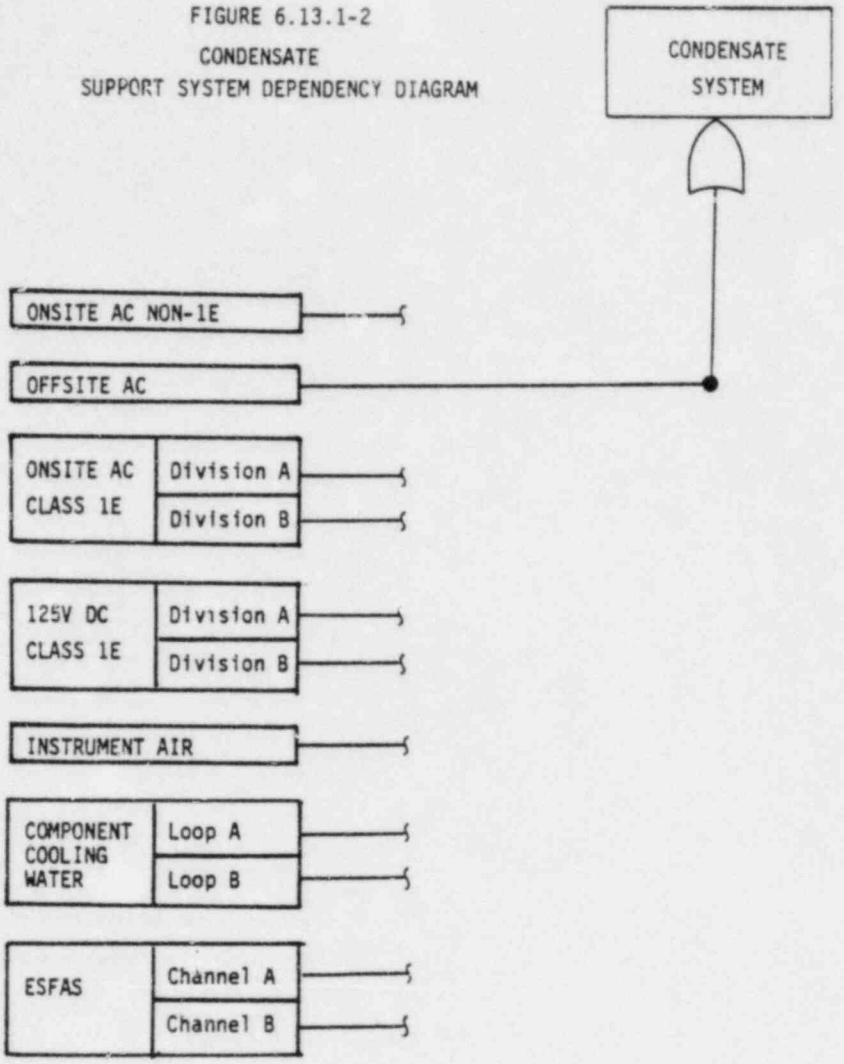
ALTERNATE SECONDARY HEAT REMOVAL CAPABILITY
(CONDENSATE SYSTEM)

FIGURE 6.13.1-1

FIGURE 6.13.1-2

CONDENSATE

SUPPORT SYSTEM DEPENDENCY DIAGRAM



2. Sufficient flow is defined as the flow from one condensate pump delivered to one steam generator.

3. Both steam generators are intact for secondary flow delivery.

4. One condensate pump (P050) is unavailable due to maintenance.

5. Condensate pumps take suction from the condenser hotwells. Makeup to the hotwells from condensate storage tank T120 is included in he fault tree model.

6. The availability of make-up water from Units 3 and 1 is not included in the analysis.

7. Use of the chemical addition tanks (hydrazine and ammonia pumps) or the condensate transfer pump is not considered.

8. Failure to bypass the main feedwater pumps results in failure to deliver sufficient feed flow.

9. The following operator actions to align the secondary system are considered:

   - Operator action to bypass the main feedpumps (Human Error Probability of 0.05).

     Manual Valves 254-R-189
     024-R-082
     343-R-189
     414-R-189

   - Operator action to assure correct positioning of the main feedwater bypass control valves, control valves and isolation valves.

Operator action to establish flow from the condensate pumps will be conducted in parallel with actions to restore auxiliary feedwater flow. The operator will have approximately 50 minutes to align condensate pumps.

10. The operator has a written procedure detailing the necessary actions to establish the alternate flow.

11. Pressure on the secondary side has been reduced using either the steam bypass system or the atmospheric dump system.

6.13.3 Results

The fault tree logic diagram for Failure of the Alternate Secondary Heat Capability was used to determine the probability of failing to achieve sufficient alternate secondary flow for the Loss of Secondary Heat Sink event tree. The model was used to evaluate the following cases:

- Failure of the alternate secondary heat removal capability

- Failure of the alternate secondary heat removal capability given loss of MFW and loss of AFW

For the latter case, the dependencies which exist between the MFW, AFW and Condensate System have been incorporated into the Alternate Secondary Heat Removal Capability failure probability.

The quantitative results of the analyses are presented as Cases One and Two respectively in Table 6.13.3-1. The confidence distributions of the failure probabilities are presented in terms of the median values and associated error factors. The error factor is defined as the ratio of the 95 to 50 percentile.

Table 6.13.3-2 contains a list of the dominant cutsets for each case presented in Table 6.13.3-1. Included in the table is a brief description of each cutset as well as the percent contribution to the total failure probability. The percentage is based on a point estimate ratio.

TABLE 6.13.3-1

FAILURE PROBABILITIES FOR SONGS ALTERNATE SECONDARY HEAT REMOVAL CAPABILITY

Case Number	Description	Failure Probability (Median Value)	Error Factor
One	Failure of the alternate secondary heat removal system - System Unavailability	5.6E-2	5
Two	Failure of the alternate secondary heat removal system given loss of MFW and AFW - System Unavailability	1.4E-1	3

TABLE 6.13.3-2

DOMINANT CUTSETS FOR SONGS ALTERNATE SECONDARY HEAT REMOVAL CAPABILITY

Case Number	Cutset	Description	% of Total Failure Probability
One	1. MVZ00379	Operator fails to align system	>97%
Two	1. EBGP0160	Spurious grid collapse	50%
	2. MVZ00379	Operator fails to align system	45%

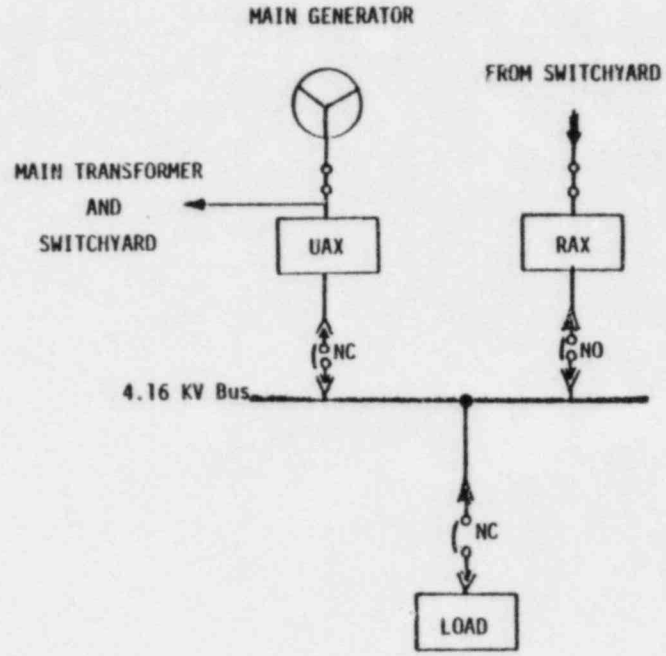
6.14 ELECTRICAL DISTRIBUTION SYSTEM

The Electrical Distribution System fault tree logic diagrams were constructed to support development of the system level fault trees used as input to the systemic event trees. Utilization of the EDS logic diagrams as support branches to other fault trees provides a consistent method of modelling the EDS interactions between mitigating systems. The EDS fault tree logic diagrams were not independently evaluated, therefore, no quantitative results are provided in this section. It should be noted that the fault tree models include system faults that lead to reactor trip as well as failures that may occur after the reactor has tripped. In some cases the EDS logic diagrams were modified to suit the particular system being evaluated, e.g., the HPSI System is actuated post reactor trip, therefore, EDS failures that lead to reactor trip (e.g. a generator fault) would not be applicable as input to the fault tree "Fail to Deliver Sufficient HPSI Flow". Or, if offsite power was given as unavailable, spurious grid collapse would not be included as a valid failure mode in the HPSI fault tree.

6.14.1 System Description

Schematics of the SONGS EDS are provided in Figures 6.14.1-1 to 6.14.1-6. The electrical distribution system is divided into two categories, the non-class 1E power system and the class 1E power system. Both the non-class 1E and class 1E power systems are further divided into AC and DC systems.

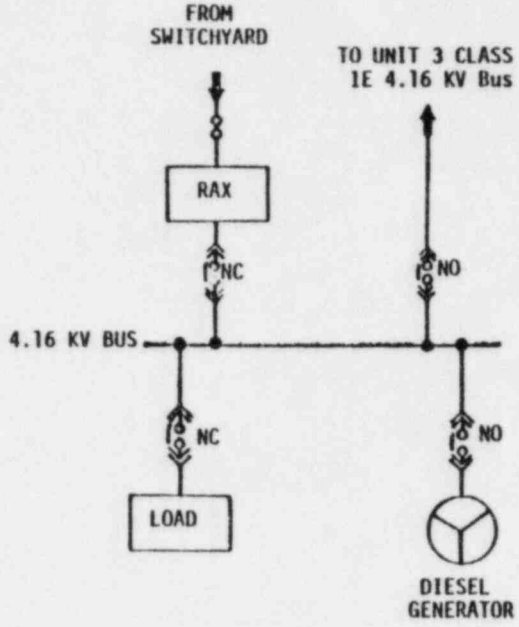
The non-class 1E AC system distributes power at the 6.9KV, 4.16KV, 480V, and 208/120V levels for all non-safety related loads. The non-class 1E AC buses normally are supplied through the unit auxiliary transformers from the main generator. However, during plant startup or shutdown power is supplied from the switchyard through the secondary windings of the reserve auxiliary transformers. In the event of failure of the unit auxiliary transformer, a generator trip, or backup protective trip, fast transfer to offsite power (switchyard) maintains continuity of power to the 4.16KV and 6.9KV non-class 1E buses.



4.16 KV Bus	UAX	RAX
2A08	2XU1	2XR1
2A03	2XU1	2XR1
2A07	2XU1	2XR2
2A09	2XU1	2XR2

TYPICAL NON-CLASS 1E 4.16 KV BUS

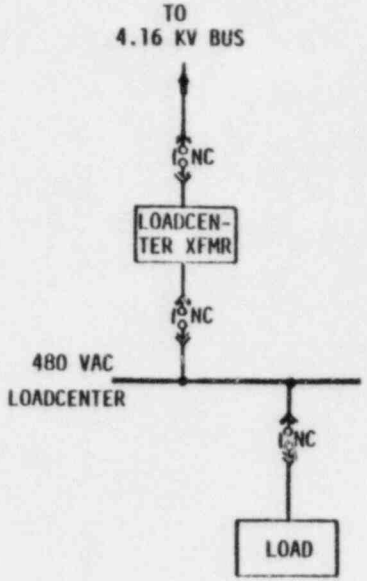
FIGURE 6.14.1-1



4.16 KV BUS	RAX	DG
2A04	2XR1	2G002
2A06	2XR2	2G003

TYPICAL CLASS 1E 4.16 KV BUS

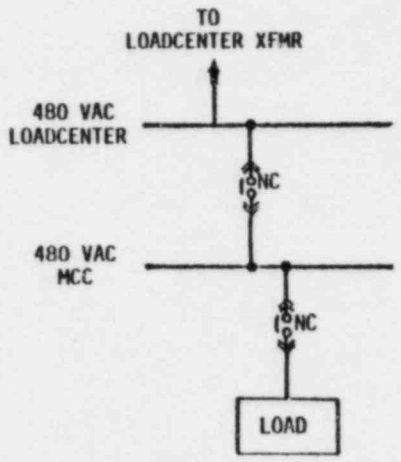
FIGURE 6.14.1-2



480 VAC LC	LC XFMR	4.16 KV BUS
2B01	2B01X	2A08
2B04	2B04X	2A04 (ESF)
2B06	2B06X	2A06 (ESF)
2B09	2B09X	2A09
2B16	2B16X	2A08
2B03	2B03X	2A03
2B11	2B11X	2A07
2B10	B10X-A	2A08

TYPICAL 480 VAC LOADCENTER

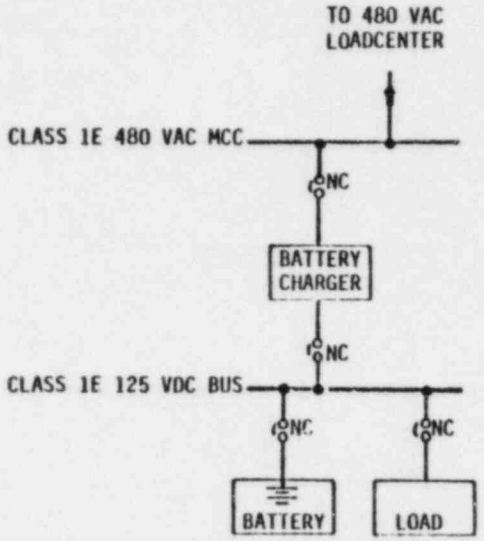
FIGURE 6.14.1-3



480 VAC MCC	480 VAC LC
2BA	2B01
2BE	2B04 (ESF)
2BJ	2B06 (ESF)
2BN	2B09
2BB	2B03
2BX	2B16
2BI	2B11

TYPICAL 480 VAC MCC

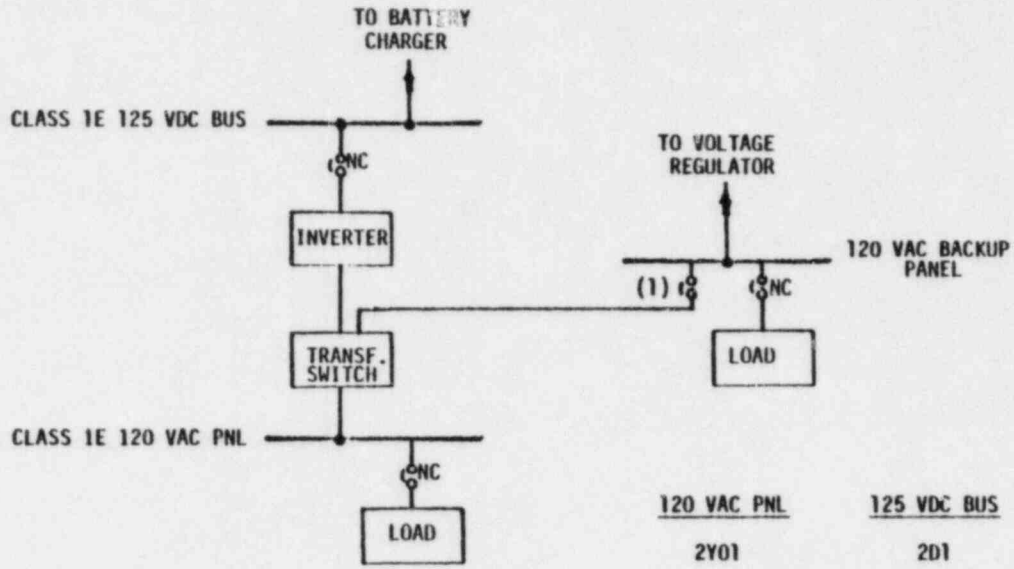
FIGURE 6.14.1-4



125 VDC BUS	BAT.	BAT. CHARGER	480 VAC MCC
2D1	2B007	2B001	2BY
2D2	2B008	2B002	2BZ
2D3	2B009	2B003	2BE
2D4	2B010	2B004	2BJ

TYPICAL CLASS 1E 125 VDC BUS

FIGURE 6.14.1-5



120 VAC PNL	125 VDC BUS
2Y01	2D1
2Y02	2D2
2Y03	2D3
2Y04	2D4

1. Interlocked to prevent simultaneous alignment of two 120 VAC Panels

TYPICAL CLASS 1E 120 VAC PANEL

FIGURE 6.14.1-6

The class 1E AC system distributes power at the 4.16KV, 480V, and 120V levels to safety-related loads. The class 1E AC buses normally are supplied through the reserve auxiliary transformers from the switchyard. In the event of loss of offsite power, the class 1E AC system is powered from the standby diesel generators.

6.14.2 Assumptions

The following assumptions were made in constructing EDS fault tree logic diagrams:

1. Electrical disturbances due to the loss of offsite power have significant impact on only the 4.16 KV class 1E buses.

2. Spurious opening of normally closed circuit breakers is not considered.

3. Third-of-a-kind loads can be powered from either of the two class 1E load groups (trains) through a manual transfer switch. The 125 VDC control power for the third-of-a-kind load is provided from the load group that the load is aligned with.

4. The 125 VDC non-class 1E control power for normally operating loads is available.

5. Operator action is required to realign the third-of-a-kind loads and the 120 VAC class 1E vital buses to their backup power sources.

6.14.3 Results

The results of this evaluation consist of fault tree logic diagrams. EDS interactions can be modelled by utilizing these logic diagrams as support branches to other fault trees.

6.15 COMPONENT COOLING WATER

The Component Cooling Water System fault tree logic diagrams were constructed to support development of the system level fault trees used as input to the systemic event trees. Utilization of the CCW logic diagrams as support branches to other fault trees provides a consistent method of modelling the CCW interactions between mitigating systems. The CCW fault tree logic diagrams were not independently evaluated, therefore, no quantitative results are provided in this section.

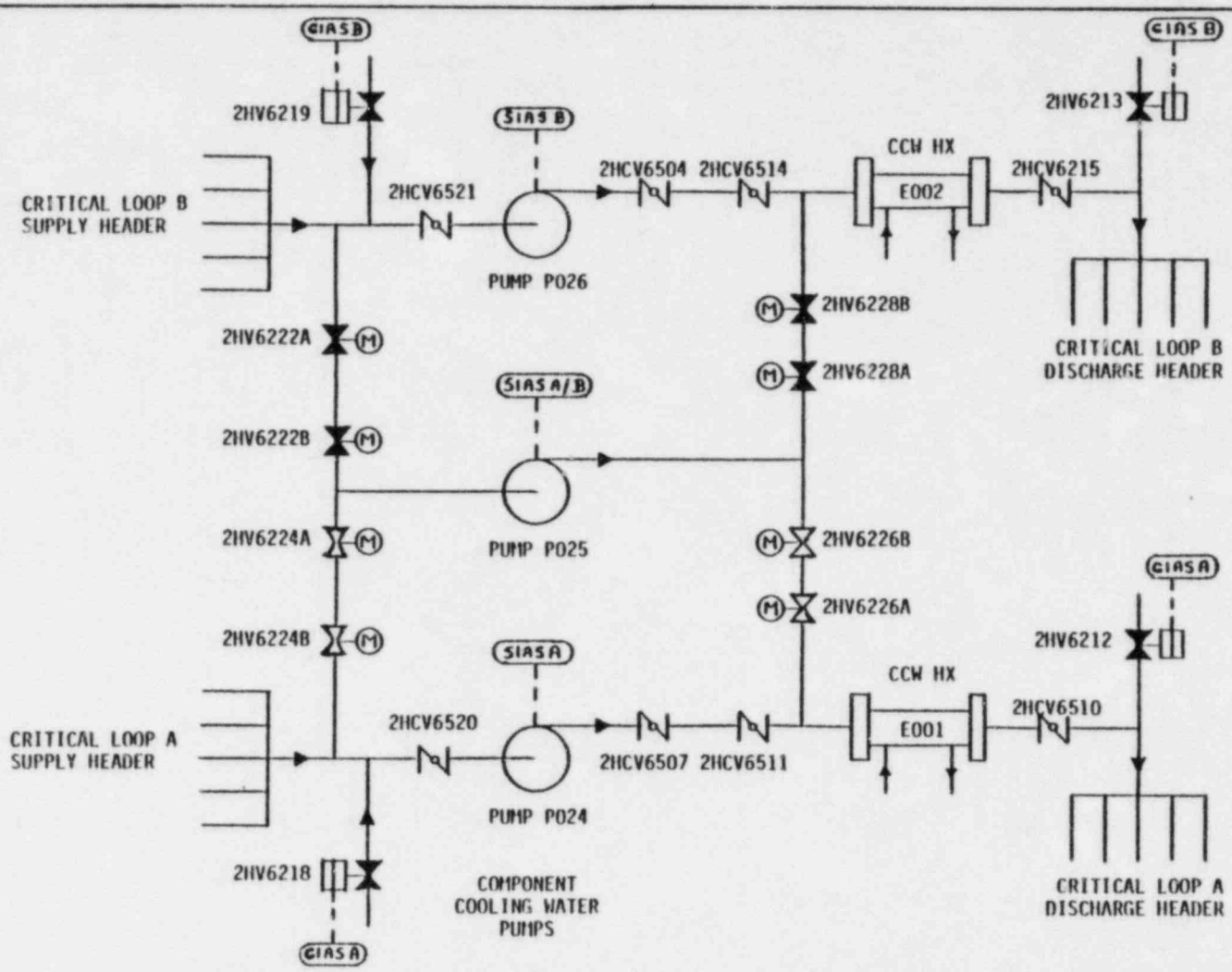
6.15.1 System Description

A schematic of the CCW System is presented in Figure 6.15.1-1. All heat absorbed by the system through the nuclear components of the station is rejected to the sea through the saltwater cooling system. The Pacific Ocean is the ultimate heat sink for the component cooling water system. The system is continuously monitored for radioactivity and all components can be isolated.

The component cooling water system is arranged as two independent, full-capacity, critical cooling loops and one noncritical cooling loop.

Each critical loop provides cooling water to equipment needed for plant shutdown and emergency cooldown conditions. Each critical loop is capable of removing 50% of the heat load generated during the safety injection phase, and 100% of the heat load during the recirculation phase following a LOCA condition.

The noncritical loop supplies cooling water to the components and equipment that require cooling during normal plant operation and/or plant shutdown, including refueling operation.



COMPONENT COOLING WATER SYSTEM

FIGURE 6.15.1-1

The maximum loss of cooling capacity that could result from any single failure would be the loss of one redundant critical loop. Loss of one redundant critical loop does not affect the functional capability of the safety injection system during emergency conditions.

Motors for the three component cooling water pumps are connected to the 4.16KV ESF buses, with emergency diesel-generator backup in the event offsite power is lost. One motor is supplied from a load group A bus, one from a load group B bus, and the third may be manually aligned to either the Group A or the Group B bus as a substitute during maintenance of one of the pumps. On the loss of offsite power, power for the pumps and motor-operated valves required for engineered safety system cooling or normal shutdown cooling is automatically supplied by the emergency diesel generators.

6.15.2 Assumptions

The following assumptions were made in constructing the CCW fault tree logic diagrams:

1. CCW critical loop A is normally operating to supply CCW to non-safety equipment prior to reactor trip.

2. The non-critical CCW flow paths are isolated upon CIAS.

3. CCW pump P025 is aligned to backup CCW pump P026.

4. The heat sink for the CCW heat exchangers is available.

6.15.3 Results

The results of this evaluation consist of fault tree logic diagrams. CCW interactions can be modelled by utilizing these logic diagrams as support branches to other fault trees.

6.16 INSTRUMENT AIR SYSTEM

This analysis includes construction and evaluation of a fault tree logic diagram for Loss of Instrument Air. The model is used to evaluate the probability of Loss of Instrument Air prior to and following a reactor trip. The results are used as input to the system level fault trees.

6.16.1 System Description

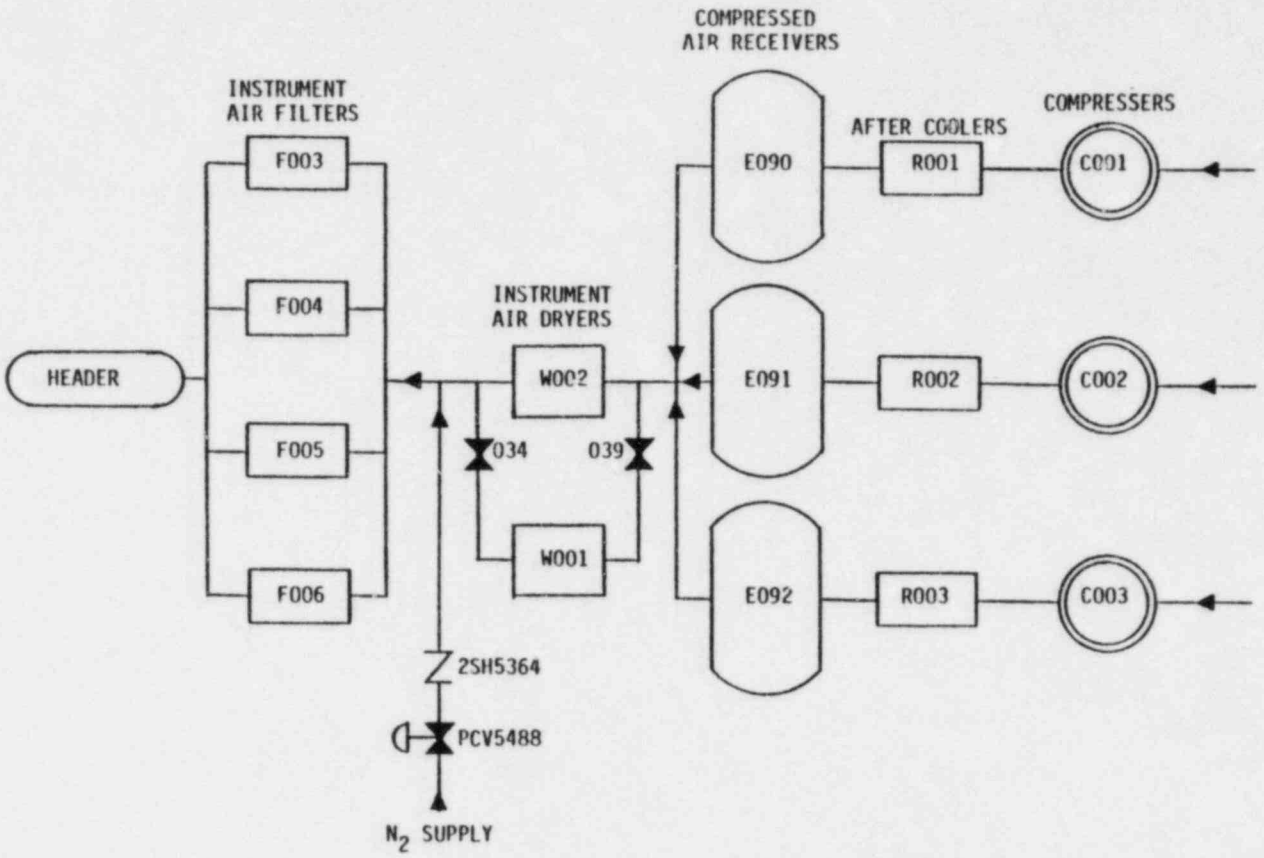
A schematic of the SONGS Instrument Air System is presented in Figure 6.16.1-1. The Instrument Air System includes three identical 100% capacity air compressing trains. Each train consists of an air intake filter/silencer, a compressor unit, an inter-and after cooler with moisture separator, an air receiver, and interconnecting piping and valving. The three air receivers are connected in parallel by a common header. The Instrument Air then passes through a drying/filtering train. The drying/filtering train consists of two parallel refrigerated dryer units. The air passes next to the air header for distribution to the instrument air piping system.

The instrument air system is required for normal operation and startup of the plant. One air compressing train is in service during normal operation with the other two in standby. A pressure switch installed in the instrument air supply main header provides an actuation signal for the standby air compressors. A back-up nitrogen system is actuated by a pressure control valve on loss of air pressure (air pressure < 70 psig). The instrument air system is not essential for safe shutdown of the plant and is unavailable on loss of offsite power.

6.16.2 Assumptions

The following assumptions were made in performing the fault tree analysis:

1. System failure is defined as the inability to maintain sufficient compressed air supply in the instrument air lines. Sufficient compressed air is defined as one compressor train air supply or the backup nitrogen supply.



COMPRESSED AIR SYSTEM

FIGURE 6.16.1-1

2. System boundaries include the air intake filters to the instrument air header.

3. Compressing unit C001 is in service during normal operation with compressing units C002 and C003 in standby.

4. Lag 1 compressing unit starts automatically at 98 psi and loads to 50%, at 94 psi it loads to 100% capacity.

5. Lag 2 compressing unit starts automatically at 90 psi and loads to 50%, at 86 psi it loads to 100% capacity.

6. The backup nitrogen supplies the instrument air header automatically at 70 psi.

7. Failures associated with the air intake filter/silencer, inter-after coolers, and air receivers are not considered in the fault tree model.

8. Operator action to establish a compressed air supply is not included in the fault tree model.

6.16.3 Results

A fault tree logic diagram was used to evaluate the following failure probabilities:

- Loss of instrument air prior to reactor trip. This value was used as input to the Loss of Main Feedwater frequency evaluation.

- Loss of instrument air following reactor trip.

- Loss of instrument air following reactor trip given offsite power is available at the time of the initiating event. This value was used as input to fault trees in the SGTR event trees.

It should be noted that the Instrument Air System is assumed to be unavailable following loss of offsite power.

The quantitative results of the analyses are presented as Cases One through Three respectively in Table 6.16.3-1. The confidence distributions of the failure probabilities are presented in terms of the median values and associated error factors. The error factor is defined as the ratio of the 95 to 50 percentile.

Table 6.16.3-2 contains a list of the dominant cutsets for each case presented in Table 6.16.3-1. Included in the table is a brief description of each cutset as well as the percent contribution to the total failure probability. The percentage is based on a point estimate ratio.

TABLE 6.16.3-1

FAILURE PROBABILITIES FOR SONGS INSTRUMENT AIR SYSTEM

Case Number	Description	Failure Rate/Probability (Median Value)	Error Factor
One	Loss of instrument air-System Failure Rate	4.8E-6/hr.	2
Two	Loss of instrument air-System Unavailability	1.7E-3	7
Three	Loss of instrument air-System Unavailability given offsite power is available at the time of the initiating event	3.0E-4	10

TABLE 6.16.3-2

DOMINANT CUTSETS FOR SONGS INSTRUMENT AIR SYSTEM

Case Number	Cutset	Description	% of Total Failure Rate/ Probability
One	1. EBGP0160	Spurious grid collapse	96%
	2. ITHE0064	Loss of instrument air header	.7%
Two	1. EBGP0161	Grid collapse on TT	77%
	2. EBFR0165	Failure of fast transfer logic	18%
Three	1. EBFR0165	Failure of fast transfer logic	83%
	2. ELBN0166 ELBN0168	4.16 KV Bus 2A03 fails on LOOP 4.16 KV Bus 2A07 fails on LOOP	3%

6.17 RESTORATION OF FEED FLOW ANALYSIS

6.17.1 Methodology

An analysis of the Human Error Probability (HEP) of the operator manually restoring secondary feedwater flow following a loss of heat sink was performed. The analysis was based on the methodology developed by Swain and Guttmann (14). A model of operators' actions was developed based on plant operating procedures and instructions, and interviews with an operator and an operator instructor. A human error probability event tree was then developed. The event tree models the operators actions as discrete events performed sequentially. Recovery factors and operator discovery of previous errors were also considered in the analysis. Physical indications, such as meters or status lights, provide indication that previous actions were done incorrectly. This gives the operator an opportunity to correct himself. Each discrete action is analyzed and a total error probability for eachactivity is calculated. The discrete actions are then combined to give operator error probabilities. The methodology used in this analysis is described in the PRA Procedures Guide (6) and in a specific procedural guide for human reliability analysis (14).

The first step in developing the HEP event tree was to become familiar with the loss of heat sink event and secondary systems. The MFW and AFW systems were reviewed. Plant emergency procedures for loss of feedwater were also used (8). For the purposes of this study, total loss of feedwater flow was the initiating event and restarting any one of the three independent AFW trains constituted successful recovery of feed flow. SGTR was not considered. After reviewing the AFW system design, a reactor operator and an instructor from the C-E simulator were interviewed to determine how the operator would attack the problem and in what order he would attempt to restore auxiliary feedwater equipment.

A HEP event tree was developed which graphically displays operator actions as a series of single discrete actions which the operator either successfully completes or fails to complete. The actions are ordered sequentially in time. The HEP event tree was reviewed with the instructor and operator.

The HEP event tree was generated for the most general case, failure of the AFW actuation signal (EFAS). In this case, all three AFW trains are available. For more specific cases, such as having one pump out of service for maintenance at the start of the transient, the general HEP event tree was modified by eliminating non-existing branches.

A task analysis table was generated for the total restoration activity. Each specific task was listed and human error probabilities including dependencies and modifications were assigned. A HEP for each specific action was calculated. The full HEP event tree was then evaluated for the failure of the EFAS. For other failure modes, specific parts of the total event tree were used. Success was obtained if the operator started any one of the three auxiliary feedwater trains.

6.17.2 Analysis and Assumptions

The analysis for restoration of auxiliary feedwater was divided into two parts: 1) detecting no feedwater flow and 2) starting one of the three auxiliary feedwater trains.

The initial actions of the operator following a reactor scram are shown in Table 6.17.2-1. These actions are automatic and occur with every reactor scram (about 7 times/RY). The operator first checks that the reactor scrams. He then checks for AC power and ESF actuation. These actions include checking the displays from his present location and take only a few seconds. Next, the operator checks the feedwater panel to verify delivery of 5% MFW flow or auxiliary feedwater flow. The operator spends little or no time trying to restore main feedwater. His primary concern after reactor trip is to stabilize the plant and he will rely on the auxiliary feedwater system since this system is simpler and designed as a redundant backup.

The operators scan the feedwater control panel to recognize the total loss of feedwater condition (Step 8 of Table 6.17.2-1). The operator will check feedwater flow and steam generator level. These meters are located in a prominent location on the panel and are used constantly during normal operation. If the operator misreads these two meters, he will assume that the automatic control (MFW or AFW) is operating and will not spend any more time on the feedwater panel. He may recover from this error by reading the AFW status on the ESF panel. He could later recover by noticing primary coolant pressure and temperature are increasing. Approximately 15 minutes after reactor trip, the primary safety valves lift and additional alarms go off indicating to the operator that there is a RCS heat generated/heat removed mismatch. The operator has about thirty-five minutes after the safety valves lift (50 minutes after reactor trip) to recognize that there is no feedwater flow before core damage conditions cannot be prevented (28, Section 2.8).

The operator is assumed to be at a normal stress level for the initial SG status readings and at a moderatly high stress level for subsequent actions. Dependencies of specific actions on the execution of the previous action are also considered in the analysis. The probability of the operator not recognizing total loss of feedwater in the allotted time is less than 1.0E-4.

Operator action includes three basic activities in restoring the AFW. He first attempts to start AFW by manually activating the EFAS (assuming no signal was generated). If he fails at this activity, he will manually start the pump and open the AFW valves. Recovery activities at each step are considered.

For manual override of the EFAS, the operator has four push buttons he can activate. He can omit this step or make a commission error (wrong push buttons). Complete dependency between the four switches is assumed, i.e., if he fails to activate the first switch, he will fail to activate the other three switches. If he fails to start the pumps, he may correct himself by noticing the pump status indicators on the ESF panel or pump status lights on the pump handswitch.

If the operator fails to initiate AFW by activating the EFAS (or the EFAS fails) he can manually start the pumps from the control room. Again complete dependency between the operator starting the first pump and starting the other two pumps was assumed. The operator starts all three pumps as a single activity. The HEPs for failure to start one pump and for failure to start all three is therefore identical. If he fails to start one of the pumps, he has two chances to recover. He can either notice there is no pump discharge pressure or he can notice the pump status light on the ESF panel. If he fails to start the pump, he does not recover during the valve alignment step and AFW is not restored. This is a conservative assumption.

The next general task required of the operator is to open AFW manual discharge, control and isolation valves. For the general case of failure of the EFAS signal, he can open any one of the three valve trains. For specific cases, he must open a specific train or one of two trains. For the electric pumps, the discharge, control and isolation valves (one of two isolation valves) must be open. There are control valve position lights on both the feedwater and ESF panels to help in recovery actions. The operator can open any one of the two isolation valves but a moderate dependency was assumed between the two valves. No credit was given for error recovery for correcting one train or valve while working on another.

When the operator fails to restore a valve, his final action is to send an auxiliary operator to manually open the valve at the valve location. Both operator and auxiliary operator errors are included. Since the auxiliary operator is performing a dynamic activity, the HEP has a stress adjustment of five times the normal HEP. The error probability for the operator and auxiliary operator restoring a single valve is 0.080. (In the second case where the operator has 20 minutes, no manual valve corrections are assumed possible.) The total HEP value of the operator failing to align the valves for the electric driven pump is 1.0E-3. For the general case where any one of three trains can be opened, a high dependency between aligning the first and subsequent trains was assumed. The HEP for failing to align the remaining two trains was 0.5 each. The turbine driven AFW train has

two steam supply valves (one from each SG), and a turbine control valve. The HEP for failing to align the turbine control valve is 1.0E-4 (2.0E-4 for Case 2). The HEP for failing to start the turbine-driven AFW train is 8.0E-4 (1.5E-3 for Case 2).

One of the failure modes considered in this study is station blackout. Recovery is defined as restoration of offsite AC power or restoration of the diesel generator. The restoration of offsite power was taken from an EPRI study (21) and is consistent with WASH-1400 (16). Failure probabilities for restoration of offsite AC are 0.23 (1 hr.) and 0.32 (20 min.). The failure probability of restoration of the diesel generator was taken from Reference (35) and is 0.77 (1 hr.) and 0.84 (20 min., linear interpolation). The combined failure to restore any AC power is 0.18 (1 hr.) and 0.27 (20 min.). It was also assumed that for station blackout, manual correction of valves was not possible in Case 1 because the operator would concentrate on restoring power (Step 3, Table 6.17.2-1).

6.17.3 Results

The Human Error Probabilities (HEPs) for specific actions and combined actions (Table 6.17.3-1) were used to calculate the probability of failing to restore auxiliary feedwater for specific failure modes. An earlier fault tree analysis of the AFW system identified the dominant failure modes. For the thirty most probable failure modes, restoration failure probabilities were calculated and are given in Table 6.17.3-2. Results for both the fifty minute period and twenty minute period are given. Case 1 represents the best estimate case where the operator has 50 minutes to restore feedwater before fuel damage is unavoidable. Case two represents the case where the operator has twenty minutes to restore feedwater before he must commit to use of feed and bleed operation (28, Section 2.8).

The results are based on three operators trying to restore AFW flow. One operator is assigned to the primary side and the second operator is assigned to the secondary side and operates the EFW controls. It is assumed there is a high dependency between the two operators. The control room supervisor assists the two operators after twenty minutes but also has a high dependency on the actions of the secondary side operator (model suggested by Swain and Guttmann). Contributions by the shift supervisor, the shift technical advisor, and the nuclear auxiliary operator (NAO) are neglected although they would also be present. This would reduce the HEPs since the additional personnel could identify errors. This effect has not been considered in this study.

The error bounds for HEPs listed in Table 6.17.3-2 are given in Table 6.17.3-3. These values are taken from Tables 20 - 26 of Reference (14). An error factor of 1.0 was assigned to the cases where the operator is assumed to fail, i.e., HEP of 1.0.

The HEPs developed for the various failure modes of Table 6.17.3-2 were combined to determine the total failure probability for restoration of AFW. To determine the total failure probability, the restoration failure probability for each failure mode was multiplied by the fraction of AFW unavailability contributed by that failure mode. Failure modes not addressed in detail by the analysis were conservatively considered to be non-restorable and therefore have a HEP of 1.0 with an error factor of 1.0. The failure modes specifically analyzed comprise approximately 99.3% of the total AFW unavailability. The sum of the products of the HEP and fraction of system unavailability yields the probability of failing to restore feedwater flow given a loss of MFW and AFW flow. The failure to restore feedwater flow results and associated error factors for the 50 and 20 minute time periods presented in Table 6.17.3-4 are employed in the Loss of Secondary Heat Sink event tree analysis. The error factor is defined as the ratio of the 95 to 50 percentile.

TABLE 6.17.2-1

INITIAL OPERATOR ACTIONS FOR
TOTAL LOSS OF FEEDWATER[1]

1) Reactor scrams. Lights and alarms alert operator.

2) Operator verifies reactor trip by actuating all 4 reactor manual trip pushbuttons.

3) Operator verifies turbine trip.

4) Operator scans power panel to see if transfer from auxiliary to startup transformer has occurred.

   a) If failed - loss of off-site power

   b) Manual transfer used if necessary

   c) Diesel generator status check

5) Operator verifies unit output breakers are open and turbine speed is decreasing.

6) Operator scans ESF panel for actuation

7) Operator verifies SG pressure is at 1000 psia.

8) Operator scans feedwater panel for 5% runback (MFW flow)

[1] Obtained from Operating Instruction SO23-3-5.1, Immediate Operator Action.

TABLE 6.17.3-1

HEP FOR COMBINED TASKS

Action	Description	Value	
		Case One (50 min.)	Case Two (20 min.)
I	Manually Open Valve	8.0E-2	1.0
DT	Actuate ESFAS Signal	2.5E-4	5.0E-4
E_{TOT}	Actuate Pump (Electric or Steam)	8.0E-4	1.5E-3
F_{TOT}	Manually Align Valves	1.0E-3	2.0E-3
AC	Restore AC Power	1.8E-1	2.7E-1
ES	Start Steam Pump	8.0E-4	1.5E-3
EE	Start One Electric Pump	8.0E-4	1.5E-3
F_i	Alignment of Valves on Train i	1.0E-4	2.0E-4

TABLE 6.17.3-2

HEPs for RESTORATION OF AUXILIARY FEEDWATER
FOR SPECIFIC EVENTS

Failure Mode	Combined Actions	Failure to Restore Prob. 50 Min.	20 Min.
ESFAS Failure	DT	2.5E-4	5.0E-4
Station Blackout Turbine Pump FTS	AC	1.8E-1	2.7E-1
Station Blackout Turbine Pump Maint.	AC	1.8E-1	2.7E-1
Condensate Tank T120	-	No Action Required	
AFRS	DT	2.5E-4	5.0E-4
1 Motor Pump in Maint. Turbine Pump FTS 1 Motor Pump FTS	ES	8.0E-4	1.5E-4
1 Motor Pump in Maint. Turbine Pump FTS Control Valve FTO	ES X I	4.0E-4	7.5E-4
Station Blackout Battery 2B009 Fails	AC	1.8E-2	2.7E-1
Station Blackout Motor Valve 4716 FTO	AC	1.8E-2	2.7E-1
1 Motor Pump in Maint. Turbine Pump FTS Manual Discharge Vlv Closed	ES X I	4.0E-4	7.5E-4
Station Blackout Manual Valve Closed	AC	1.8E-2	2.7E-1
1 Motor Pump in Maint. Turbine Pump FTS Motor Pump FTS	ES	8.0E-4	1.5E-3
Station Blackout Turbine Pump FTR	AC	1.8E-1	2.7E-1

TABLE 6.17.3-2
(continued)

HEPs for RESTORATION OF AUXILIARY FEEDWATER
FOR SPECIFIC EVENTS

Failure Mode	Combined Actions	Failure to Restore Prob. 50 Min.	20 Min.
Check Valves FTO	No Action	1.0	1.0
Pumps FTS (All)	E_{TOT}	8.0E-4	1.5E-3
1 Motor Pump FTS Turbine Pump FTS Control Valve FTO	ES	8.0E-4	1.5E-3
Turbine Pump FTS Control Valves FTO	ES	8.0E-4	1.5E-3
1 Motor Pump FTS Turbine Pump FTS Manual Discharge Vlv. Closed	ES	8.0E-4	1.5E-3
1 Motor Pump FTS 1 Control Valve FTO Manual Discharge Vlv. Closed	EE	8.0E-4	1.5E-3
Turbine Pump FTS 2 Manual Discharge Valves Closed	ES X I	4.0E-4	7.5E-4
Turbine Pump in Maint. 2 Motor Pumps FTS	E_{TOT}	8.0E-4	1.5E-3
Turbine Pump in Maint. 1 Motor Pump FTS 1 Control Val FTO	ES + F_{TOT}	4.0E-4	7.5E-4
Turbine Pump in Maint. 2 Control Valves FTO	I	8.0E-2	1.0
1 Motor Pump in Maint. Turbine Pump FTS Manual Suction Valve Plugged	ES	8.0E-4	1.5E-3

TABLE 6.17.3-2
(continued)

HEPs for RESTORATION OF AUXILIARY FEEDWATER
FOR SPECIFIC EVENTS

Failure Mode	Combined Actions	Failure to Restore Prob. 50 Min.	20 Min.
1 Motor Pump in Maint. Turbine Pump FTS Discharge Valve Plugged	ES	8.0E-4	1.5E-3
1 Motor Pump in Maint. Turbine Pump FTS Motor Pump Actuation Act. Relay Fails	ES	8.0E-4	1.5E-3
1 Motor Pump in Maint. Turbine Pump FTS Control Valve Act. Relay Fails	ES	8.0E-4	1.5E-3
1 Motor Pump in Maint. Turbine Pump FTS Check Valve FTO	ES	8.0E-4	1.5E-3
1 Motor Pump in Maint. Turbine Steam Vlv FTO 1 Motor Pump FTR	I	8.0E-2	1.0
Station Blackout Manual Valve Plugged in Turbine Line	AC	1.8E-1	2.7E-1

TABLE 6.17.3-3

ERROR BOUNDS FOR AFW-HEP CALCULATIONS
GIVEN IN TABLE 6.17.3-2

Basic Value	Error Bounds
HEP Task Probability $< 10^{-1}$	$X \div 10$
HEP Task Probability $> 10^{-1}$	$X \div [1/(HEP + e)]$

e = Small Number

TABLE 6.17.3-4

FAILURE TO RESTORE FEED FLOW PROBABILITIES

Restoration Time Period (min.)	Failure Probability	Error Factor
50	1.7E-2	1.4
20	2.2E-2	1.5

7.0 ACCIDENT SEQUENCE ANALYSIS

7.1 LOSS OF SECONDARY HEAT SINK SEQUENCE ANALYSIS

The core damage scenarios resulting from loss of secondary heat sink were determined based on the systemic event trees developed in Section 5.1. (See Figure 5.1.4.1-1 and Figure 5.1.4.2-1.) The loss of heat sink analysis was performed with and without primary feed and bleed capability. Section 7.1.1 will discuss the minimal core damage scenarios for the current plant design including the use of a low pressure secondary alternate decay heat removal system. Section 7.1.2 will discuss the minimal core damage scenarios assuming primary feed and bleed operation is provided.

7.1.1 Loss of Heat Sink Core Damage Scenarios

The loss of heat sink core damage scenarios are presented in Table 7.1.1-1. One minimal core damage scenario was identified. The total frequency of scenarios eliminated by the cutoff frequency of 10^{-8} per year is approximately 9.4E-9 per year. The result is presented in terms of the median frequency and associated error factor. The scenario can be described as failure of the safety function, RCS Heat Removal. The magnitude and impact of the core damage frequency are discussed in Section 9.0. The accident sequence is discussed below:

Scenario 1. $LF\text{-}G_1U_1V$

This sequence is defined by Loss of Main Feedwater, Failure to Deliver AFW Flow, Failure to Restore Feed Flow and Failure of the Alternate Secondary Heat Removal Capability. In this sequence, core damage conditions are a result of failure to provide a secondary heat sink. This loss of heat sink involves the failure of the AFW System, and a failure to manually establish the low-pressure alternate heat sink. The preferred course of action following a loss of main and auxiliary feed flow is the restoration of

TABLE 7.1.1-1

LOSS OF SECONDARY HEAT SINK
CORE DAMAGE SEQUENCES

	Path	Description	Frequency (Median value per year)	Error Factor
1.	LF-G_1U_1V	• Initiating Event • Fail to Deliver AFW Flow • Failure to Restore Feed Flow • Failure of Alt. Sec. Heat Removal Capability	3.14E-07	21
		Total Core Damage Frequency	3.1E-07	21

AFW flow with the alternate secondary system being employed after restoration actions have failed. The analysis assumed a 50 minute time period following reactor trip on low steam generator level for operator action (28, Section 2.8). (Introduction of feed flow after the 50 minute time period, while resulting in core damage conditions as set forth in this study, would aid in the accident mitigation).

The loss of secondary heat sink analysis determined a core damage frequency of 3.1E-7 per year. Factors that contributed to this loss of heat sink core damage frequency are:

- AFW System Design. There are no major single component cutset contributors to the SONGS AFWS system unavailability. In addition, the major contributors to system unavailability are restorable by operator action within the 50 minute time period employed in the analysis.

- Electric Distribution System Design. Electrical power is supplied to plant equipment through multiple power sources. Four class 1E 125 VDC power subsystems are provided for each unit. Each subsystem is independent and consists of one 125V battery, one battery charger, one distribution switchboard and one ESF distribution panel. The battery chargers of each subsystem are supplied separately with 480 VAC ESF power. Each unit has 2 backup diesel generators available in the event of loss of offsite power.

- Operator Action. The operator has approximately 50 minutes following reactor trip to restore the AFW system and prevent core damage conditions. The time period allowed consideration of local manual actions.

- Alternate Secondary Heat Removal Capability. The analysis also considered the use of a low-pressure source of secondary feedwater flow (condensate pumps).

7.1.2 Loss of Secondary Heat Sink with Feed and Bleed Operation Core Damage Scenarios

The loss of secondary heat sink with feed and bleed capability core damage scenarios are presented in Table 7.1.2-1. Two minimal core damage scenarios were identified. The total frequency of scenarios eliminated by the cutoff frequency of 10^{-9} per year is approximately 1.3E-9 per year. The scenarios can be described as failure of the safety function RCS Heat Removal by the primary feed and bleed system. Also listed in Table 7.1.2-1 is the total core damage frequency contribution for the Loss of Secondary Heat Sink event assuming feed and bleed operation is provided. The total core damage frequency represents a statistical combination (using the SAMPLE code described in Section 2.2.3.5) of the two core damage sequences identified in Table 7.1.2-1. The magnitude and impact of the core damage frequency contribution due to loss of heat sink assuming feed and bleed capability is provided are discussed in Section 9.0. The accident sequences are discussed below:

Scenario 1. LF-G_1U_2Y This sequence is defined by loss of Main Feedwater, Failure to Deliver AFW Flow, Failure to Restore Feed Flow, and Failure of Feed Bleed Operation. In this sequence, main and auxiliary feed flow are unavailable and primary feed and bleed operation, primary depressurization by the PORVs and injection by Charging System and/or HPSI System flow, has failed. The analysis assumed that the operator initiated feed and bleed operation at 20 minutes into the transient (28, Section 2.8). For the 20 minute time period following reactor trip, plant personnel will be directed towards restoration of AFW. Restoration of AFW following the initiation of feed and bleed

TABLE 7.1.2-1

LOSS OF SECONDARY HEAT SINK
WITH FEED AND BLEED OPERATION CORE DAMAGE SEQUENCES

Path	Description	Frequency (median value)	Error Factor
1. LF-G_1U_2Y	• Initiating Event • Fail to Deliver AFW Flow • Failure to Restore Feed Flow • Failure of Feed Bleed Operation	1.54E-07	29
2. LF-G_1U_2R	• Initiating Event • Fail to Deliver AFW Flow • Failure to Restore Feed Flow • Failure to Achieve HP Recirc.	5.76E-09	40
	Total Core Damage Frequency	1.6E-07	28

operation is not considered. Due to the time limitations, use of low-pressure alternate secondary capability is also not considered. A separate task analysis was performed to determine the probability of restoring AFW in a 20 minute time period. Note also that the Feed and Bleed System design employed is not redundant. Both trains of PORVs located off the pressurizer are required for successful depressurization. (See Section 6.5).

Scenario 2. LF-G_1U_2R

This sequence is defined by Loss of Main Feedwater, Failure to Deliver AFW Flow, Failure to Restore Feed Flow, and Failure to Achieve HPSI Recirculation Flow. In this scenario, the normal secondary heat sink, main and auxiliary feedwater flow, is unavailable. The primary Feed and Bleed System is successful in depressurizing the primary system and providing makeup flow. However, to reach Shutdown Cooling entry conditions, Feed and Bleed Operation is assumed to require the HP recirculation flow. Failure to achieve recirculation flow will result in depletion of the RWT inventory and subsequent HPSI pump failure and core damage conditions.

7.2 STEAM GENERATOR TUBE RUPTURE SEQUENCE ANALYSIS

The core damage scenarios resulting from SGTR were selected from the list of event tree output sequences provided in Figures 5.2.4.1-1, 5.2.4.2-1, 5.2.4.3-1 and 5.2.4.4-1. Any sequence including a failed open secondary valve or a failure to deliver sufficient HPSI flow was assumed to lead to core damage. Only the minimal core damage scenarios were used to calculate the total core damage frequency. The accident sequences associated with each SGTR initiating event are discussed in detail in the following sections.

None of the minimal core damage scenarios obtained from the four SGTR event trees contained the branch Fail to Initiate Auxiliary Spray Flow due to the cutoff frequencies used to filter the accident sequences. Therefore, the use of PORVs as a backup to the Auxiliary Spray System is expected to have a negligible impact on the total core damage frequency derived for each of the four SGTR initiating events. The effect of PORVs on SGTR core damage frequency is quantitatively discussed in Section 7.2.5.

7.2.1 SGTR in One Steam Generator Core Damage Scenarios

The SGTR in one SG core damage scenario are presented in Table 7.2.1-1. Seven minimal core damage scenarios were identified. The total frequency of scenarios eliminated by the cutoff frequency of 10^{-8} per year is approximately 2.4E-7 per year. The results are presented in terms of the median frequencies and associated error factors. Also listed in Table 7.2.1-1 is the total core damage frequency contribution for SGTR in One SG. The total core damage frequency represents a statistical combination (using the SAMPLE code described in Section 2.2.3.5) of the seven core damage sequences identified in Table 7.2.1-1. The magnitude and impact of the core damage frequency contribution due to SGTR are discussed in Section 9.0. The core damage scenarios are discussed below.

TABLE 7.2.1-1

SGTR IN ONE SG CORE DAMAGE SEQUENCES

Path	Description	Frequency (Median Value per Year)	Error Factor
1. T1-OQ_1L	• Initiating Event • Fail to Throttle HPSI • Fail to Initiate Blowdown • ADV on Affected SG Fails to Reclose	1.95E-8	26
2. T1-OQ_1KM_1	• Initiating Event • Fail to Throttle HPSI • Fail to Initiate Blowdown • ADV on Affected SG Unavailable • 1 MSSV on Affected SG Fails to Reclose	5.42E-8	10
3. T1-F_1M_1	• Initiating Event • Loss of TBV Flow Prior to Iso. of Affected SG • 1 MSSV on Affected SG Fails to Reclose	1.02E-6	7
4. T1-DM_1	• Initiating Event • TBV Fails to Reclose • 1 MSSV on Affected SG Fails to Reclose	9.25E-7	11
5. T1-DE_1	• Initiating Event • TBV Fails to Reclose • MSIV on Affected SG Fails to Close	8.50E-8	10
6. T1-C_1M_1	• Initiating Event • TBVs Fail to Quick Open • 1 MSSV on Affected SG Fails to Reclose	4.07E-6	9
7. T1-A	• Initating Event • Fail to Deliver Sufficient HPSI Flow	1.43E-6	6
	Total Core Damage Frequency:	1.0E-5	5

Scenario 1. $T1\text{-}0Q_1L$ Following a tube rupture in one SG, the affected SG is isolated and RCS cooldown is initiated using the intact SG. However, the operator maintains RCS pressure by failing to throttle HPSI which results in a large integrated leak flow through the tube rupture. If blowdown is not initiated from the affected SG, the SG is assumed to fill with subcooled water. The ADV is opened by the operator to prevent a MSSV from opening and begins to discharge primary inventory. When the ADV fails to close (outside containment LOCA) a large pressure differential develops between the RCS and the SG which supports a continued leak flow. Eventually, RWT inventory is assumed to reach the RAS setpoint and the potential lack of inventory leads to subsequent core damage.

Scenario 2. $T1\text{-}0Q_1KM_1$ Following a tube rupture in one SG, the affected SG is isolated and RCS cooldown is initiated using the intact SG. However, the operator maintains RCS pressure by failing to throttle HPSI which results in a large integrated leak flow through the tube rupture. Blowdown flow from the affected SG is not initiated and the SG is assumed to fill with subcooled water. The operator fails to open the ADV from the control room which results in a challenge to the MSSV with the lowest open setpoint (2PSV-8401). The MSSV opens and begins to discharge primary inventory. When the MSSV fails to reclose (outside containment LOCA) a large pressure differential develops between the RCS and the SG which supports a continued leak

flow. Eventually, RWT inventory is assumed to reach the RAS setpoint and the potential lack of inventory leads to subsequent core damage.

Scenario 3. $T1\text{-}F_1M_1$ In this scenario, turbine bypass flow is lost prior to isolation of the affected SG. The resulting upward pressure transient in the steam generators causes one MSSV on each SG to open. The MSSV on the affected SG fails to close (outside containment LOCA) and a large pressure differential develops between the RCS and the SG which supports continued leak flow. Eventually RWT inventory is assumed to reach the RAS setpoint and the potential lack of inventory leads to subsequent core damage.

Scenario 4. $T1\text{-}DM_1$ Following a tube rupture in one SG, the TBVs Quick Open following Turbine Trip to prevent the MSSVs from being challenged. In this scenario, one TBV fails to reclose which leads to low SG pressure and a subsequent MSIS. The resulting upward pressure transient in the steam generators eventually causes one MSSV on each SG to open. The MSSV on the affected SG fails to close (outside containment LOCA) and a large pressure differential develops between the RCS and the SG which supports continued leak flow. Eventually RWT inventory is assumed to reach the RAS setpoint and the potential lack of inventory leads to subsequent core damage.

Scenario 5. $T1\text{-}DE_1$ Following a tube rupture in one SG, the TBVs Quick Open following Turbine Trip to prevent the MSSVs from being challenged. In this scenario, one TBV fails to reclose which leads to low SG pressure

and a subsequent MSIS. The MSIV on the affected SG fails to close which results in uncontrolled blowdown through the TBS. The large pressure differential between the RCS and the affected SG supports a continued leak flow. Eventually, RWT inventory is assumed to reach the RAS setpoint and the potential lack of inventory leads to subsequent core damage.

Scenario 6. T1-C_1M_1 — In this scenario, the TBVs fail to quick open following turbine trip. The resulting pressure spike opens 5 MSSVs on each SG. (The steam flow through 10 MSSVs is estimated to be equivalent to the steam flow capacity of the TBS). One MSSV on the affected SG fails to reclose (outside containment LOCA) and a large pressure differential is assumed to develop between the RCS and the affected SG. The continued leak flow eventually causes RWT inventory to reach the RAS setpoint and the potential lack of inventory leads to subsequent core damage.

Scenario 7. T1-A — Following a tube rupture in one SG, the HPSI system fails to deliver sufficient HPSI flow. Decreasing RCS inventory combined with the lack of inventory makeup is assumed to lead to core uncovery and subsequent core damage.

7.2.2 SGTR in One Steam Generator with Coincident Loss of Offsite Power Core Damage Scenarios

The SGTR in one SG with coincident LOOP core damage scenarios are presented in Table 7.2.2-1. Six minimal core damage scenarios were identified. The total frequency of scenarios eliminated by the cutoff frequency of 10^{-10} per year is approximately 1.7E-9 per year. The results are presented in

TABLE 7.2.2-1

SGTR IN ONE SG WITH COINCIDENT LOOP CORE DAMAGE SEQUENCES

Path	Description	Frequency (Median Value per Year)	Error Factor
1. T2-M_2	• Initiating Event • MSSV on Affected SG Fails to Close Following TT	4.93E-7	15
2. T2-L	• Initiating Event • ADV on Affected SG Fails to Close	9.07E-10	46
3. T2-KM_1	• Initiating Event • ADV on Affected SG Unavailable • MSSV on Affected SG Fails to Reclose	2.56E-9	18
4. T2-OKM_1	• Initiating Event • Fail to Throttle HPSI • ADV on Affected SG Unavailable • MSSV on Affected SG Fails to Recluse	5.49E-10	27
5. T2-A	• Initiating Event • Fail to Deliver Sufficient HPSI Flow	7.42E-8	37
6. T2-A'	• Initiating Event • Fail to Maintain HPSI Flow	1.43E-8	45
	Total Core Damage Frequency	7.4E-7	20

terms of the median frequencies and associated error factors. Also listed in Table 7.2.2-1 is the total core damage frequency contribution for SGTR in One SG with Coincident LOOP. The total core damage frequency represents a statistical combination (using the SAMPLE code described in Section 2.2.3.5) of the six core damage sequences identified in Table 7.2.2-1. The magnitude and impact of the core damage frequency contribution due to SGTR are discussed in Section 9.0. The core damage scenarios are discussed below.

Scenario 1. $T2\text{-}M_2$ Following a tube rupture in one SG with coincident LOOP, the TBS is unavailable on turbine trip. The secondary pressure spike following turbine trip causes 5 MSSVs to open on each SG. In this scenario, one MSSV on the affected SG fails to reclose following turbine trip (outside containment LOCA) and a large pressure differential is assumed to develop between the RCS and the affected SG. The continued leak flow eventually causes RWT inventory to reach the RAS setpoint and the potential lack of inventory leads to subsequent core damage.

Scenario 2. T2-L Following a tube rupture in one SG with coincident LOOP, the TBS is unavailable. The operator is required to open the ADVs to initiate cooldown. In this scenario, the ADV on the affected SG fails to close (outside containment LOCA) and a large pressure differential is assumed to develop between the RCS and the affected SG. The continued leak flow eventually causes RWT inventory to reach the RAS setpoint and the potential lack of inventory leads to subsequent core damage.

Scenario 3. T2-KM_1 Following a tube rupture in one SG with coincident LOOP, the operator is required to open the ADVs to initiate cooldown. In this scenario, the ADV on the affected SG fails to open which causes one MSSV on the affected SG to open. The MSSV fails to reclose and a large pressure differential is assumed to develop between the RCS and the affected SG. The continued leak flow eventually causes RWT inventory to reach the RAS setpoint and the potential lack of inventory leads to subsequent core damage.

Scenario 4. T2-$0KM_1$ Following a tube rupture in one SG with coincident LOOP, the affected SG is isolated and RCS cooldown is initiated using the intact SG. However, the operator maintains RCS pressure by failing to throttle HPSI which results in a large integrated leak flow through the tube rupture. Since the blowdown system is unavailable the SG is assumed to fill with subcooled water. The operator fails to open the ADV from the control room and one MSSV on the affected SG opens and fails to reclose. The resulting pressure differential between the RCS and the affected SG supports a continued leak flow until RWT inventory reaches the RAS setpoint. The potential lack of inventory is assumed to lead to subsequent core damage.

Scenario 5. T2-A Following a tube rupture in one SG with coincident LOOP, the HPSI system fails to deliver sufficient HPSI flow. Decreasing RCS inventory combined with the lack of inventory makeup is assumed to lead to core uncovery and subsequent core damage.

Scenario 6. T2-A' In this scenario, 480V AC power is being supplied to the HPSI system from the diesel generators. The HPSI system is unable to maintain sufficient flow for eight hours following the SGTR with coincident LOOP. Decreasing RCS inventory combined with insufficient inventory makeup is assumed to lead to core uncovery and subsequent core damage.

7.2.3 SGTR in Two Steam Generators Core Damage Scenarios

The SGTR in both SG core damage scenarios are presented in Table 7.2.3-1. Nine minimal core damage scenarios were identified. The total frequency of scenarios eliminated by the cutoff frequency of 10^{-8} per year is approximately 4.8E-7 per year. The results are presented in terms of the median frequencies and associated error factors. Also listed in Table 7.2.3-1 is the total core damage frequency contribution for SGTR in Two SGs. The total core damage frequency represents a statistical combination (using the SAMPLE code described in Section 2.2.3.5) of the nine core damage sequences identified in Table 7.2.3-1. The magnitude and impact of the core damage frequency contribution due to SGTR are discussed in Section 9.0. The core damage scenarios are discussed below.

Scenario 1. T3-DE_2 Following tube ruptures in both SGs, the TBVs quick open following turbine trip to prevent the MSSVs from being challenged. In this scenario, one TBV fails to reclose which leads to low SG pressure and a subsequent MSIS. The MSIV on the least affected SG fails to close which results in uncontrolled SG blowdown through the TBS. The large pressure differential between the RCS and the least affected SG supports a continued leak

TABLE 7.2.3-1

SGTR IN TWO SG CORE DAMAGE SEQUENCES

Path	Description	Frequency (Median Value per Year)	Error Factor
1. T3-DE_2	• Initiating Event • TBV Fails to Reclose • MSIV on Least Affected SG Fails to Close	1.71E-8	13
2. T3-DE_1	• Initiating Event • TBV Fails to Reclose • MSIV on Most Affected SG Fails to Close	1.71E-8	13
3. T3-C_1M_1	• Initiating Event • TBVs Fail to Quick Open • MSSV on Most Affected SG Fails to Reclose	7.34E-7	11
4. T3-C_1I_1	• Initiating Event • TBVs Fail to Quick Open • MSSV on Least Affected SG Fails to Reclose	7.44E-7	12
5. T3-F_1M_1	• Initiating Event • Loss of TBV Flow Prior to Iso. of Affected SG • MSSV on Most Affected SG Fails to Reclose	2.14E-7	10
6. T3-F_1I_1	• Initiating Event • Loss of TBV Flow Prior to Iso. of Affected SG • MSSV on Least Affected SG Fails to Reclose	2.07E-7	10
7. T3-DM_1	• Initiating Event • TBV Fails to Reclose • MSSV on Most Affected SG Fails to Reclose	1.87E-7	11

TABLE 7.2.3-1
(Continued)
SGTR IN TWO SG CORE DAMAGE SEQUENCES

Path	Description	Frequency (Median Value per Year)	Error Factor
8. T3-DI_1	• Initiating Event • TBV Fails to Reclose • MSSV on Least Affected SG Fails to Reclose	1.83E-7	14
9. T3-A	• Initiating Event • Fail to Deliver Sufficient HPSI Flow	2.83E-7	8
	Total Core Damage Frequency	3.7E-6	7

flow to the least affected SG. Eventually, RWT inventory is assumed to reach the RAS setpoint and the potential lack of inventory leads to subsequent core damage.

Scenario 2. $T3\text{-}DE_1$ This scenario is similar to $T3\text{-}DE_2$ except that the MSIV on the most affected SG fails to close on MSIS.

Scenario 3. $T3\text{-}C_1M_1$ This scenario is similar to $T1\text{-}C_1M_1$ except that the MSSV on the "affected" SG becomes the MSSV on the "most affected" SG.

Scenario 4. $T3\text{-}C_1I_1$ This scenario is similar to $T3\text{-}C_1M_1$ except that the MSSV on the least affected SG fails to reclose following failure of the TBVs to quick open.

Scenario 5. $T3\text{-}F_1M_1$ This scenario is similar to $T1\text{-}F_1M_1$ except that the MSSV on the "affected" SG becomes the MSSV on the "most affected" SG.

Scenario 6. $T3\text{-}F_1I_1$ This scenario is similar to $T3\text{-}F_1M_1$ except that the MSSV on the least affected SG fails to reclose following loss of TBV flow prior to isolation of the most affected SG.

Scenario 7. $T3\text{-}DM_1$ This scenario is similar to $T1\text{-}DM_1$ except that the MSSV on the "affected" SG becomes the MSSV on the "most affected" SG.

Scenario 8. $T3\text{-}DI_1$ This scenario is similar to $T3\text{-}DM_1$ except that the MSSV on the least affected SG fails to reclose.

Scenario 9. T3-A This scenario is similar to T1-A. Only the initiating events differ.

7.2.4 SGTR in Two Steam Generators with Coincident Loss of Offsite Power Core Damage Scenarios

The SGTR in two SGs with coincident LOOP core damage scenarios are presented in Table 7.2.4-1. Ten minimal core damage scenarios were identified. The total frequency of scenarios eliminated by the cutoff frequency of 10^{-10} per year is approximately 7.6E-10 per year. The results are presented in terms of the median frequencies and associated error factors. Also listed in Table 7.2.4-1 is the total core damage frequency contribution for SGTR in Two SGs with Coincident LOOP. The total core damage frequency represents a statistical combination (using the SAMPLE code described in Section 2.2.3.5) of the ten core damage sequences identified in Table 7.2.4-1. The magnitude and impact of the core damage frequency contribution due to SGTR are discussed in Section 9.0. The core damage scenarios are discussed below.

Scenario 1. T4-M_2 This scenario is similar to T2-M_2 except that the MSSV on the "affected" SG becomes the MSSV on the "most affected" SG.

Scenario 2. T4-I_2 This scenario is similar to T4-M_2 except that the MSSV on the least affected SG fails to reclose following turbine trip.

Scenario 3. T4-L This scenario is similar to T2-L except that the ADV on the "affected" SG becomes the ADV on the "most affected" SG.

Scenario 4. T4-H This scenario is similar to T4-L except that the ADV on the least affected SG fails to close.

TABLE 7.2.4-1

SGTR IN TWO SG WITH COINCIDENT LOOP CORE DAMAGE SEQUENCES

Path	Description	Frequency (Median Value per Year)	Error Factor
1. T4-M_2	• Initiating Event • MSSV on Most Affected SG Fails to Close Following TT	1.05E-7	14
2. T4-I_2	• Initiating Event • MSSV on Least Affected SG Fails to Close Following TT	1.05E-7	17
3. T4-L	• Initiating Event • ADV on Most Affected SG Fails to Close	1.58E-10	37
4. T4-H	• Initiating Event • ADV on Least Affected SG Fails to Close	1.63E-10	41
5. T4-KM_1	• Initiating Event • ADV on Most Affected SG Unavailable • MSSV on Most Affected SG Fails to Close	4.76E-10	24
6. T4-JI_1	• Initiating Event • ADV on Least Affected SG Unavailable • MSSV on Least Affected SG Fails to Close	5.38E-10	19
7. T4-OKM_1	• Initiating Event • Fail to Throttle HPSI • ADV on Most Affected SG Unavailable • MSSV on Most Affected SG Fails to Close	1.14E-10	29
8. T4-OJI_1	• Initiating Event • Fail to Throttle HPSI • ADV on Least Affected SG Unavailable • MSSV on Least Affected SG Fails to Close	1.12E-10	27

TABLE 7.2.4-1
(Continued)
SGTR IN TWO SG WITH COINCIDENT LOOP CORE DAMAGE SEQUENCES

Path	Description	Frequency (Median Value per Year)	Error Factor
9. T4-A	• Initiating Event • Fail to Deliver Sufficient HPSI Flow	1.54E-8	39
10. T4-A'	• Initiating Event • Fail to Maintain HPSI Flow	2.97E-9	43
	Total Core Damage Frequency	2.8E-7	15

Scenario 5. T4-KM_1 This scenario is similar to T2-KM_1 except that the MSSV on the "affected" SG becomes the MSSV on the "most affected" SG.

Scenario 6. T4-JI_1 This scenario is similar to T4-KM_1 except that the ADV on the least affected SG fails to open and the MSSV on the least affected SG fails to reclose.

Scenario 7. T4-OKM_1 This scenario is similar to T2-OKM_1 except that the MSSV on the "affected" SG becomes the MSSV on the "most affected" SG.

Scenario 8. T4-OJI_1 This scenario is similar to T4-OKM_1 except that the ADV on the least affected SG fails to open and the MSSV on the least affected SG fails to reclose.

Scenario 9. T4-A This scenario is similar to T2-A. Only the initiating events differ.

Scenario 10. T4-A' This scenario is similar to T2-A'. Only the initiating events differ.

7.2.5 The Effect of PORVs on SGTR Core Damage Frequencies

The consequences of a SGTR and PORV LOCA are addressed in Section 7.3.2. For this discussion, the role of PORVs in SGTR events will focus on the backup RCS depressurization capability provided by PORVs should the Auxiliary Spray System be unavailable. In order to quantify the effect of PORV depressurization capability on SGTR core damage frequencies, all minimal core damage scenarios containing the branch Fail to Initiate Auxiliary Spray Flow were selected from the list of potential core damage sequences that fell below the cutoff frequency for each event tree. The accident sequences were quantified using the branch median failure

probabilities to determine the core damage frequency for each scenario. The results are presented in Table 7.2.5-1. (See Section 5.2.4 for branch descriptions). Table 7.2.5-2 provides the total core damage frequency of all minimal sequences that include failure of the Auxiliary Spray System for each event tree with and without the added depressurization capability of PORVs. As shown in Table 7.2.5-2, the decrease in core damage frequency due to the added depressurization capability of PORVs is negligible compared to the core damage frequency contribution from all other SGTR accident sequences.

7.2.6 Steam Generator Overfill Scenarios

One of the NRC questions concerning SGTR focused on the likelihood of steam lines filling with subcooled water following a SGTR event. Potential SG overfill scenarios were selected from the list of event tree output sequences provided in Figures 5.2.4.1-1, 5.2.4.2-1, 5.2.4.3-1 and 5.2.4.4-1. SG overfill was assumed to occur if one of the following failure combinations appeared in an accident scenario:

- Excess feedwater to the affected (or most or least affected) SG

- Failure to throttle HPSI and failure to initiate auxiliary spray flow. The high primary to secondary pressure differential would result in a high integrated leak flow to the affected (or most affected and least affected) SG.

- Failure to throttle HPSI and failure to initiate blowdown from the affected (or most or least affected SG). Failure to throttle HPSI leads to a large integrated leak flow. If the blowdown system was unavailable, SG overfill could occur. For SGTR with coincident LOOP the blowdown system is unavailable, therefore, failure to throttle HPSI flow would result in SG overfill.

TABLE 7.2.5-1

MINIMAL CORE DAMAGE SEQUENCES INCLUDING AUXILIARY SPRAY SYSTEM FAILURE

Sequence	Core Damage Frequency (Per Year)
T1-ONL	4.6E-10
T1-ONKM$_1$	1.2E-9
T1-NQ$_1$L	1.6E-10
T1-NQ$_1$KM$_1$	4.3E-10
T2-NL	1.9E-11
T2-NKM$_1$	5.4E-11
T3-ONL	9.0E-11
T3-ONKM$_1$	2.3E-10
T3-ONH	9.0E-11
T3-ONJI$_1$	2.3E-10
T3-NQ$_2$L	4.2E-12
T3-NQ$_2$KM$_1$	1.1E-11
T3-NQ$_3$H	4.2E-12
T3-NQ$_3$JI$_1$	1.1E-11
T3-NQ$_4$L	2.5E-11
T3-NQ$_4$KM$_1$	6.7E-11
T3-NQ$_4$H	2.5E-11
T3-NQ$_4$JI$_1$	6.7E-11
T4-NL	3.7E-12
T4-NKM$_1$	1.0E-11
T4-NH	3.7E-12
T4-NJI$_1$	1.0E-11

TABLE 7.2.5-2 [1]

CHANGE IN CORE DAMAGE FREQUENCY (λ CD) DUE TO ADDED DEPRESSURIZATION CAPABILITY OF PORVs

Event Tree Description	λ CD (per yr.) Aux. Spray Accident Scenarios	λ CD (per yr.) with PORVs	$\Delta\lambda$ CD (per yr.)	λCD (per yr.) all other Scenarios
SGTR in One SG	2.3E-9	2.3E-12	2.3E-9	1.0E-5
SGTR in One SG with Coincident LOOP	5.9E-11	4.4E-13	5.9E-11	7.4E-7
SGTR in Two SG	8.5E-10	8.5E-13	8.5E-10	3.7E-6
SGTR in Two SG with Coincident LOOP	2.7E-11	2.1E-13	2.1E-11	2.8E-7

[1] Column one provides the total core damage frequency of all minimal sequences that include failure of the Auxiliary Spray System for each SGTR event tree. Column two is similar to column one except that each core damage frequency includes the additional failure of backup PORV depressurization capability. The change in core damage frequency presented in column three is obtained by subtracting column two from column one. This value can be considered negligible when compared to the core damage frequency contribution from all other SGTR accident sequences. The core damage frequency contribution from all other SGTR accident sequences is provided in column four. (These values are the results of Sections 7.2.1-7.2.4).

- Failure to initiate auxiliary spray flow and failure to initiate blowdown from the affected (or most or least affected) SG. The failure to initiate auxiliary spray flow results in a high primary to secondary pressure differential and therefore a large integrated leak flow. If the blowdown system was unavailable, SG overfill could occur. For SGTR with coincident LOOP the blowdown system is unavailable, therefore, failure to initiate spray flow would result in SG overfill.

The accident sequences presented in Table 7.2.6-1 are assumed to represent the minimal sequences that lead to SG overfill for each of the four SGTR initiating events. The results are presented in terms of the median frequencies and associated error factors. (See Section 5.2.4 for branch descriptions).

Table 7.2.6-2 provides the total SG overfill frequency for each initiating event.

TABLE 7.2.6-1

STEAM GENERATOR OVERFILL SCENARIOS

Sequence	Frequency (Median Value per Year)	Error Factor
T1-P_1	2.5E-6	18
T1-ON	5.1E-6	8
T1-OQ_1	2.2E-4	6
T1-NQ_1	2.0E-6	8
T2-P_1	2.4E-9	41
T2-O	2.1E-6	20
T2-N	2.1E-7	19
T3-P_1	5.0E-7	23
T3-P_3	5.5E-7	27
T3-ON	1.0E-6	11
T3-OQ_2	5.5E-6	11
T3-OQ_3	5.9E-6	11
T3-OQ_4	3.4E-5	9
T3-NQ_2	4.6E-8	14
T3-NQ_3	4.7E-8	14
T3-NQ_4	2.9E-7	13
T4-P_1	4.7E-10	41
T4-P_2	4.3E-10	49
T4-O	4.4E-7	16
T4-N	4.3E-8	23

TABLE 7.2.6-2

FREQUENCY OF STEAM GENERATOR OVERFILL

Event Tree Description	Frequency of SG Overfill (Median value per year)	Error Factor
SGTR in One SG	2.5E-4	7
SGTR in One SG with Coincident LOOP	3.3E-6	15
SGTR in Two SG	7.7E-5	5
SGTR in Two SG with Coincident LOOP	6.2E-7	12

7.3 PORV LOCA SEQUENCE ANALYSIS

The core damage scenarios resulting from PORV LOCA were selected from the systemic event tree sequences provided in Figures 5.3.4.1-1, 5.3.4.2-1, and 5.3.4.3-1. Only the minimal core damage scenarios were selected to calculate the core damage frequency for each of the three types of PORV LOCA. The accident sequences associated with the different types of PORV LOCA are discussed in Sections 7.3.1, 7.3.2, and 7.3.3.

7.3.1 PORV LOCA Following Loss of Secondary Heat Sink Core Damage Scenarios

Two minimal core damage scenarios for PORV LOCA following loss of secondary heat sink were identified in Figure 5.3.4.1-1. These scenarios are presented in Table 7.3.1-1 along with the median frequencies and the associated error factors. Also listed in the table is the total core damage frequency which represents a statistical combination (using the SAMPLE code described in Section 2.2.3.5) of the individual core damage scenario frequencies for this type of PORV LOCA. These scenario frequencies are then statistically combined with the other types of PORV LOCA scenario frequencies to represent the total core damage frequency for the three types of PORV LOCA considered. The magnitude and impact of the core damage frequency contribution due to PORV LOCA are discussed in Section 9.0. For this type of PORV LOCA, no scenario was eliminated by the cutoff frequency of 1.0E-15 per year. The core damage scenarios are described as follows:

Scenario 1. P1-R This scenario refers to a PORV LOCA followingloss of secondary heat sink and the inability to achieve high pressure recirculation. Following the initiation of PORV LOCA the HPSI System provides makeup to the RCS until the RWT inventory is depleted. Normal operating procedures require that the HPSI System be realigned to

TABLE 7.3.1-1

PORV LOCA FOLLOWING LOSS OF SECONDARY
HEAT SINK CORE DAMAGE SEQUENCES

Path	Description	Frequency (Median Value per Year)	Error Factor
1. P1-R	• Initiating Event • Failure to Achieve High Pressure Recirculation	3.88E-11	82
2. P1-A	• Initiating Event • Failure to Deliver Sufficient HPSI Flow	2.82E-10	43
	Total Core Damage Frequency:	3.9E-10	64

the containment sump when the RWT inventory is depleted so that high pressure recirculation through the reactor core can be achieved. The failure to achieve high pressure recirculation leads to increased core temperature, core uncovery, and subsequent core damage.

Scenario 2. P1-A This scenario refers to a PORV LOCA following loss of secondary heat sink and failure to deliver sufficient high pressure injection. Failure to deliver sufficient high pressure injection flow following the initiation of a LOCA results in continued loss of RCS inventory which leads to core uncovery and subsequent core damage.

7.3.2 PORV LOCA Following SGTR Core Damage Scenarios

Three minimal core damage scenarios for PORV LOCA following SGTR were identified in Figure 5.3.4.2-1. These scenarios are presented in Table 7.3.2-1 along with the median frequencies and the associated error factors. Also listed in the table is the total core damage frequency which represents a statistical combination (using the SAMPLE code described in Section 2.2.3.5) of the individual core damage scenario frequencies for this type of PORV LOCA. These scenario frequencies are then statistically combined with the other types of PORV LOCA scenario frequencies to represent the total core damage frequency for the three types of PORV LOCA considered. The magnitude and impact of the core damage frequency contribution due to PORV LOCA are discussed in Section 9.0. One scenario was eliminated by the cutoff frequency of 1.0E-15 per year. The eliminated scenario frequency is 7.9E-18 per year. The core damage scenarios are described as follows:

Scenario 1. P2-R This scenario refers to a PORV LOCA following SGTR and the inability to achieve high pressure recirculation. Following the initiation of PORV LOCA the HPSI System provides makeup to the RCS

TABLE 7.3.2-1

PORV LOCA FOLLOWING SGTR
CORE DAMAGE SEQUENCES

Path	Description	Frequency (Median Value per Year)	Error Factor
1. P2-R	• Initiating Event • Failure to Achieve High Pressure Recirculation	3.33E-9	34
2. P2-Z_1G_2	• Initiating Event • Failure to Deliver 5% MFW to One Steam Generator • Failure to Deliver AFW to One Steam Generator	4.16E-9	24
3. P2-A	• Initiating Event • Failure to Deliver Sufficient HPSI Flow	2.40E-8	12
	Total Core Damage Frequency	4.3E-8	12

until the RWT inventory is depleted. Normal operating procedures require that the HPSI System be realigned to the containment sump when the RWT inventory is depleted so that high pressure recirculation through the reactor core can be achieved. The failure to achieve high pressure recirculation leads to increased core temperature, core uncovery, and subsequent core damage.

Scenario 2. $P2\text{-}Z_1G_2$

This scenario refers to a PORV LOCA following SGTR, failure to deliver 5% MFW to the intact steam generator, and failure to deliver AFW to the intact steam generator. For this type of PORV LOCA the intact steam generator becomes unavailable due to loss of both 5% MFW and AFW flow. This condition will inhibit the rapid RCS cooldown which will cause a large pressure differential between the RCS and the affected steam generator that supports continued leak flow. Eventually, the continued leak flow will cause the core to become uncovered and subsequently core damage will occur.

Scenario 3. P2-A

This scenario refers to a PORV LOCA following SGTR and failure to deliver sufficient high pressure injection. Failure to deliver sufficient high pressure injection flow following the initation of a LOCA results in continued loss of RCS inventory which leads to core uncovery and subsequent core damage.

7.3.3 Spurious PORV LOCA Core Damage Scenarios

Three minimal core damage scenarios for Spurious PORV LOCA were identified in Figure 5.3.4.3-1. These scenarios are presented in Table 7.3.3-1 along with the median frequencies and the associated error factors. Also listed in the table is the total core damage frequency which represents a statistical combination (using the SAMPLE code described in Section 2.2.3.5) of the individual core damage scenario frequencies for this type of PORV LOCA. These scenario frequencies are then statistically combined with the other types of PORV LOCA scenario frequencies to represent the total core damage frequency for the three types of PORV LOCA considered. The magnitude and impact of the core damage frequency contribution due to PORV LOCA are discussed in Section 9.0. The total frequency of scenarios eliminated by the cutoff frequency of 1.0E-15 per year is 2.0E-15 per year. The core damage scenarios are described as follows:

Scenario 1. P3-R

This scenario refers to a spurious PORV LOCA and the inability to achieve high pressure recirculation. Following the initiation of PORV LOCA the HPSI System provides makeup to the RCS until the RWT inventory is depleted. Normal operating procedures require that the HPSI System be realigned to the containment sump when the RWT inventory is depleted so that high pressure recirculation through the reactor core can be achieved. The failure to achieve high pressure recirculation leads to increased core temperature, core uncovery, and subsequent core damage.

Scenario 2. P3-Z_2G_1

This scenario refers to a Spurious PORV LOCA, failure to deliver 5% MFW, and failure to deliver AFW. For this type of PORV LOCA, the steam generators become unavailable due to the loss of both 5% MFW and AFW flow. This condition will

TABLE 7.3.3-1

SPURIOUS PORV LOCA CORE
DAMAGE SEQUENCES

Path	Description	Frequency (Median Value per Year)	Error Factor
1. P3-R	• Initiating Event • Failure to Achieve High Pressure Recirculation	7.86E-10	60
2. P3-Z_2G_1	• Initiating Event • Failure to Deliver 5% MFW • Failure to Deliver AFW	4.36E-11	51
3. P3-A	• Initiating Event • Failure to Deliver Sufficient HPSI Flow	5.97E-9	25
	Total Core Damage Frequency	9.0E-9	20

cause the RCS temperature and pressure to increase thus inhibiting makeup. Eventually, the core will become uncovered and subsequently core damage will occur.

Scenario 3. P3-A

This scenario refers to Spurious PORV LOCA and failure to deliver sufficient high pressure injection. Failure to deliver sufficient high pressure injection flow following the initiation of a LOCA results in continued loss of RCS inventory which leads to core uncovery and subsequently core damage.

7.4 OTHER CORE MELT SEQUENCES

The NRC questions focused on those particular initiating events which the staff considered to be most relevant with respect to the PORV issue. The purpose of this section is to survey other potential core damage scenarios and to identify those which could be mitigated via improved methods of depressurization or decay heat removal.

For the purpose of this survey, the results of the draft Calvert Cliffs IREP (29) are referenced. The survey method used was to identify those IREP sequences which contributed more than 1% of the total core damage probability, and to determine which of those sequences have not been covered in the models presented in Section 5.0, and of these identify the ones that could be prevented or mitigated through improved means of depressurization or decay heat removal.

Table 7.4-1 contains a list of the dominant sequences from Reference (29).

Table 7.4-2 defines the terms used in Table 7.4-1.

Table 7.4-3 categorizes each of the dominant sequences as covered in Section 5, not covered in Section 5 and not PORV related, or not covered by Section 5 and PORV related. As shown in the table, no sequences were identified as PORV related which have not been covered in the event trees of Section 5.0.

TABLE 7.4-1[1]

SUMMARY OF DOMINANT SEQUENCES (No Feed and Bleed)

Sequence Number	Event Tree	Sequence Description Shorthand	Fraction Core Melt(w/recovery)	Status
S3	Large LOCA	AHH'		
S13	Large LOCA	AD'	0.3%	Less Dominant
S17	Large LOCA	AD	2.5%	Dominant
S36	Small LOCA	S_1H		
S39	Small LOCA	$S_1D"$		
S43	Small LOCA	S_1K		
S48'	Small-small LOCA	S'_2H	2.4%	Less Dominant
S67'	Small-small LOCA	S'_2K		
S91-1'	Loss of Off-site Power	$T_1'L$	50%	Dominant
S93-1'	Loss of Off-site Power	$T_1'LCC'$	2%	Less Dominant
S91-2'	Loss of Off-site Power	$T_2'L$	45.6%	Dominant

[1] This information was obtained from the draft Calvert Cliffs IREP Study and is not necessarily applicable to SONGS.

TABLE 7.4-2

KEY TO ACCIDENT SEQUENCE SYMBOLS

EVENT TREE SYMBOL	FRONT LINE SYSTEM FAILURE
C	Containment Air Recirculation and Cooling System (CARCS)
C'	Containment Spray System - Injection Phase (CSSI)
D	Safety Injection Tanks (SIT)
D'	Low Pressure Safety Injection - Injection Phase (LPSI)
D"	High Pressure Safety Injection - Injection Phase (HPSI)
F	Containment Spray System - Recirculation Phase (CSSR)
H	High Pressure Safety Injection - Recirculation Phase (HPSR)
H'	Low Pressure Safety Injection - Recirculation Phase (LPSR)
K	Reactor Protection System (RPS)
L	Secondary Steam Relief and Auxiliary Feedwater System (SSR & AFWS)
M	Secondary Steam Relief and Power Conversion System (SSR & PCS)
O	Primary Safety Relief Valve Demand (SRV Demand)
P	Primary Safety Relief Valve Open (SRV Open)
P'	Power Operated Relief Valves Blocked Open (PORVs Blocked Open)
Q	Primary Safety Relief Valve Reclose (SRV Reclose)
U	Chemical, Volume, and Control System - Emergency Boration (CVCS)

INITIATION

A	Large Break LOCA
S_1	Small LOCA
S_2	Small-Small LOCA
T_1	Loss of Offsite Power
T_2	Loss of Power Conversion System
T_3	Transient requiring reactor coolant system pressure relief
T_4	All other transients not included in T_1, T_2, or T_3

TABLE 7.4-3

DOMINANT SEQUENCE CATEGORIES

SEQUENCE		DISPOSITION		
Number	Description	Covered in Section 5.0	Not Covered in Section 5.0	
			Irrelevant to PORV Issue	PORVs could Prevent or Mitigate
S3	AHH'		X	
S13	AD'		X	
S17	AD		X	
S36	S_1H		X	
S39	$S_1D"$		X	
S43	S_1K		X	
S48'	S'_2H	X (PORV incr. freq.)		
S67'	S'_2K		X	
S91-1'	$T_1'L$	X		
S93-1'	$T_1'LCC'$	X		
S91-2'	$T_2'L$	X		

8.0 STEAM GENERATOR TUBE STRENGTH MODEL

The empirical tube strength model and simulator described in Appendix B were used to analyze the consequences of a group of events which provide excess primary/secondary pressure differences. The events, frequencies, and primary/secondary pressure differences are given in Table 8.0-1 (10,15).

The simulation consisted of many trials for each of the listed events. With the exception of the Steam Line Break, no event resulted in more than 2 ruptured tubes, in one steam generator, for any trial. The event-specific tube failure probabilities (0, 1, 2, etc.) obtained from each simulation were weighted by the event frequencies to obtain the results shown in Figure 8.0-1 for the affected steam generator (the steam generator exposed to the higher primary/secondary pressure difference).

Examination of Figure 8.0-1 shows an increase in frequency between 3 and 4 ruptured tubes. This is a consequence of the Steam Line Break for which the most probable number of tube failures is four. It should be noted, however, that no tube failures were observed for the less affected steam generator.

A second simulation was performed to evaluate the probability of concurrent ruptures in both steam generators. The Steam Line Break event was excluded from this study because of the low level of insult to the unaffected steam generator. The simulation was performed with a 1420 PSID insult to both steam generators. Simultaneous tube ruptures in both steam generators (i.e. one tube rupture in each SG) were observed in only 9 of the 10^4 trials ($P(E_1) = 9 \times 10^{-4}$). The cumulative frequency of events with similar symmetric insult is approximately 1.56/yr. yielding a frequency of tube ruptures in both steam generators of 1.4E-3/year. In all the observed cases, no more than 1 tube rupture was encountered in any steam generator.

TABLE 8.0-1

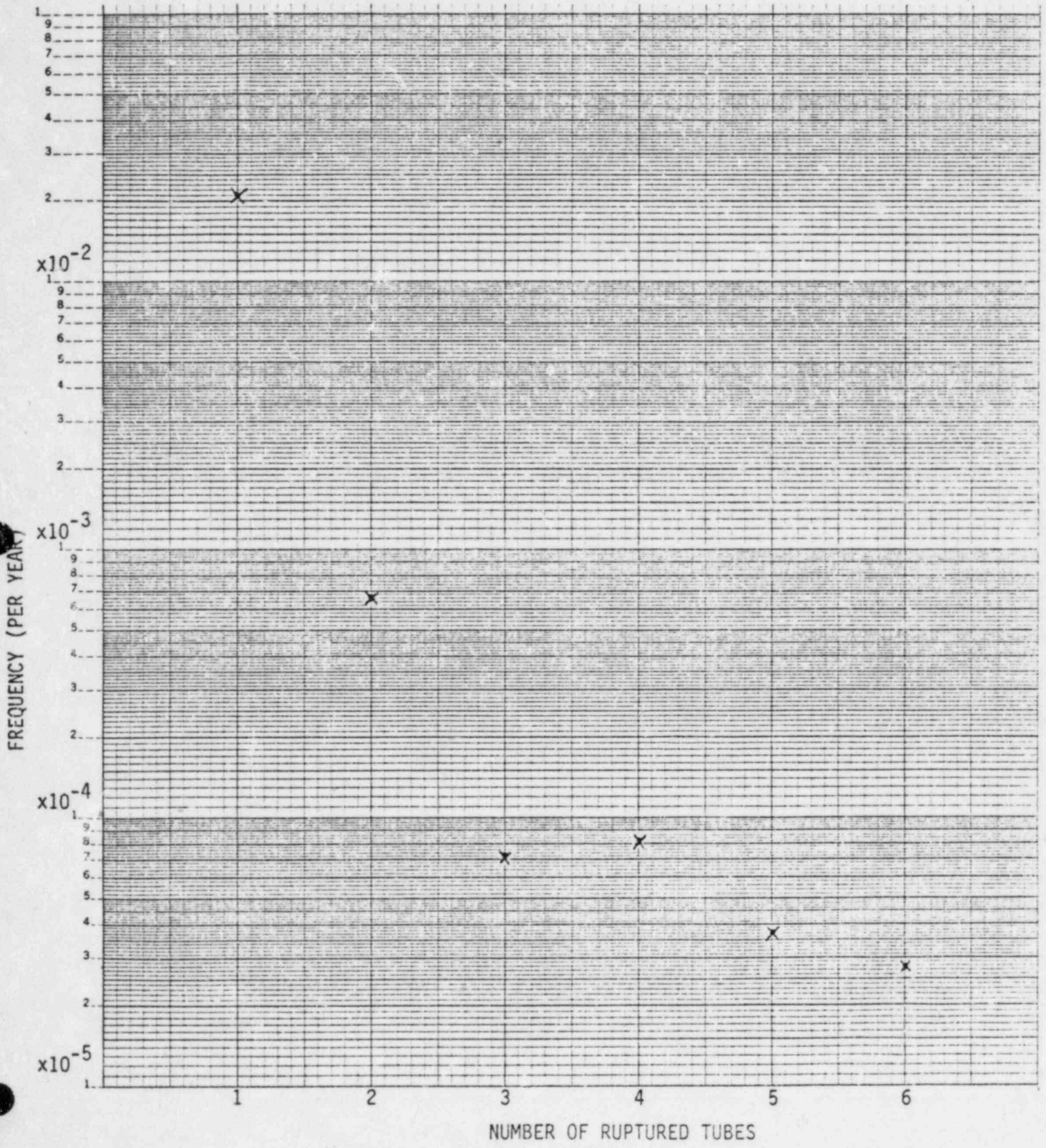
EVENTS CONSIDERED IN TUBE STRENGTH MODEL

Event	Frequency (per year)	SG-1 P (PSID)	SG-2 P (PSID)
Turbine Trip	1.0	1190	1190
Loss of Offsite Power	4.0E-2	1200	1200
Loss of Condenser Vacuum	2.0E-1	1085	1085
Loss of MFW	1.0E-1	1320	1320
Increased MFW	7.2E-1	1320	1320
Steam Line Break	3.4E-4 [1]	2060	1090
Open TCVs	1.7E-2	1400	1400
Loss of One RCP	4.3E-1	1158	1158
CE Withdrawal	2.0E-2	1420	1420
CEA Drop	7.0E-1	1420	1420
Let-Down Line Break	1.0E-3	1340	1340

[1] Obtained from Reference (2)

FIGURE 8.0-1

FREQUENCY OF TUBE RUPTURES FOR
AFFECTED STEAM GENERATOR



An alternative computation of frequencies of tube ruptures in multiple steam generators was performed using tube rupture frequencies for individual steam generators. In the second simulation a single tube rupture in one steam generator was observed in 302 of the trials ($P(E_2)$=0.0302) and double tube ruptures in one steam generator were found in 12 of the trials ($P(E_3)$=0.0012) combining event probabilities gives:

$$P(E_1) = P(E_2 \cap E_2) = P(E_2)^2 = 9.1E\text{-}4$$
$$P(E_4) = P(E_2 \cap E_3) = P(E_2) \cdot P(E_3) = 3.6E\text{-}5$$
$$P(E_5) = P(E_3 \cap E_3) = P(E_3)^2 = 1.4E\text{-}6$$

where: $P(E_n)$ = probability of N^{th} event

E_1 = occurrence of a tube rupture in each steam generator

E_2 = occurrence of one tube rupture in one steam generator

E_3 = occurrence of two tube ruptures in one steam generator

E_4 = occurrence of two tube ruptures in one steam generator and simultaneous occurrence of one tube rupture in the remaining steam generator

E_5 = simultaneous occurrence of two tube ruptures in each steam generator

The value computed in this manner for $P(E_1)$ agrees well with the results of the second simulation. Confirmation of the remaining probabilities ($P(E_4)$, $P(E_5)$) would require an extensive modification to the second simulation procedure.

The following conclusions may be made from the present work. The frequency of a multiple steam generator tube rupture with more than one tube rupture in either steam generator is therefore less than 1.0E-4/year. The frequency of an event involving multiple ruptures in both steam generators is much less than 1.0E-4/year. When the probability of loss of offsite power is included, the frequency of a multiple SGTR in both SGs with coincident LOOP is much less than 1.0E-7/year.

9.0 RESULTS

9.1 CORE DAMAGE FREQUENCY CONTRIBUTIONS

The core damage frequencies determined in Section 7.0 are further combined and summarized in Table 9.1-1. The 90% confidence distributions of the core damage frequencies are presented in terms of the median values and associated error factors. The error factors are defined by the ratio of the 95th percentile to the 50th percentile. The frequency of the accident sequences involving SGTR have been statistically combined (using the SAMPLE code described in Section 2.2.3.5) into two categories: 1) scenarios resulting from SGTR in one or two steam generators assuming offsite power is available and 2) scenarios resulting from SGTR in one or two steam generators with a coincident loss of offsite power. As noted in Section 2.2.1.2, the purpose for evaluating SGTR with the unavailability of offsite power incorporated into the initiating event frequency was to minimize the size of the extensive SGTR event trees. The LOHS and PORV LOCA event trees employed the fault tree linking approach (see Section 2.2.1.2) to model the availability of offsite power.

It should be noted that there is substantial conservatism in the calculated base values of core damage due to SGTR. The emphasis of the analyses was to estimate the change in core damage frequency rather than develop an accurate estimate of the absolute values. The following major assumptions were made for the SGTR analyses which may have resulted in an over estimate of the base value of core damage frequency of as much as an order of magnitude.

Assumption 1. HPSI is needed to prevent core uncovery and subsequent core damage following SGTR. This assumption is conservative in that, if faced with a SGTR with no HPSI available, the operator could initiate an aggressive cooldown and thereby minimize leakage to the secondary system and bring the primary system pressure down to where the safety injection tanks could prevent or mitigate

TABLE 9.1-1

CORE DAMAGE FREQUENCY CONTRIBUTIONS DUE TO LOHS, SGTR AND PORV LOCA

INITIATING EVENTS	LOHS	SGTR WITH OFFSITE POWER AVAILABLE	SGTR WITH COINCIDENT LOOP	PORV LOCA
Case One: Median λ_{CD} (per year) without PORVs, with ASHR* capability	3.1E-7	1.5E-5	1.5E-6	N/A
Error Factor	21	5	11	
Case Two: Median λ_{CD} (per year) with manually actuated PORVs, without ASHR* capability	1.6E-7	1.5E-5	1.5E-6	7.2E-8
Error Factor	28	5	11	10
Case Three: Median λ_{CD} (per year) with automatically actuated PORVs, without ASHR* capability	1.6E-7	1.5E-5	1.5E-6	7.9E-7
Error Factor	28	5	11	9
Case Four: Median λ_{CD} (per year) with no PORVs or ASHR* capability	2.1E-6	1.5E-5	1.5E-6	N/A
Error Factor	19	5	11	

*Alternate Secondary Heat Removal

core uncovery and prevent core damage. Additional transient analysis would be required to verify the effectiveness of this action. Current emergency procedures do not suggest this action.

Assumption 2.

A SGTR followed by a stuck open secondary valve is assumed to lead to core damage. This assumption is conservative in that no credit was taken for the operator recognizing early in the transient that there is a danger of running out of borated water in the long term. This event is essentially an outside containment LOCA. Therefore, when the Refueling Water Tanks (RWTs) are drained and the Recirculation Actuation Signal (RAS) is generated, the Safety Injection System will switch-over to a dry (or insufficiently filled) containment sump. This switch-over would occur at approximately 15 to 30 hours after the SGTR. The leak will persist until the primary coolant system is cooled to 212°F. For SGTR events that have occurred (e.g. Ginna) it has taken approximately 24 hours to get to shutdown cooling entry conditions. It could take an additional 10 to 20 hours to cool to 212°F.

Emergency procedures provide no guidance on the need to make-do with the limited supply of borated water in the RWT, or to supplement it. Therefore, no credit was taken for other sources of water, including borated water in the spent fuel pool. No credit was taken for early recognition of the problem followed by an aggressive cooldown. Also, no penalty was assigned to the PORVs for their

potential for aggravating the problem, i.e., use of the PORVs (and possible subsequent containment spray) would tend to drain the RWT sooner and lead to an RAS and a switch-over to an inadequately filled containment sump.

The frequency of the accident sequences involving PORV LOCA were also statistically combined into a single distribution representing the total core damage frequency of PORV LOCA. The result provides an estimate of the magnitude of the core damage frequency contribution due to PORV LOCA.

The core damage frequencies were evaluated for the currently planned plant design which includes alternate secondary heat removal capability but has no PORVs (presented as case one) and the alternate plant design which does not credit alternate secondary heat removal capability but includes PORV depressurization and decay heat removal capability (presented as case two). In this design, the PORVs are manually opened and the plant is assumed to operate with the PORV block valves closed which minimizes the risk associated with PORV LOCA. It should be noted that the use of PORVs as a backup to the safety related Auxiliary Spray System was determined to have an insignificant impact on the total core damage frequency derived for each of the SGTR initiating events as discussed in Sections 5.2.4 and 7.2.5. Therefore, the decrease in core damage frequency due to the added depressurization capability of PORVs is considered to be negligible.

If automatic actuation of the PORVs were to be assumed and if the plant were to operate with the block valves open, the core damage frequencies for case two (with PORVs) could be re-evaluated assuming an automatic PORV design. The results are presented as case three (automatic PORVs) in Table 9.1-1.

The event tree model for the loss of secondary heat sink evaluation which included alternate secondary heat removal capability was re-evaluated to determine a core damage frequency due to loss of heat sink assuming no alternate secondary heat removal capability and no PORV depressurization and decay heat removal capability. The results are presented as case four of Table 9.1-1.

9.2 CHANGE IN CORE DAMAGE FREQUENCY DUE TO IMPROVED DECAY HEAT REMOVAL CAPABILITY

9.2.1 Change in Core Damage Frequency due to Added Alternate Secondary Heat Removal Capability

As shown for case four in Table 9.1-1, core damage frequencies were determined for the plant configuration prior to the SCE agreement to provide ADHR capability via the condensate pumps and associated procedures. Core damage frequencies were also calculated for the currently planned plant configuration which includes ADHR capability via the condensate pumps. The results are presented as case one in Table 9.1-1. In order to determine the reduction in total core damage frequency associated with utilizing alternate secondary heat removal capability, the LOHS core damage frequency which included alternate secondary heat removal capability (case one) was statistically subtracted from the LOHS core damage frequency presented as case four (no alternate secondary heat removal capability and no PORVs). The calculation was performed with the SAMPLE code at the sequence level to account for dependencies between the sequences using branch median failure probabilities and associated error factors as input. The result indicates a net decrease in core damage frequency due to alternate secondary heat removal capability of 2.0E-6 per year (median value) with an associated error factor of 17.

9.2.2 Change in Core Damage Frequency due to Installation of PORVs

As shown in cases one and two of Table 9.1-1, core damage frequencies were determined for the proposed plant configuration which includes alternate secondary heat removal capability but has no PORVs (case one) and the alternate plant design which excludes alternate secondary heat removal capability but includes PORV depressurization and decay heat removal capability (case two). In this design, the PORVs are manually opened and the plant is assumed to operate with the PORV block valves closed.

The overall change in core damage frequency (net gain or loss in safety) due to the installation of PORVs was determined by examining only those events which were considered to significantly contribute to an increase or decrease in the total core damage frequency, i.e. core damage frequency due to LOHS events and PORV LOCA is impacted by the presence of PORVs while the change in SGTR core damage frequencies does not contribute appreciably to a net gain or loss in safety.

The calculation was performed with the SAMPLE code at the sequence level to account for dependencies between the sequences using branch median failure probabilities and associated error factors as input. For Case Two in Table 9.1-1, the core damage scenario frequencies which contribute to the LOHS (with manually actuated PORVs) core damage frequency and the PORV LOCA core damage frequency were statistically subtracted from the scenario frequency which comprises the LOHS without PORVs core damage frequency (Case One). In equation form:

Change =

LOHS without PORVs - [LOHS with PORVs + PORV LOCA (manually actuated)]

or

$$(LF\text{-}G_1U_1V) - [(LF\text{-}G_1U_2Y) + (LF\text{-}G_1U_2R^*) + (P1\text{-}R) + (P1\text{-}A) + (P2\text{-}R) + (P2\text{-}Z_1G_2) + (P2\text{-}A) + (P3\text{-}R) + (P3\text{-}Z_2G_1) + (P3\text{-}A)]$$

* This branch median failure probability is conditional on loss of MFW and loss of AFW and therefore is not equal to the "R" appearing in the PORV LOCA sequences.

The quantitative solution to the above equation (see Section 5.0 for branch definitions) is presented in Table 9.2.2-1 in terms of a median value and 95% and 5% confidence limits. The results indicate a negligible decrease in core damage frequency due to PORVs (less than 1.0E-8 per year if PORVs were added).

Recalculating the above equation, assuming an automatically actuated PORV design (where the plant operates with the block valves open), i.e.:
Change =
LOHS without PORVs - [LOHS with PORVS + PORV LOCA (automatically actuated)]

the resulting negative median value would indicate a net increase in core damage frequency due to PORVs of 6.1E-7 per year. The quantitative solution is presented in Table 9.2.2-1.

It should be noted that the above values are very small compared to the proposed NRC safety guideline of 10^{-4} core melts/year (37).

TABLE 9.2.2-1

CHANGE IN TOTAL CORE DAMAGE FREQUENCY DUE TO PORVs[1]

	Manually Actuated PORVs ($\Delta\lambda$CD per year)	Automatically Actuated PORVs ($\Delta\lambda$CD per year)
Median	negligible[4]	-6.1E-7
95% Confidence Limit[2]	4.3E-6	3.2E-6
5% Confidence Limit[3]	-1.1E-6	-6.4E-6

1 A positive value indicates a net decrease in total core damage frequency while a negative value indicates a net increase in total core damage frequency.

2 Based on data uncertainty the reduction in core damage risk due to PORVs is less than the 95% Confidence Limit, with 95% probability.

3 Based on data uncertainty the increase in core damage risk due to PORVs is less than the 5% Confidence Limit, with 95% probability.

4 The actual change is less than 1.0E-8 per year

10.0 REFERENCES

1. NRC Letter, R. L. Tedesco to A. E. Scherer, dated March 26, 1982, Subject: Depressurization and Decay Heat Removal Capability of the CESSAR Design.

2. Zion Probabilistic Safety Study, Commonwealth Edison

3. ACRS Letter, J. Carlson Mark to Nunzio J. Palladino, dated December 15, 1981, Subject: ACRS Report on Final Design Approval for Combustion Engineering, Inc. Standard Nuclear Steam Supply System.

4. SCE Letter, K. P. Baskin to Frank Maraglia, Branch Chief, dated April 30, 1982.

5. CE Letter, A. E. Scherer to D. G. Eisenhut, dated May 26, 1982, Subject: Rapid Depressurization and Decay Heat Removal Capability.

6. PRA Procedures Guide, NUREG/CR-2300, January 1983.

7. San Onofre Nuclear Generating Station (SONGS) Units 2 and 3 Final Safety Analysis Report.

8. San Onofre Nuclear Generating Station Units 2 and 3 Emergency Procedures (various event types).

9. C-E Emergency Procedure Guidelines, CEN-152, Revision 1, November, 1982.

10. Responses of C-E NSSSs to Transients and Accidents, CEN-128, April, 1980.

11. San Onofre Nuclear Generating Station Units 2 and 3 Operating Instructions (various systems).

12. San Onofre Nuclear Generating Station Units 2 and 3 One-Line Diagrams (various electrical buses).

13. San Onofre Nuclear Generating Station Units 2 and 3 Control Panel Layout Drawings and Instrumentation Lists.

14. Swain, A. D. and Guttman, H. E., Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Operations, NUREG/CR-1278, October, 1980.

15. Generic Data Base for Data and Models Chapter of the National Reliability Evaluation Program Guide, EGG-EA-5887, June, 1982.

16. Reactor Safety Study, An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants, WASH 1400/NUREG-75/014, October, 1975.

17. IEEE Guide to the Collection and Presentation of Electrical, Electronic, and Sensing Component Reliability for Nuclear Power Generating Stations, IEEE-STD500-1977.

18. Design and Application of Combustion Engineering's Reliability Data System for Nuclear Steam Supply Systems, TIS-6736, April, 1981.

19. Combustion Engineering Interim Data Base, "Failure Rates for Nuclear Plant Components", 207010, February, 1976.

20. PWR Power Plant Pump Reliability Data, EPRI-NP-2592, September, 1982.

21. Loss of Offsite Power at Nuclear Power Plants: Data and Analysis, EPRI-NP-2301, March, 1982.

22. General Evaluation of Feedwater Transients and Small Break Loss of Coolant, NUREG-0635, January, 1980.

23. A Probabilistic Safety Analysis of DC Power Supply Requirements for Nuclear Power Plants, NUREG-0666, April, 1981.

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

25. Analysis of Steam Generator Tube Rupture Events at Oconee and Ginna, INPO 82-030, November, 1982.

26. Bourne, A. J. and Green, A. E., Reliability Technology, 1972.

27. Nuclear Power Experience: Reactor Coolant System, Relief and Safety Valves, Vol. PWR-2.

28. Depressurization and Decay Heat Removal, CEN-239 Main Report.

29. Interim Reliability Evaluation Program: Calvert Cliffs Unit 1, SAI-001-82-BE, January 15, 1982.

30. SONGS Units 2 and 3 Training System Description, "Steam Generator Blowdown Processing System".

31. Kolb, G. J., S. W. Hatch, P. Cybulskis, and R. O. Wooton, Reactor Safety Study Methodology Applications Program: Oconee #3 PWR Power Plant, NUREG/CR-1659, January 1981.

32. W. R. Corcoran, et. al "The Operator's Role and Safety Functions", Presented at Workshop on Licensing and Technical Issues - Post TMI, March 1980, TIS-6555A.

33. ATWS Analysis, Analysis of Anticipated Transients Without Scram in Combustion Engineering NSSSs, CENPD-158, Revision 1, May, 1976.

34. ATWS Early Verification, Response to NRC Letter on February 15, 1979 for Combustion Engineering NSSSs, CENPD-263, November 1979.

35. NRC, "Data Summaries of Licensee Event Reports for Diesel Generators at U.S. Commercial Nuclear Power Plants", NUREG/CR-1362, March 1980.

36. Review of Small Break Transients in Combustion Engineering Nuclear Steam Supply System, CEN-114-P, Amendment 1-P, July, 1979.

37. Safety Goals for Nuclear Power Plants: A Discussion Paper, NUREG-0880 (Draft), February, 1982.

38. C-E Standard Safety Analysis Report

APPENDIX A

NRC STAFF REQUEST FOR ADDITIONAL INFORMATION

CAPABILITIES FOR THE DEPRESSURIZATION AND DECAY
HEAT REMOVAL WITHOUT PORVs

REQUEST FOR ADDITIONAL INFORMATION

1. CE has not demonstrated that the auxiliary spray system can satisfactorily depressurize the reactor coolant system during events where depressurization must be accomplished and the normal spray is unavailable. In addition, for some scenarios, containment isolation results in a loss of preheating to the auxiliary spray, which can result in a thermal transient to the spray nozzle piping and pressurizer spray. Please address the capability of the spray system to accommodate such thermal transients.

   Please address the following aspects of auxiliary spray system:

   a. A full description of the system.
   b. The means to control the depressurization rate.
   c. The maximum depressurization rate available.
   d. The consequences of a failed open spray valve.
   e. An evaluation of the ability to depressurize using the technique in the event of void formation in the vessel upper head. In such an eventuality, continued auxiliary spray operation could collapse the pressurizer steam bubble and result in a rapid insurge producing water solid pressurizer. It is not readily apparent that the auxiliary spray would be effective in such a situation.
   f. The sources of reactor coolant grade borated water for auxiliary spray.
   g. The time available for manual loading of the charging pump onto the emergency diesel generator.
   h. The stresses induced in the pressurizer and nozzle must be shown to be acceptable, considering the worst combination of flows, temperatures and pressures.

2. In general, it is desirable to limit the number of challenges to the reactor protection system to minimize the probability of ATWS. Moreover, it is desirable to minimize the number of reactor trips during the lifetime of the plant for the following reasons: First, a ramp down in the reactor power will reduce the likelihood of a turbine trip. A turbine trip has the potential to cause a loss of condenser system and lift the secondary safety valves, increasing releases to the environment. Second, a controlled power reduction will increase the availability of the reactor coolant pumps. Third, a crud burst is less likely during a controlled reactor shutdown reducing the possibility of increasing coolant activity levels. Based on these considerations, as well as the lessons learned from the TMI accident, how is the overall plant safety effected by the absence of PORVs.

3. Even though the Commission has not approved a final ATWS rule, the ability to limit RCS pressure rise in an ATWS event is being contemplated for most LWR designs. Address the advantages and disadvantages of PORVs from the ATWS standpoint.

4. A PORV or other direct depressurization methods may be a viable technique for mitigating pressurized thermal shock (PTS). Address the exclusion of the PORV from the CESSAR-80 design considering PTS.

5. While the PORV may not be required based on classical safety analyses, there are a number of relatively low probability scenarios in which the ability to directly depressurize the RCS or to initiate primary feed and bleed may be essential for plant safety. For example, should tube ruptures occur in both steam generators to the extent that offsite releases would be excessive if the secondary systems were used, a PORV may be the only means of removing core decay heat without excessive offsite releases or running out of ECCS water. Small break LOCAs could be dealt with by depressurizing the RCS down to the pressure where low head safety injection pumps replenish fluid volume. Show how a variety of multiple failure events, including the above, are satisfactorily handled without the PORV.

6. CE has proposed the use of a low pressure system to supplement the auxiliary feed system. The submittal did not specify which low pressure system, so an evaluation of its capabilities or uses could not be performed. Provide the following specific information:

   a. Describe the system and its use, including water supplies (and their capacity), flow paths, pumps, power supplies to components, control equipment and procedures.

   b. Describe the water chemistry interface requirements for the proposed low pressure system in order to assure its use will not cause unacceptable steam generator integrity degradation or heat transfer capability. (see item 7)

   c. Show that blowdown of the steam generator is a viable technique without adverse core cooling consequences. Show that a concurrent rapid primary system cooldown and potential primary system contract does not result in inadequate core cooling or a return to power.

   d. Show that there are no adverse consequences while feeding a dry steam generator with the low pressure system.

   e. If steam generator pressure rises above the shutoff head of the low pressure pumps intended to be used, describe the method of regaining feed flow without compromising core cooling.

7. Provide information and test data which will demonstrate that steam generator structural integrity and heat transfer capabilities will be maintained under secondary water chemistry conditions that deviate from the recommended CE water chemistry program. Specifically, the following considerations should be addressed for the spectrum of CESSAR plant sites:

   a. Provide data to demonstrate that excessive corrosion of the primary pressure boundary will not occur which could result in primary to secondary leakage complicating the accident condition. (Data pertaining to synthetic cooling water is not considered appropriate, due to the inability to include all potentially corrosive species in their exact chemical conditions).

   b. Provide an assessment of the total corrosive damage anticipated in the steam generators as a consequence of main condensor cooling water injection. Relate the anticipated corrosion damage to the steps which will be necessary to ensure structural integrity prior to a restart.

   c. For your proposed shutdown method, provide calculations and/or test data which will demonstrate that excessive heat transfer surface fouling will not occur and impede the ability of the steam generators to perform their cooldown function.

   d. Describe the steam generator design features which will reduce their susceptibility to excessive corrosion during the proposed injection of main condenser cooling water.

8. For extended loss of main and auxiliary feedwater case where feed/bleed would be a potential backup:

   a. What is the frequency of loss of main feedwater events; break down initiators that affect more than MFW e.g., DC power?

   b. What is the probability of recovering main feedwater. Provide your bases such as availability of procedures and the human error rates?

   c. What is the probability of losing all auxiliary feedwater (given Item a)? Include considerations of recovering auxiliary feedwater as well as common cause failures (including those which could affect main feedwater availability and support system dependencies) and failures that could be hidden from detection via tests?

   d. What is the uncertainty in the estimates provided for a), b) and c)?

e. How long would it take for core melt to initiate?

f. Were core to melt under these conditions, what is the likelihood of steam generator tube rupture(s) due to steam pressure from slumping core?

g. Characterize the consequences from core melt events of e) and f).

9. What is the risk from steam generator(s) tube failures? As a minimum, consider the following:

a. Scenarios leading to core melt from one or more steam generator tubes failing in one steam generator. Include paths which consider failure of relief or safety valve in the faulted steam generator, capability of (or loss thereof) to depressurize the secondary side, the role of the ECCS including inventory and Baron availability.

b. What is the frequency of steam generator tube ruptures in two steam generators? This estimate should include consideration of common cause failures such as design errors, events resulting in extremely high ΔP across the tubes, aging, etc. If tubes were to fail in both steam generators, what is the probability of core melt and generally characterize the consequences.

c. For a) and b) above, discuss the likelihood of steamlines filling with subcooled water and any consequential failures.

d. For a) and b), discuss uncertainties including human error rates (carefully considering the clarity and unambiguity of procedures).

10. What is the core melt frequency from PORV initiated LOCA? Characterize the consequences?

11. What is the net gain (or loss) in safety considering 8, 9 and 10 above if PORVs were to be installed? Are there any additional benefits (or drawbacks) achieved by installing PORVs? Examples of potential benefits are mitigation of ATWS and pressurized thermal shock, and reduced risk associated with depressurized primary system during a core melt.

12. If the results in 11 yield appreciable gain in safety, what could be the cost of installing PORVs?

13. One of the main reasons CE has concluded that PORVs are not needed for emergency decay heat removal is that alternative water sources could be made available to the steam generators for decay heat removal purposes. An inherent assumption in this approach is that steam generator integrity will be maintained throughout the life of the plant. One method of assuring combined steam generator integrity is by inservice inspection and plugging of tubes excessively degraded. Please discuss the following:

a. What is the minimum allowable wall thining that could exist in the steam generator tubes without plugging?

b. What is the probability that ISI will not detect a degraded tube? Provide the margin of error in eddy current measurements at various depths of degradation.

c. Given a steam generator with the maximum allowed tube thinning and degradation, confirm that those tubes will maintain their integrity by demonstrating they have been analyzed and shown to remain intact for all design basis loadings used for the steam generator design including seismic loads.

d. Describe the analytical and experimental justification for establishing a minimum acceptable steam generator tube wall thickness for the CE System 80 steam generators in accordance with guidelines in Regulatory Guide 1.121, "Bases for Plugging Degraded PWR Steam Generator Tubes". The justification should include the analyses to calculate the hydraulically induced loading on the steam generator and the thermal response of its tubes and shell to an assumed LOCA, MSLB and an FWLB.

14. Fretting wear type damage of steam generator tubes in the vicinity of the feedwater inlet has been observed in certain preheat type steam generators of design similar to the CE System 80 steam generators. This damage is attributed to flow induced vibrations originating in the economizer of the steam generator. Provide a description of vibration analyses and model flow testing performed during the design of the CE System 80 steam generators to assure that no damaging flow induced vibrations would occur in these steam generators.

APPENDIX B

PROBABILISTIC TUBE STRENGTH MODEL

I. INTRODUCTION

An empirical tube-strength model has been developed to evaluate steam-generator tube rupture probabilities. The failure mechanism assumed in the model was tube rupture caused by overpressurization. A sequence of transient events resulting in increased primary/secondary pressure differences were included in the analysis. The failure probabilities for individual steam-generator tubes were derived from bursting experiments using undefected and mechanically defected steam-generator tubing.

In order to model the mechanical state of an aging steam generator, a defect inventory distribution was included in the model. The defect distribution was inferred from current steam generator inspection procedures. In practice, a measured defect inventory can be used.

The model uses Monte-Carlo simulation to compute tube rupture probabilities on an event-specific basis for each of two steam generators. For a given event, the probabilities of 1 to 30 tube ruptures are computed. These probabilities are convoluted with the event probabilities to compute an overall frequency distribution (Figure 8.0-1).

At present, the model does not include provisions for non-mechanical degradation of tube performance or loose-part impact induced failure. For the purposes of the PORV risk impact study the question that this model is designed to answer is "What is the expected frequency and character of events involving simultaneous tube ruptures in both steam generators?" Therefore, failure modes involving loose-parts or jet impingement were not considered.

II. PROBABILITY DISTRIBUTIONS FOR TUBE BURST PRESSURE

In a PWR steam generator, tubes are pressurized from the interior by primary coolant. The primary/secondary pressure difference under normal operation can range from 1000-1350 psid. Experimental evidence has suggested that the pressure required to burst steam generator tubes is a random variable and can be described by an appropriate probability density function. Since this model was concerned with computing the probabilities of 1 to 30 tube failures out of a population exceeding 10^4 tubes, an adequate treatment of extremal phenomena was required. For this reason an extreme value distribution was chosen to model the probabilistic behavior of burst pressure.

Trankel (Reference 1) and Kao (Reference 2) have used Type I and Type III (Weibull) extreme value distributions to describe tube bursting phenomena. In the present model, the Weibull distribution, which has been widely applied for the analysis of fatigue data, is used. This distribution has the distinct advantage of possessing a finite lower bound. Since the present model does not analyze the steam generator tube rupture as an initiating event, but as a consequence of an event resulting in an increased primary/secondary pressure difference, the Weibull distribution, with a lower threshold burst pressure, was particularly appropriate.

The cumulative distribution function (CDF) of a Weibull variate is given by:

$$F(X;N,\sigma,\mu) = 1 - \left[\text{EXP} -\left(\frac{X-\mu}{\sigma}\right)^N\right]$$

for $X > \mu$

where X = burst pressure

N, σ - location and scale parameters

μ = lower limit value

$F(X_i)$ = probability of burst pressure $\leq X$

For undefected tubing, the data of Kao (Reference 2) was used. This data set agreed well with later investigations of tube bursting documented in Reference 3. The fit obtained for the data is given by:

$$F(X) = 1 - EXP\left[-\left(\frac{X-1.0}{9.059}\right)^{17.13}\right] \qquad X \geq 1.0 \text{ ksi}$$

Based on this expression the following results were obtained for undefected tubing:

Prob (B.P. [Burst Pressure] $\leq$ 3 KSI) = 5.78×10^{-11}
Prob (B.P. $\leq$ 3.5 KS1) = 2.64×10^{-10}
Prob (B.P. $\leq$ 4. KS1) = 6.0×10^{-8}
Prob (B.P. $\leq$ 7. KS1) = 8.6×10^{-4}
Prob (B.P. $\leq$ 11. KS1) = 0.995

An extensive examination of the effects of various types of mechanical defects on steam generator tube performance was presented in Reference 3. Burst pressure performance was seen to be a complex function of defect geometry and length as well as wall thickness degradation. Because present tube plugging criteria are based primarily on defect depth expresed as a percentage of wall thickness, asymptotic behavior with regard to defect length and geometry was conservatively assumed. Burst pressure then could be expressed as a linear function of percent remaining wall with an intercept at the origin:

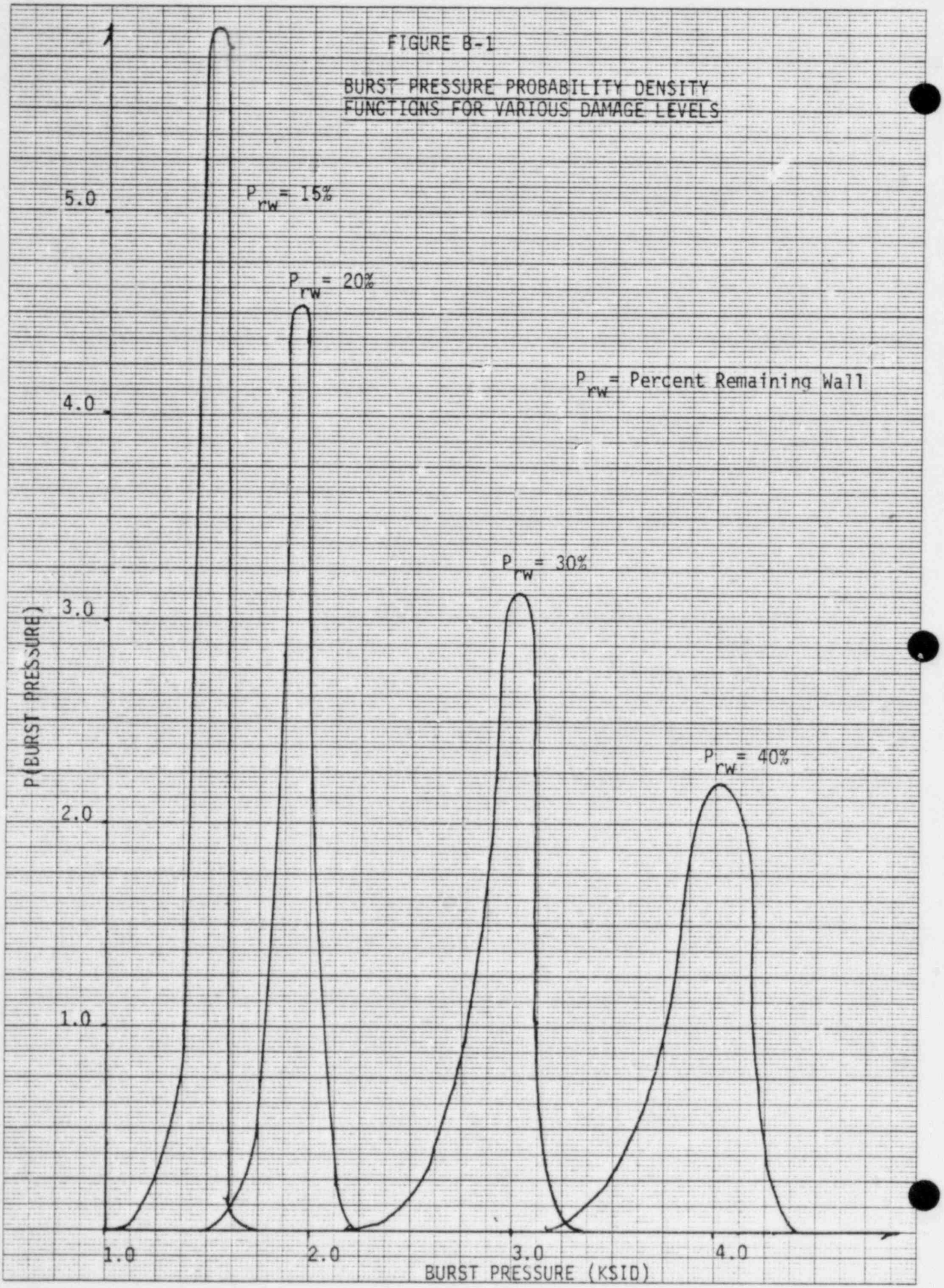
$$BP_d = BP_u \times P_{RW}/100$$

where: BP_d = Burst pressure of defected tubing
BP_u = Burst pressure of undefected tubing
P_{RW} = Percent remaining wall

The data of Reference 2 was adjusted using the above equation to allow the fitting of Weibull distributions for various levels of damage. The probability density functions (PDF) obtained using this procedure are shown in Figure B-1 for various damage levels. These burst pressure probability density functions were incorporated into the tube strength model.

FIGURE B-1

BURST PRESSURE PROBABILITY DENSITY FUNCTIONS FOR VARIOUS DAMAGE LEVELS



III. DEFECT INVENTORY

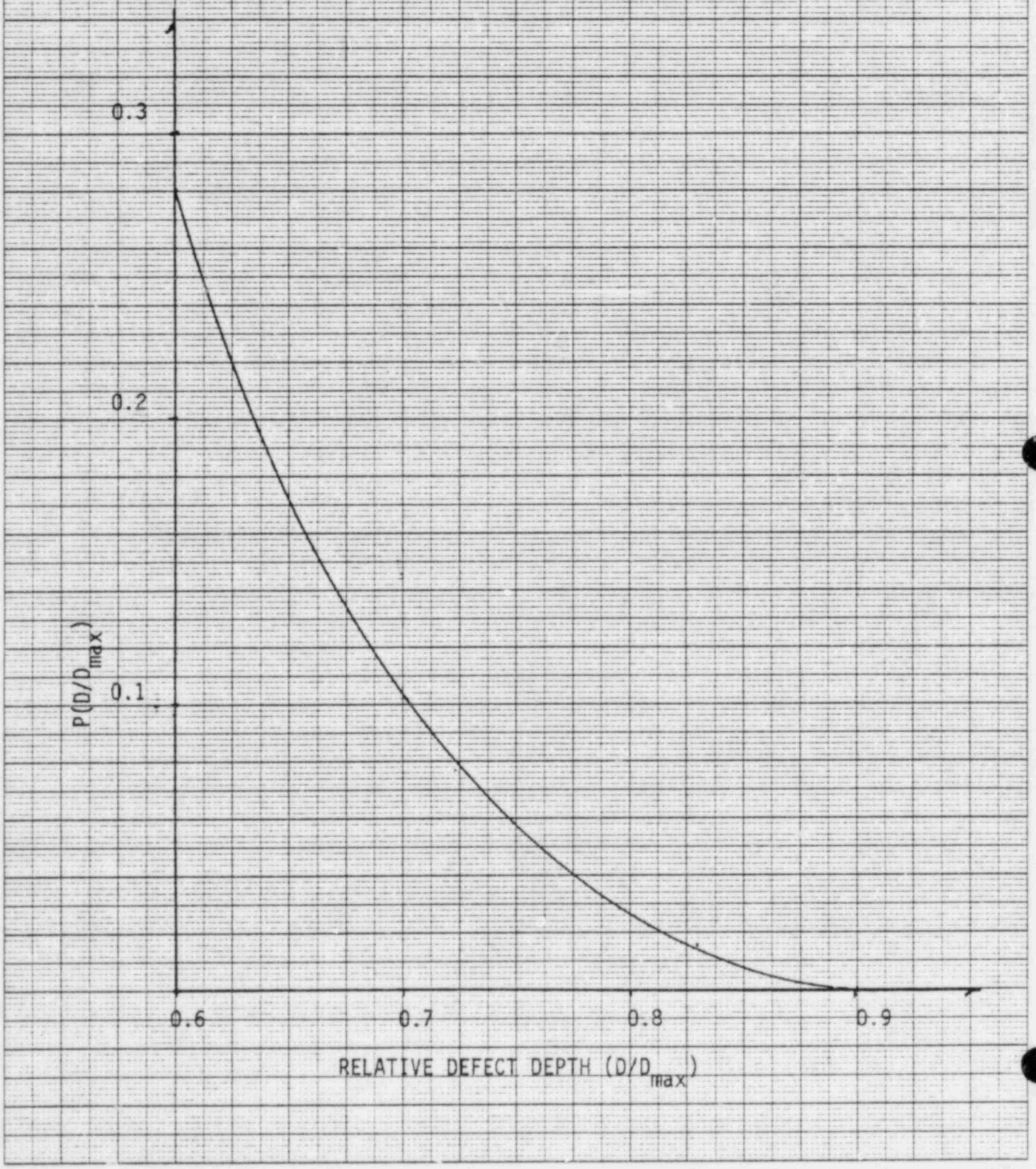
A second important element in the probabilistic tube strength model is the defect inventory, that is, the distribution of damage level among the more than 11000 tubes in a steam generator. Preliminary computations showed that only tubes degraded more than the assumed plugging limit of 60% contributed significantly to the risk of tube rupture.

Since current inspection plans called for sampling at least 3% of the steam generator tubes (more if any tubes are degraded beyond the plugging limit), an estimate of the percentage of the remaining population degraded beyond the plugging limit could be made from the Binomial distribution. The "best" estimate made at a 50% cumulative probability was approximately 1/4% or 28 tubes degraded beyond the 60% level.

The model used in this report assumes that the damage distribution can be represented by a continuous-analytical probability density function (PDF). Of the analytical PDF's, the Beta distribution most adequately models the physical limits of damage (0-100%) and provides sufficient flexibility in shape to model both relatively new and aging steam generator damage distributions. The Beta distribution has four parameters; two of which define the limits and two which can be adjusted to obtain a wide variety of shapes. The second pair of parameters were obtained by determining the parameter sets which satisfied the 1/4% tail criterion. Of these sets, the values leading to the most extreme distribution in the tail were chosen. The Beta distribution used in the model is shown in Figure B-2 for damage levels beyond the 60% plugging limit.

FIGURE B-2

DISTRIBUTION OF TUBES DEGRADED BEYOND PLUGGING LIMIT



IV. SIMULATOR STRUCTURE

Monte-Carlo simulation is used to compute tube failure probabilities on an event-specific basis. The general structure of the simulator used for these computations is shown in Figure B-3. The overall computation is a repetition of the computation shown in Figure B-3 for J events (x 2 steam generators per event).

The first step in the simulation is the computation of tube rupture probabilities for a set of four damage levels. These are computed using the distribution functions shown in Figure B-1. The probabilities thus computed represent the expected failure proportion for tubes at each damage level given the specific overpressurization characteristic of the event.

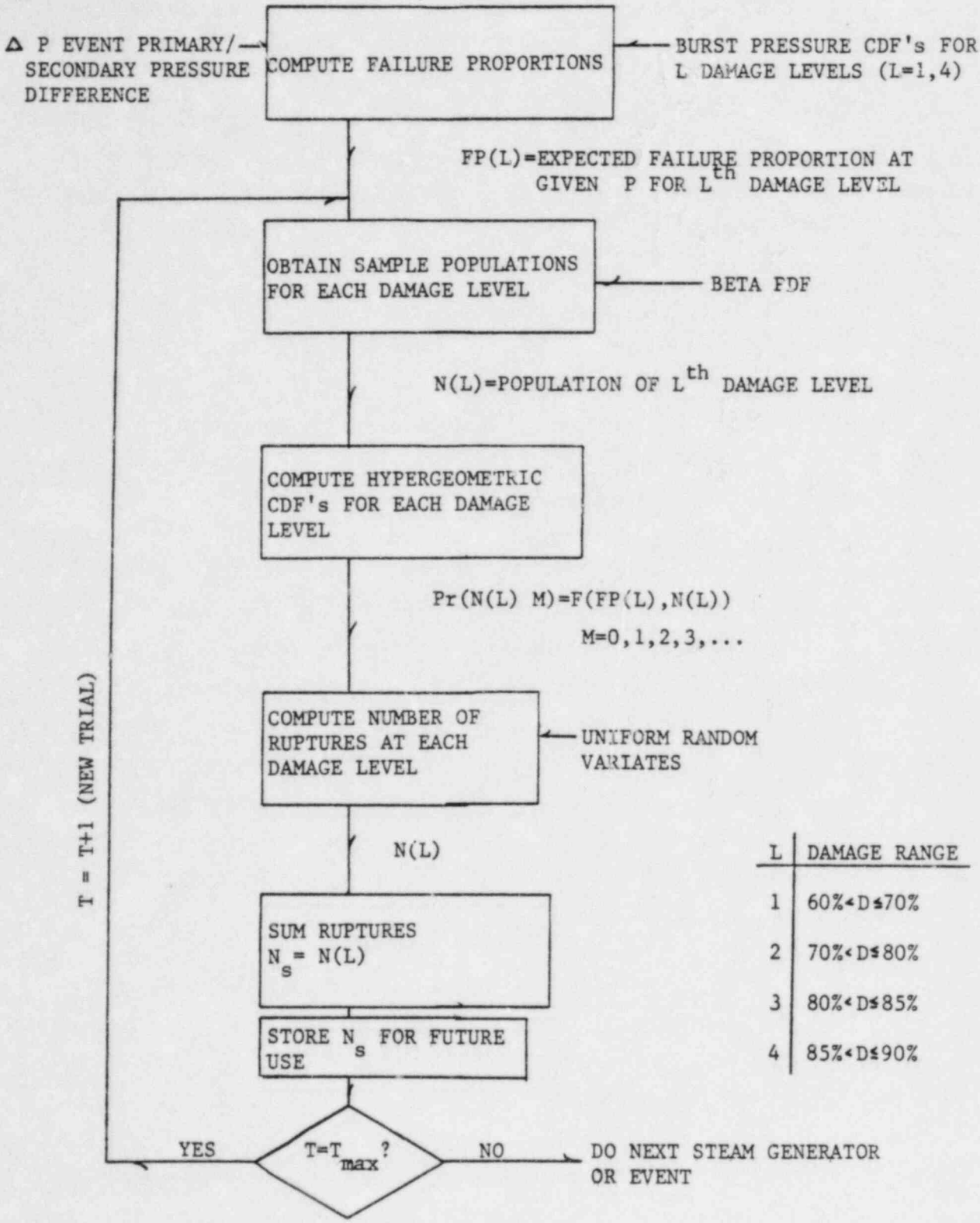
The second step in the computation is to obtain sample values for the number of tubes in each of four damage intervals. This is accomplished by randomly sampling from the distribution shown in Figure B-2. The expected failure proportions computed in the first step are then combined with their respective interval subpopulations to compute Hypergeometric cumulative distribution functions for the number of ruptured tubes in each interval. Uniformly distributed random variates are then used to obtain the number of ruptured tubes. The entire second step is repeated for the required number of trials to obtain the probabilities of N tube ruptures (N = 1,30) for the steam generator.

The output of the simulator is a [2J x N] matrix of probabilities (P(j,)). Each row contains the probabilities of n or less tube failures for a specific event/steam generator. The odd numbered rows contain the results for the more severely affected steam generator. The even numbered rows contain the results of the less affected steam generator. The frequency of tube ruptures for the spectrum of J events is computed from:

$$F(n) = P(j,n)\ E(j) \quad \begin{array}{l} j = 1,3,5,\ldots \text{affected S.G.} \\ j = 2,4,6,\ldots \text{unaffected S.G.} \end{array}$$

FIGURE B-3

SIMULATOR STRUCTURE



L	DAMAGE RANGE
1	60%<D≤70%
2	70%<D≤80%
3	80%<D≤85%
4	85%<D≤90%

where:

n = number of ruptured tubes
$E(j)$ = frequency of j^{th} event
$P(j,n)$ = probability of n tube ruptures given j^{th} event
$F(n)$ = overall frequency of n ruptured tubes

A special feature of the simulator is the ability to check for multiple generator tube ruptures. This is accomplished by storing and comparing numbers of ruptured tubes for both the affected and unaffected steam generators on a trial-by-trial basis.

where:

n = number of ruptured tubes
$E(j)$ = frequency of j^{th} event
$P(j,n)$ = probability of n tube ruptures given j^{th} event
$F(n)$ = overall frequency of n ruptured tubes

A special feature of the simulator is the ability to check for multiple generator tube ruptures. This is accomplished by storing and comparing numbers of ruptured tubes for both the affected and unaffected steam generators on a trial-by-trial basis.

APPENDIX B

REFERENCES

1. Frankel, J., "Burst Pressure Statistics for Non-Degraded Tubing", BNL20368 [Appendix II], 1975

2. Kao, C. S., "The Distribution of Burst Pressure for Tubes", BNL21917, 1976

3. Alzheimer, J. M. et. al., "Steam Generator Tube Integrity Program Phase I Report", NUREG/CR-0718 PNL2937, September 1979.