CEN-239
Supplement 3
Revision 01

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

PALO VERDE NUCLEAR GENERATING STATION

UNITS 1, 2 AND 3

Prepared for the C-E Owners Group

Nuclear Power Systems Division
September, 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.

CEN-239
Supplement 3
Revision 01

September, 1983

REVISION 01

Revision 01 to the Probabilistic Risk Assessment of the Effect of PORVs on Depressurization and Decay Heat Removal for Palo Verde Nuclear Generating Station Units 1, 2, and 3 provides changes to Supplement 3 text to amplify or update the present analysis results. These changes are the result of a more detailed treatment of the Automatic PORV cases, and a more complete analysis of Auxiliary Feedwater restoration. The changes are indicated by a change bar in the right margin. This revision supersedes the existing Supplement 3.

SUMMARY OF SUPPLEMENT 3

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 responses presented for these questions provide a synopsis of the analyses that are contained within this document. These results are specific to the Palo Verde Nuclear Generating Station (PVNGS) Units 1, 2 and 3. Responses to questions 1 thru 7, 8e and 12 thru 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 the operating experience of the nuclear industry and a fault tree analysis of the PVNGS MFW design were performed to determine the frequency of loss of MFW events. The results of the analysis are quantified by a statistical distribution which represents the frequency of loss of MFW. For PVNGS, the initiating event frequency can be expressed in terms of a median value of 1.18 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 PVNGS are 7.3E-6 per year with an associated error factor of 11 without PORVs and 1.0E-5 per year with an associated error factor of 12 with PORVs (manual design). (The resulting core damage frequency for PVNGS assuming an automatic PORV design is 5.0E-6 per year with an associated error factor of 13).

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 1.1E-5 per year with an associated error factor of 13.

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 nigh 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 generato , 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 ste · generators for PVNGS assuming offsite power is available can be expressed in terms of a median value of 1.7E-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 10.

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 5 (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 two plant designs (manual PORV design and automatic PORV design) which would be assumed to provide increased RCS decay heat removal and depressurization capability. For the manual PORV 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 8.4E-8 per year with an associated error factor of 11. 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 3.9E-6 per year with an associated error factor of 17.

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 net increase in total core damage frequency due to the installation of manually actuated PORVs of 1.2E-6 per year (median value).

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 2.6E-6 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

ADHR	Alternate decay heat removal
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
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
PVNGS	Palo Verde Nuclear Generating Station
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 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 Palo Verde Nuclear Generating Station (PVNGS), Units 1, 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, 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 responses 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.

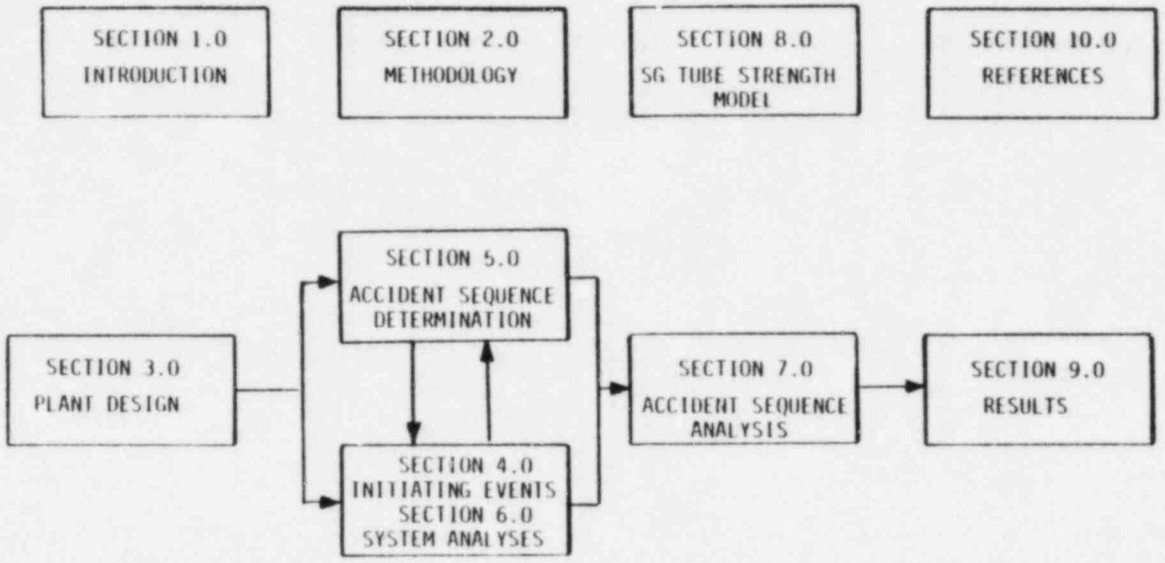


FIGURE 1.4-1

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.

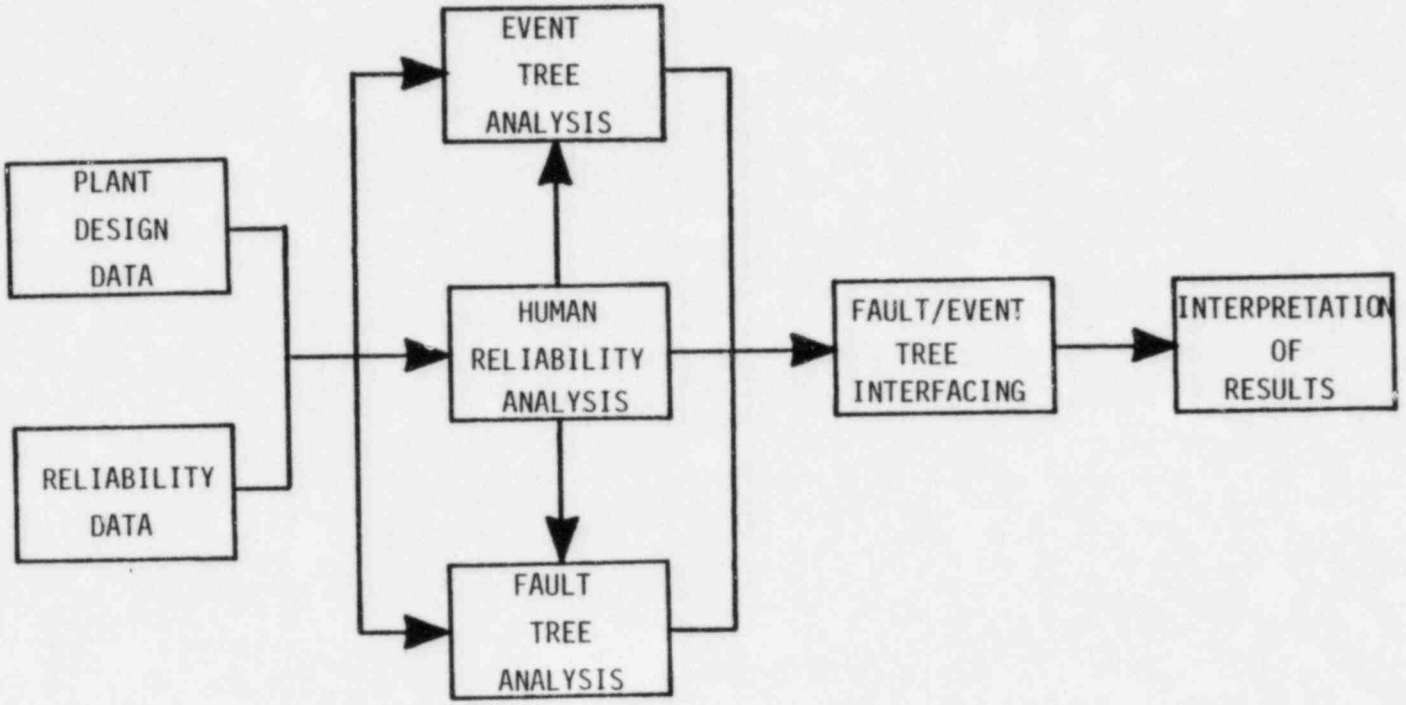


FIGURE 2.0-1

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
- Plant System Descriptions (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 respond to 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
- Plant System Descriptions (8)
- Plant system operating instructions (11)
- CEN-152, C-E Emergency Procedure Guidelines (9)
- Control board layout drawings and equipment lists (13)

In addition to these sources, interviews with reactor operators 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 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 level 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.

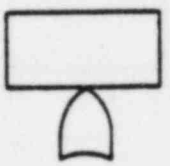
2.2.2.1 Fault Tree Construction

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

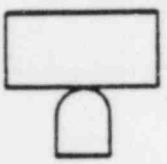
The evaluation of each fault tree yields both qualitative and quantitative information. The qualitative information consists of the "cutsets" of the model. The cutsets are the various combinations of component failures that result in the top event, i.e., the failure of the system. The cutsets form the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



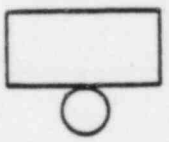
OR GATE

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



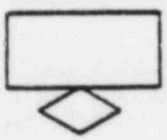
AND GATE

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



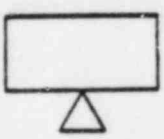
BASIC EVENT

Basic fault event requiring no further development.



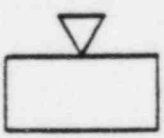
EXTERNAL INPUT

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.

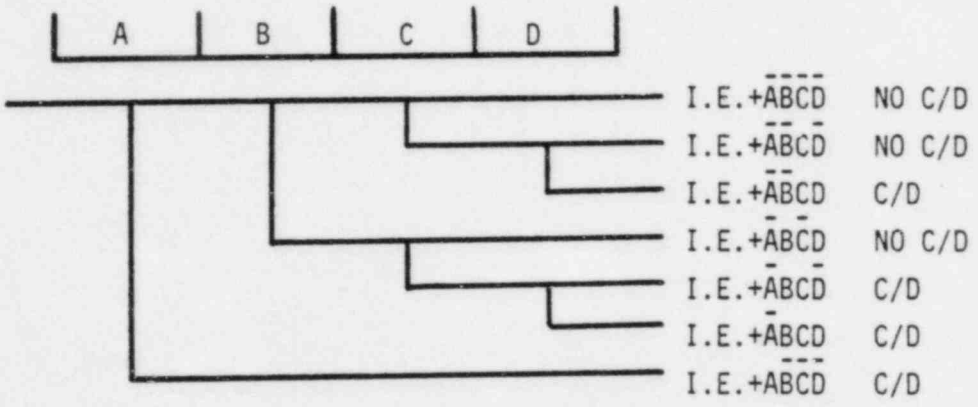
2.2.3 Fault Tree/Event Tree Interfacing

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

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

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

U 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. If the calculated conditional failure probability is less than the normal random failure probability, the random failure probability is used.

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

Palo Verde Nuclear Generating Station (PVNGS) Units 1, 2 and 3, operated by the Arizona Public Service (APS) Company is located approximately 36 miles west of the city of Phoenix in Maricopa county, Arizona. 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 Palo Verde station features separate containments, auxiliary buildings, turbine buildings, diesel generator buildings, control buildings and fuel handling buildings for Units 1, 2 and 3. One ultimate heat sink is provided for each generating unit. The ultimate heat sink consists of two Seismic Category I essential spray ponds. The ultimate heat sink is utilized for normal and emergency shutdown. The ultimate heat sink has a storage capacity that enables the associated essential spray pond system to operate continuously for 30 days without any makeup water supply.

The NSSS generates approximately 3800 MWt, producing saturated main steam. Each of the three 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. There are separate safety systems for each of the 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 to either steam generator.

The containment systems for each unit include the containment structure, the containment spray system, the containment air purification and cleanup systems, the containment building purge system, and the containment hydrogen 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.

Electrical power is supplied to plant equipment through multiple power sources. The main turbine-generator supplies the auxiliary loads during normal plant operation. Three startup transformers can be supplied by any one of the four circuits from the Southern California Edison - Arizona - New Mexico - West Texas power grid to the PVNGS switchyard. Each unit has 2 backup diesel generators available for safety related loads in the event offsite power is lost. 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 main feedwater pumps. Two identical U-tube steam generators produce saturated steam. Two steam generator outlets are on each steam generator. A header connects all main steam lines and each main steam line is routed to the main turbine.

The turbine is a 1800 r/min, tandem-compound, 6-flow, 43-inch last state bucket reheat unit. It consists of one double-flow, high-pressure (HP) turbine, three double-flow, low pressure (LP) turbines and four moisture separator-reheaters with two stages of reheating. The direct-driven generator is a General Electric Corporation three-phase, 60 Hz, four-pole, cylindrical rotor, conductor cooled, directly coupled to the last low-pressure stage of the turbine.

Electrical power from the generator is conducted from the generator terminals by an isolated-phase bus to the 24-KV side of the main step-up transformer. The other side of the main transformer is connected to 525-KV lines which carry the power to the switchyard to be fed into the 525-KV transmission system.

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

- Core thermal power level - 3817 MWt
- Net electrical power output at generator terminal - 1304 MWe
- Electrical power output consumed onsite - 34 MWe
- Net electrical power output consumed offsite - 1270 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
Auxiliary Spray System	• Safety System • Flow Provided by any One of Three Charging Pumps
Containment Spray System	• Two Train Containment Spray System
Power Operated Relief Valves	• 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 • 55% Turbine Bypass Capacity
Main Steam Isolation	• Safety System with Redundancy • Safety Coded Valve in Each Steam Line
Atmospheric Dump System	• Safety System • Two Safety Coded Valves per Steam Generator
Main Steam Safety Valves	• Banks of Coded Safety Valves with Redundancy
Main Feedwater System	• Three Motor Driven Condensate Pumps • Two Turbine Driven Feed Pumps
Auxiliary Feedwater System	• Safety System with Redundancy • Two Motor Driven Pumps • One Turbine Driven Pump
Steam Generator Blowdown 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
Cooling Water Systems	• Two Safety Systems with Redundancy • Two Motor Driven Pumps in Each Train
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 PVNGS 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	Cooling Water Systems	ESFAS
High Pressure Safety Injection		X	X	X			X
Auxiliary Spray System[2]		X	X	X	X		
Containment Spray System		X	X	X		X	X
PORV[3]		X	X	X			
Primary Feed and Bleed[3]		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
Steam Generator Blowdown 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	Cooling Water Systems	ESFAS	Instrument Air
Onsite AC Non-1E							
Offsite AC							
Onsite AC Class 1E				X		X	
125V DC Class 1E							
Cooling Water Systems		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.

4.0 INITIATING EVENTS

4.1 EVENT SELECTION

The NRC questions focused on those initiating events which the staff considered to be most relevant to the PORV issue. These events are Loss of Main Feedwater, Steam Generator Tube(s) Rupture in one or two steam generators, and PORV LOCA. In addition, a survey was made of other potential core damage scenarios to identify those which could be mitigated by improved methods of depressurization or decay heat removal.

4.2 OTHER EVENTS

The most comprehensive PRA performed to date on a plant with a C-E supplied NSSS is the Calvert Cliffs 1 Interim Reliability Evaluation Program (IREP) (29). The IREP Final Report has not yet been issued. However a draft final report was issued in January of 1982. This draft was reviewed to identify dominant accident sequences. Table 7.4-1 lists the Calvert Cliffs Unit 1 dominant sequences. Each sequence was studied to determine which ones are relevant to the PORV issue. Results of the survey are presented in Section 7.4.

4.3 INITIATING EVENT FREQUENCIES

4.3.1 Loss of Secondary Heat Sink

The Main Feedwater System provides a continuous supply of feedwater to the steam generators for full load to zero load operations during normal plant operation. The PPS provides protection against the reduction or loss of normal feedwater by the steam generator low water level trip. The MFW system is designed to automatically provide 5% 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 plant/reactor trip events causing a loss of full-load operating main feedwater flow and subsequent loss of the post-trip 5% bypass main feed 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. System perturbations or malfunctions that result in automatic plant/reactor trips were determined based on operating experience (19) and information in References (15) and (16).

Among the potential root causes of a Loss of Main Feedwater event is a Feedwater Line Break. This event is significant in that along with possibly resulting in a loss of Main Feedwater to both steam generators, it also has the potential for degrading the reliability of the Auxiliary Feedwater System. This root cause was considered but was not included in accident sequences for evaluating the change in core damage frequency associated with adding PORVs. This root cause was omitted because the frequency of core damage due to loss of heat sink following Feedwater Line Break is low compared with the sequence cut-off frequencies discussed in Section 7.1.1.

The frequency of Feedwater Line Break in the specific lengths of pipe that could effect AFW reliability has been evaluated at 4.5E-5 per year (30). The conditional unreliability of AFW (given FWLB) is 3.1E-3 (See Section 6.11). The ADHR function unreliability (from Section 6.13) is 5.8E-2. Therefore, the point estimate of the frequency of core damage due to LOHS following a FWLB is 8.1E-9.

The frequency and causes of Loss of Normal Feedwater were determined by fault tree analysis in Section 6.10. The initiating event frequency of Loss of Main Feedwater is presented in Table 4.3.1-1. To account for the PVNGS specific feedwater system design, the MFW system and its support systems were modelled at the component level in the analysis. Breakdown initiators that affect more than the MFW system were also modelled directly in the analysis. (Refer to Section 6.10).

TABLE 4.3.1-1

LOSS OF MAIN FEEDWATER INITIATING EVENT FREQUENCY

Frequency (Median Value per year)	Error Factor
1.18	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

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

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 θ is determined by using the following expression

$$\theta_{.5} = \frac{\chi^2_{.5,10}\,\hat{\theta}}{2n} = \frac{9.342\ (1.108 \times 10^{-2})}{8} = 1.3 \times 10^{-2}/\text{year}$$

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

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

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

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

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). 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

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

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

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

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

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. In order to address PORV LOCA impact on core damage frequency, a manual PORV design and an automatic PORV design were considered. Both assumed PORV designs allow 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. For the manual PORV design, the PORVs are assumed not to be designed to minimize challenges to the primary safety valves. However, for the automatic PORV design, the PORVs are assumed 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 (30 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 and 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 of either PORV flowpath following a tube rupture in one steam generator. The unaffected steam generator is available to remove RCS heat.

3. Spurious or Transient Induced PORV LOCA. This type of PORV LOCA refers to the opening of either or both PORV flowpaths. For the manual PORV design, this type of PORV LOCA includes error (test, maintenance, or operator) induced openings. For the automatic PORV design, this type of PORV LOCA includes high RCS pressure transient induced openings. 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 (manual design) 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[1] (Median Value per Year)	Error Factor
PORV LOCA Following LOHS	1.8E-5	16
PORV LOCA Following SGTR	1.3E-4	7
Spurious or Transient Induced PORV LOCA		
(a) Manual Design	3.2E-5	16
(b) Automatic Design	5.0E-3[2]	13

Note: 1. 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.

2. This value excludes challenges to the PORVs due to malfunction of the turbine runback feature. Operating experience shows that C-E NSSS supplied plants with turbine runback feature experience more challenges to the PORVs. Therefore, the affected plants are currently operating with the turbine runback feature overridden. If challenges to the PORVs due to malfunction of the turbine runback feature were included, the PORV LOCA initiating event frequency would increase by approximately 15%.

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 PVNGS Unit 1 design. The results are considered to be applicable to Units 2 and 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 70 minutes 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% 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% 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 one seismic Category I motor-driven and one turbine-driven feedwater pumps and one non-seismic Category I motor-driven pump, 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

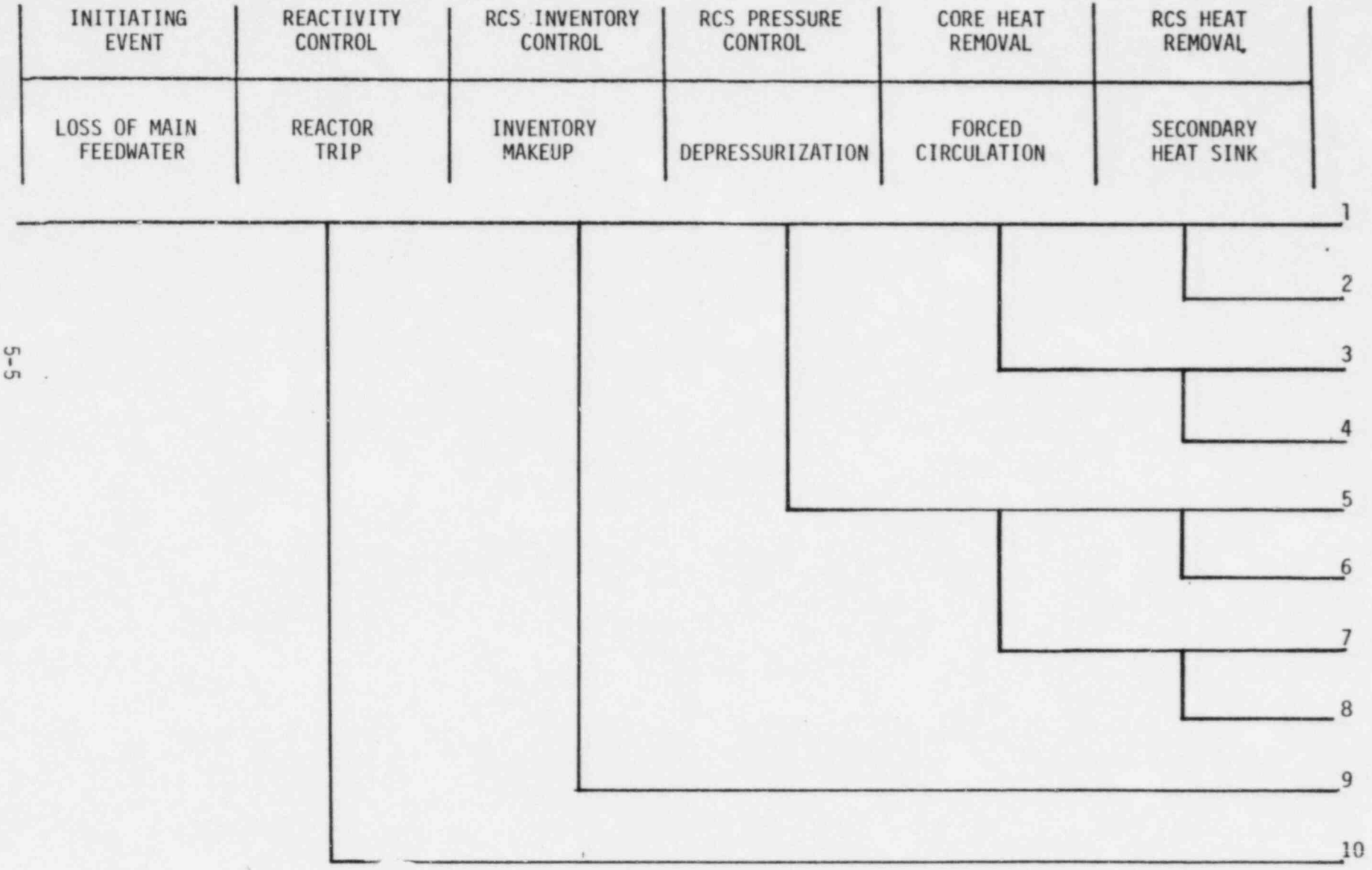
NORMAL SEQUENCE OF EVENTS FOR LOSS OF FEEDWATER

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 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 2 AFW Pumps to One SG
U_1	Failure to Restore Feed Flow	Failure to Manually Restore AFW Flow from 1 of 2 AFW Pumps to 1 SG and Failure to Establish Flow from 1 of 1 Non-essential AFW Pump in 60 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 2 AFW Pumps to 1 SG and Failure to Establish Flow from 1 of 1 Non-essential AFW pump in 25 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 60 minutes
W_1	Failure to Remove Secondary Steam	Failure to Remove Steam from SG by Opening 1 of 8 TBVs, 1 of 4 ADVs or 1 of 20 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 2 HPSI Pumps and 1 of 3 Charging Pumps or 2 of 2 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.

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 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 restore AFW flow or start the non-essential AFW pump 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 60 minutes to re-establish AFW flow before core damage conditions are unavoidable (28, Section 2.8). An analysis was performed to determine the human error probability for failure to restore AFW and align the non-essential AFW pump in the 60 minute time period in Section 6.17.

V At 60 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.

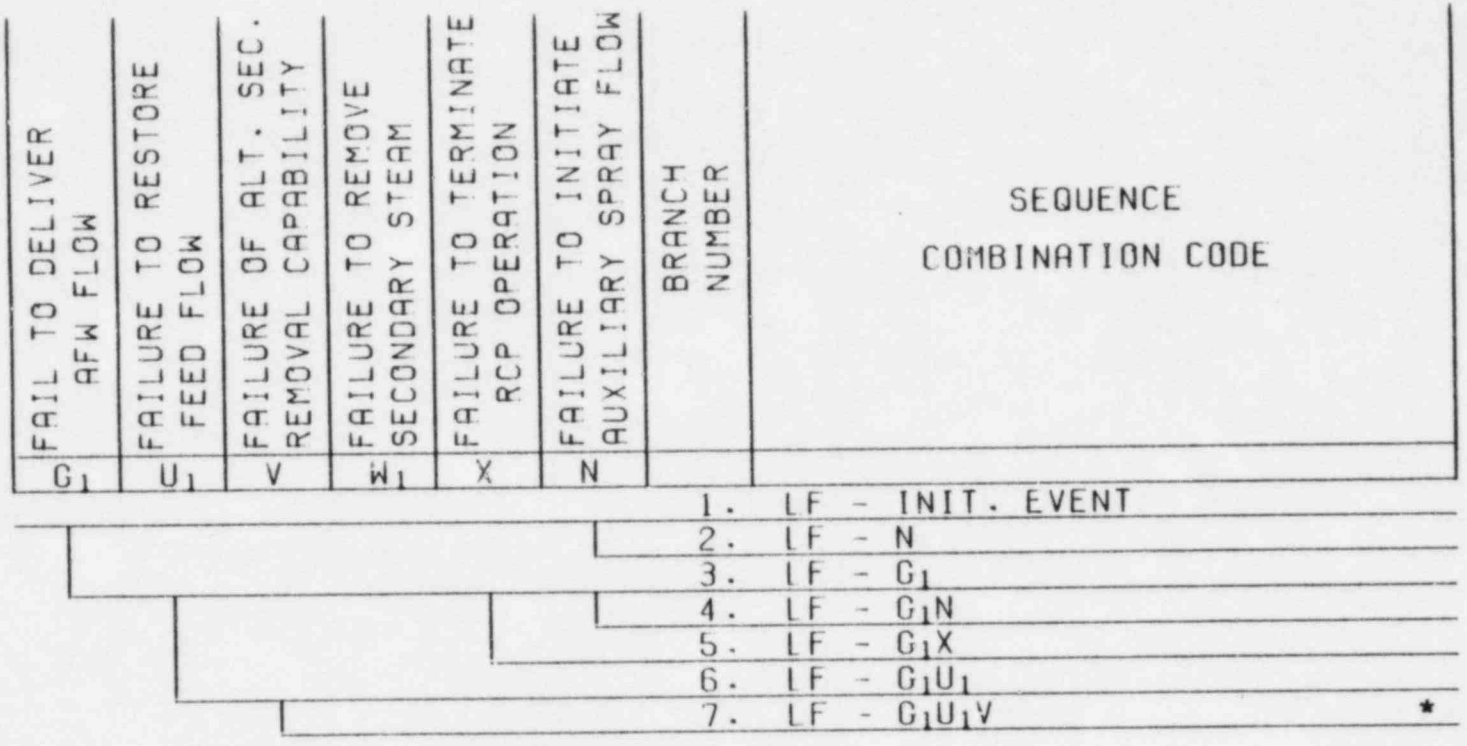


FIGURE 5.1.4.1-1

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.

M_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).

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 Tank (RWT). 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 25 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 25 minutes for restoration actions.

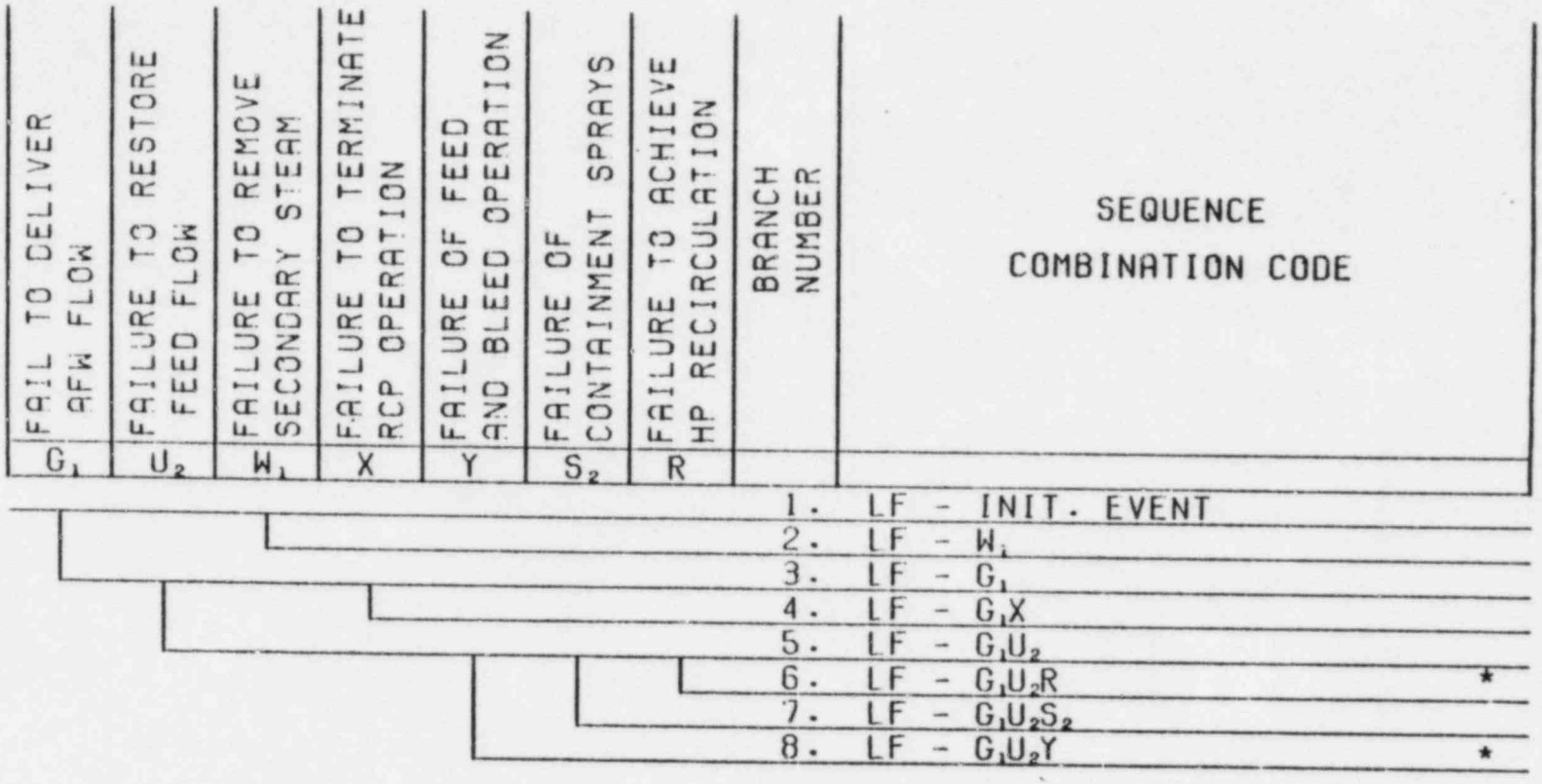


FIGURE 5.1.4.2-1

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.

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 25 minutes, opening of both PORV trains and providing the required primary inventory makeup, results 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) 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. (PORVs could be used if the Auxiliary Spray System was unavailable).[1]

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 at least one 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 at least one 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

INITIATING EVENT	REACTIVITY CONTROL	RCS INVENTORY CONTROL	RCS PRESSURE CONTROL	CORE HEAT REMOVAL	RCS HEAT REMOVAL
SGTR	REACTOR TRIP	MAINTAIN SG PRESS INVENTORY MAKE-UP LIMIT RCS PRESSURE	DEPRESSURIZATION	NONE	MAINTAIN SECONDARY HEATSINK

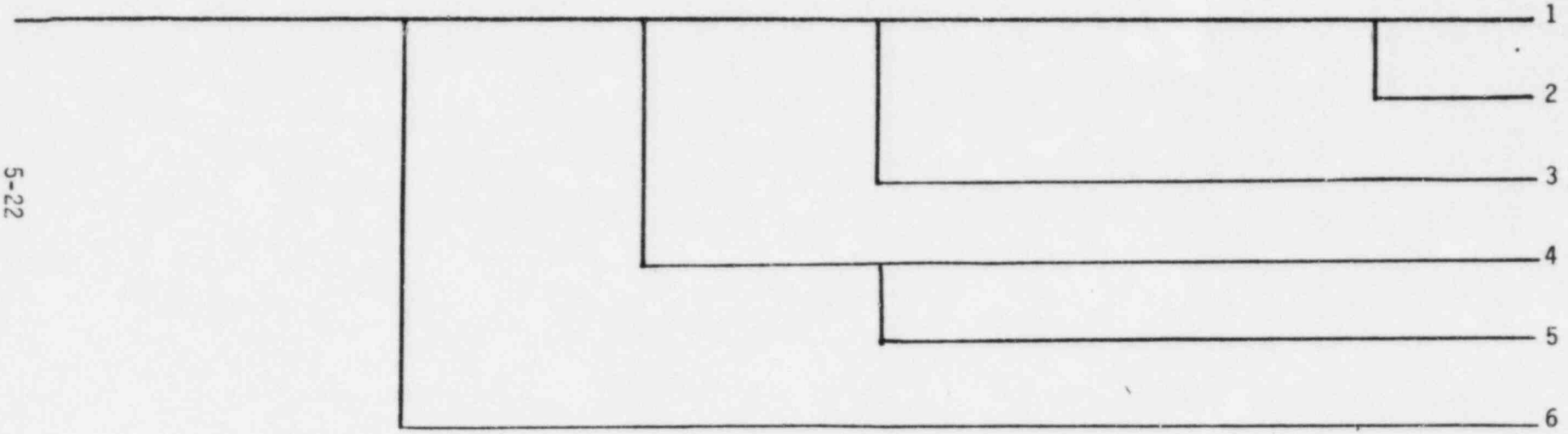


TABLE 5.2.3-1

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 analyses (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 determined to be negligible. 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-2 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 2 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	8 of 8 TBVs fail to quick open following turbine trip.
D	Turbine Bypass Valve Fails to Reclose	1 of 8 TBVs fails to reclose following quick open or during cooldown.
E_1	MSIV on Affected (or Most Affected) SG Fails to Close	One of two MSIVs 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 from both ADVs 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 at least one of two ADVs on the unaffected SG.
K	ADV on Affected (or Most Affected) SG Unavailable	Failure to initiate steam flow through at least one of two ADVs on the affected SG.
L	ADV on Affected (or Most Affected) SG Fails to Close	Failure to terminate ADV flow from both ADVs 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	One of two MSIVs on the least affected SG fails 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.

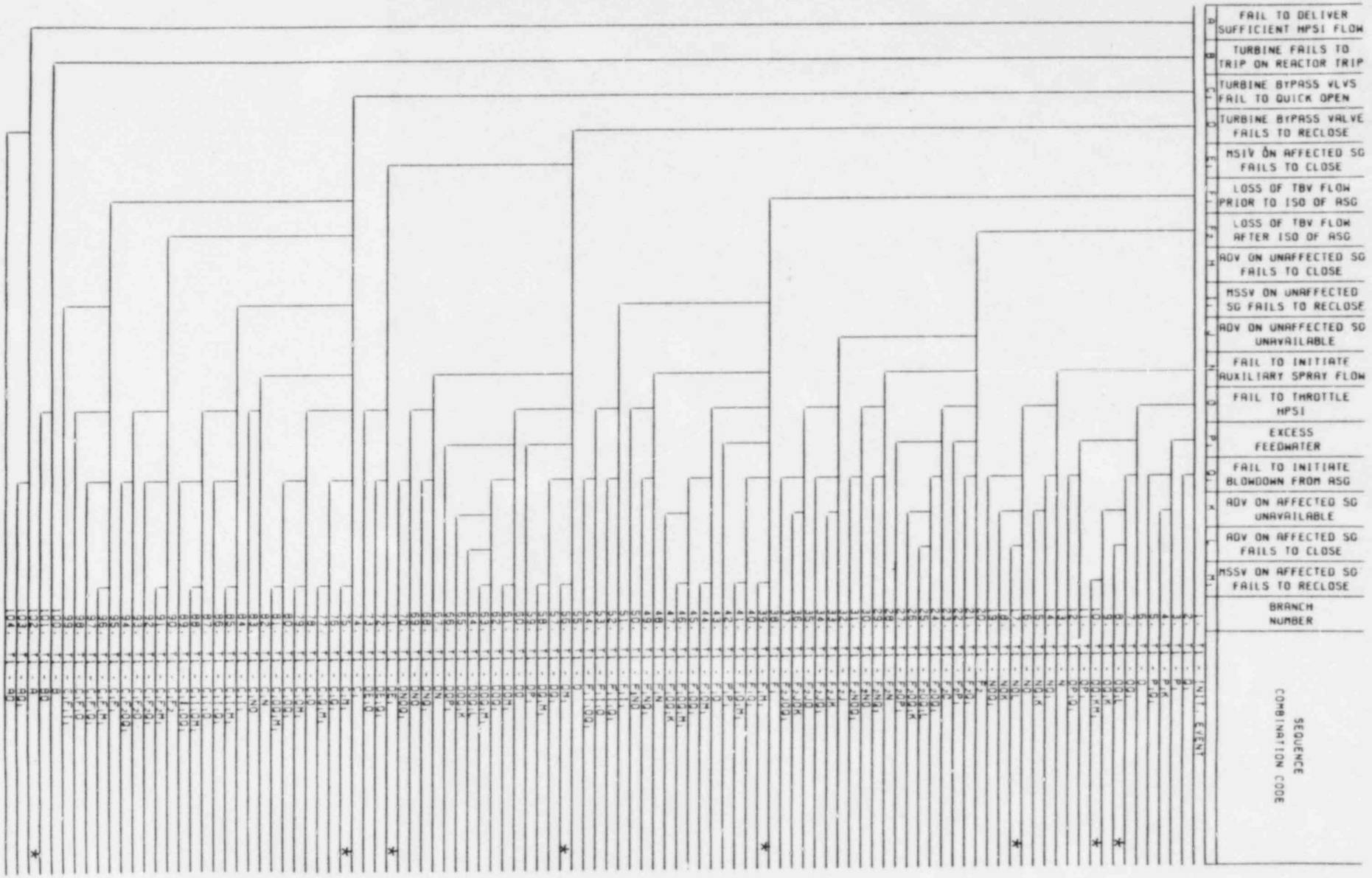
A Failure to Deliver Sufficient HPSI flow refers to the delivery of one pump flow to two RCS loops. The fault tree analysis for Failure to Deliver Sufficient HPSI flow (assuming offsite power is available at the time of the initiating event) is presented in Section 6.1.

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 one MSIV on the affected SG fails to close, uncontrolled SG blowdown will occur through the turbine. If both MSIVs close 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 one MSIV on the affected SG 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 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 one of two MSIVs on SG-2 failing to close on MSIS. The fault tree analysis for MSIV on SG-2 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
SEQUENCE
COMBINATION CODE

*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.

SGTR IN ONE SG SYSTEMIC EVENT TREE

FIGURE 5.2.4.1-1

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 ADVs on the unaffected SG are unavailable (e.g. the operator fails to open at least one 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 one of the two ADVs associated with SG-1 failing to close after being challenged by 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-1 Fails to Close is presented in Section 6.8.

I_1 MSSV on Unaffected SG Fails to Reclose refers to one MSSV on SG-1 failing to close after being challenged on turbine trip (following a TBS failure) or following a failure of the associated ADVs to open. Six MSSVs are assumed to open on SG-1 if the TBVs fail to quick open. If the ADVs are 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 failing to open at least one of two ADVs associated with SG-1 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 failing to open at least one of the two ADVs on SG-2 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 one of two ADVs on SG-2 failing to close after being challenged by 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-2 Fails to Close is presented in Section 6.8.

M_1 MSSV on Affected SG Fails to Reclose refers to one MSSV on SG-2 failing to close after being challenged by a failure of the TBVs to quick open or a failure of one ADV on the affected SG to open. Six MSSVs are assumed to open on SG-2 if the TBVs fail to quick open. If the ADVs are 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 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 the failure to initiate blowdown from the affected SG results in SG overfill and a challenge to the ADVs. 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-2. Excess feedwater in conjunction with failure to initiate blowdown from the affected SG results in SG overfill and a challenge to the ADVs. The fault tree analysis is presented in Section 6.11.

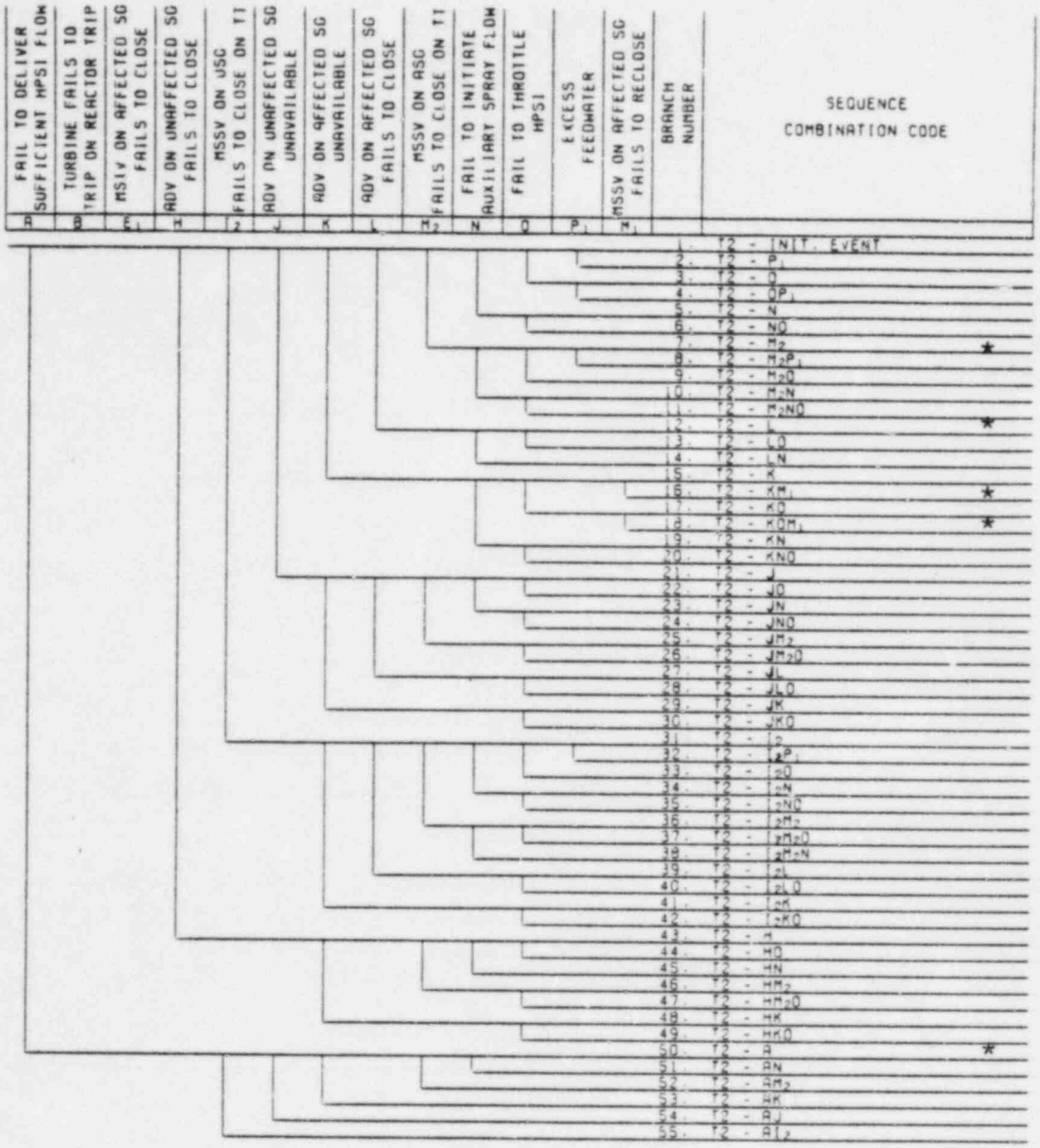
Q_1 Fail to Initiate Blowdown from the Affected SG refers to failing to initiate blowdown flow from SG-2. The fault tree analysis is presented in Section 6.12.

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-2 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 PVNGS a loss of offsite power results in loss of the Turbine Bypass System and loss of the Steam Generator Blowdown 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



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

SGTR IN ONE SG WITH COINCIDENT LOOP SYSTEMIC EVENT TREE

FIGURE 5.2.4.2-1

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-1 results in a MSIS. The fault tree analysis for ADV on SG-1 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-1 failing to close on turbine trip. Six MSSVs are assumed to open on SG-1 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 failing to open at least one of two ADVs associated with SG-1 when required (initiation of cooldown, following an MSIS to prevent a MSSV from opening). The fault tree analysis for ADV on SG-1 Fails to Open is presented in Section 6.8.

K ADV on Affected SG Unavailable refers to failing to open at least one of two ADVs on SG-2 in response to a challenge (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 one ADV on SG-2 failing to close after being challenged. 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-2 failing to close on turbine trip. Six MSSVs are assumed to open on SG-2. 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 ADVs are 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-2 failing to close after being challenged by a failure of the ADVs associated with SG-2 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.

O Fail to Throttle HPSI. See discussion for branch O 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.

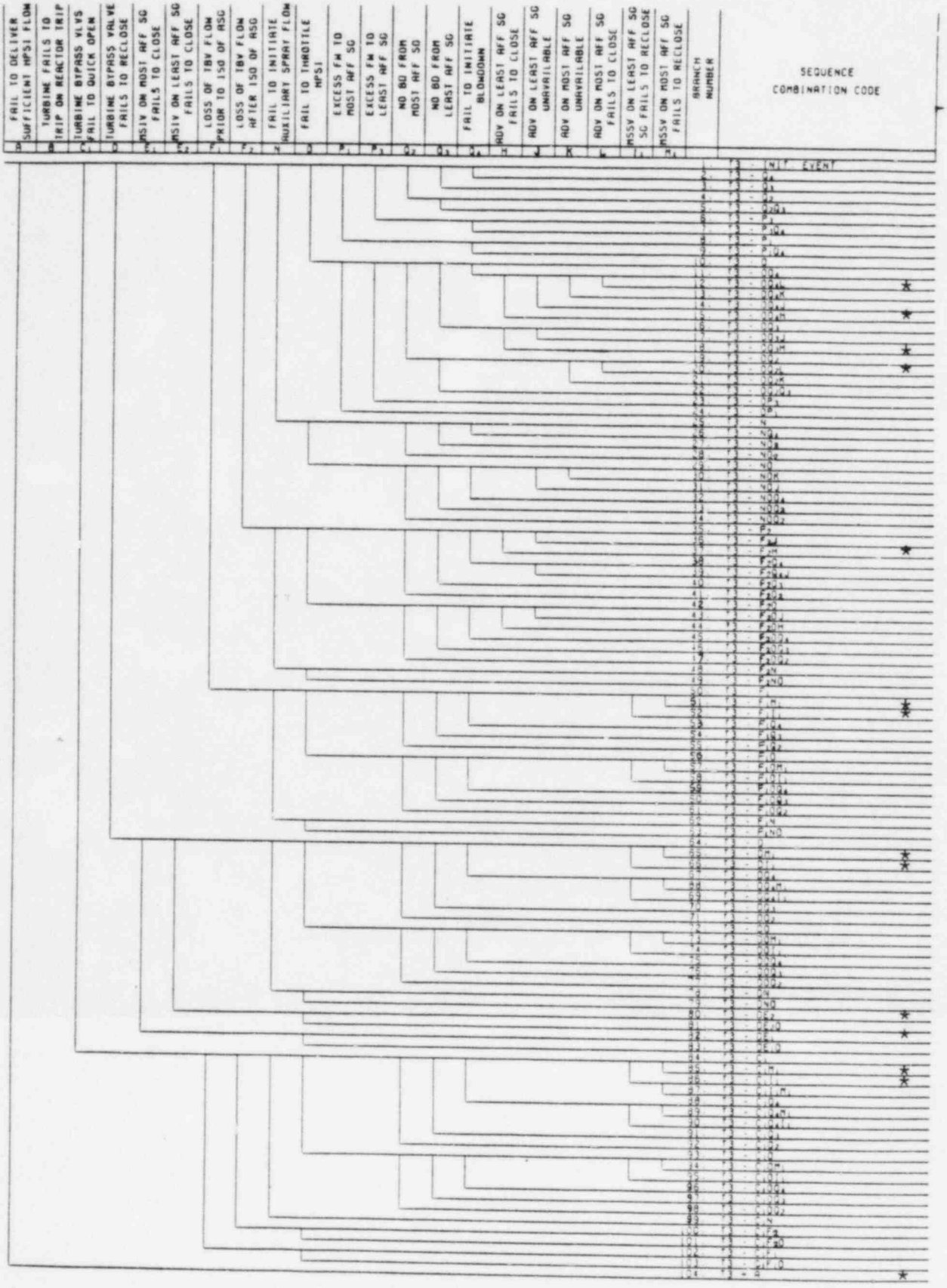
5.2.4.3 SGTR in Two Steam Generators Event Tree

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 one MSIV on either the most affected or least affected SG fails to close, uncontrolled SG blowdown will occur through the turbine. If all four MSIVs close successfully, the sudden termination in steam flow will



*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.

SGTR IN TWO SGs SYSTEMIC EVENT TREE

FIGURE 5.2.4.3-1

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 one MSIV fail to close, uncontrolled SG blowdown will occur through the Turbine Bypass System. If all four 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 one of two MSIVs on SG-1 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. One

ADV on the least affected SG could be opened by the operator (to prevent the MSSV from opening) and fail to close, or if the ADVs were 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 one of two ADVs associated with SG-1 failing to close after being challenged by 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-1 failing to close after being challenged by a failure of the TBVs to quick open or a failure of the ADVs 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 to the 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 to the 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-1. Excess feedwater in conjunction with failure to initiate blowdown from SG-1 results in SG overfill and a challenge to the ADVs 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-2. (Blowdown can still be initiated from SG-1). This branch includes failure to open the blowdown isolation valve on SG-2. 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-1. (Blowdown can still be initiated from SG-2). This branch includes failure to open the blowdown isolation valve on SG-1. 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.

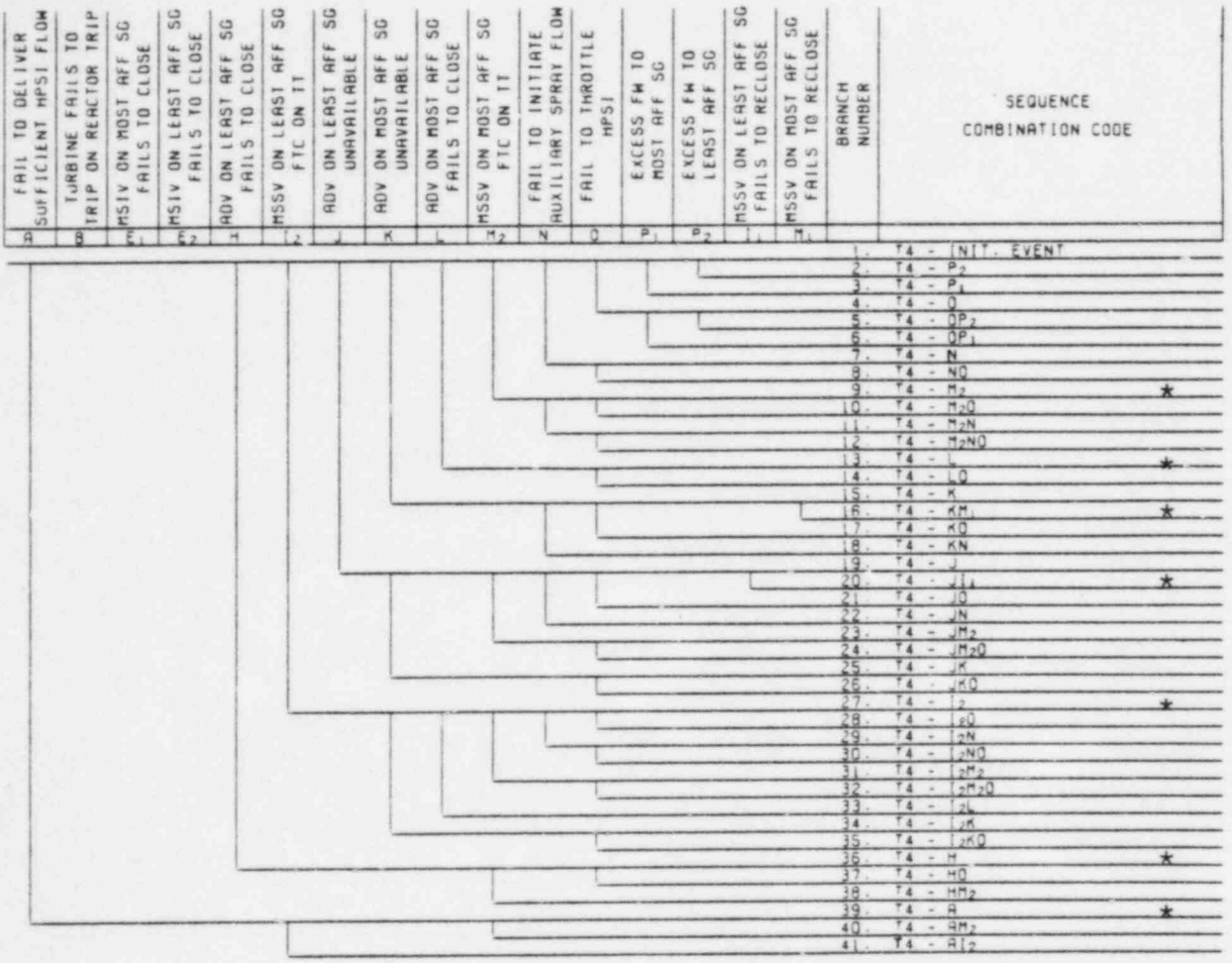
5.2.4.4 SGTR in Two SG with Coincident LOOP Event Tree

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 PVNGS a loss of offsite power results in loss of the Turbine Bypass System and loss of the Steam Generator Blowdown 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.



*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.

SGTR IN TWO SGs WITH COINCIDENT LOOP SYSTEMIC EVENT TREE

FIGURE 5.2.4.4-1

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 one of the two MSIVs on SG-1 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 one ADV associated with SG-1 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-1 failing to close on turbine trip. Six MSSVs are assumed to open on SG-1. 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 ADVs are 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-1 failing to close after being challenged by a failure of the ADVs on SG-1 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-1. 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

Both the manual and the automatic PORV designs considered feature two 50% capacity PORV flow paths. Each path consists of a motor operated block valve and a PORV. For the manual PORV design, the motor operated block valves and PORVs are closed during power operation. These valves are designed to be opened manually to reduce RCS pressure following a steam generator tube rupture event. These valves are also opened manually to establish a means for alternate decay heat removal following the loss of the preferred heat sink. For the manual PORV design, the PORVs are not designed to minimize challenges to the primary safety valves.

The automatic PORV design features normally opened motor operated block valves and closed PORVs during power operation. In the event of a high RCS pressure transient, the PORVs open automatically to prevent or minimize challenges to the primary safety valves.

The assumed PORV design allows for the valves to be manually opened following a steam generator tube rupture event or loss of the preferred

secondary heat sink event. In addition to procedural and automatic 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 designs 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. When containment pressure reaches the high-high setpoint, the containment spray pumps start and also take suction from the refueling water tank and 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 cooling 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 by the CSAS
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 or transient induced 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 either PORV flow path 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

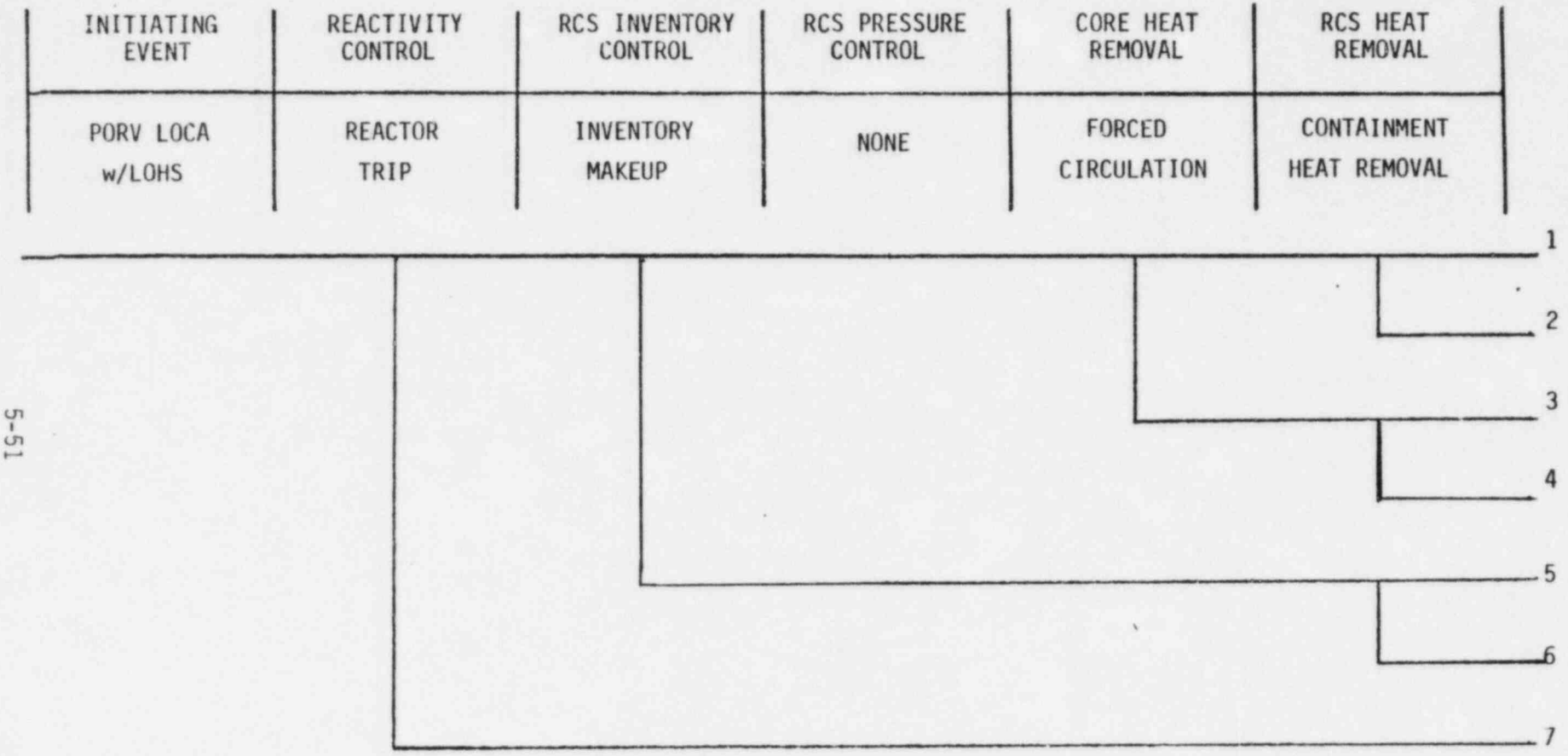


TABLE 5.3.3.1-1

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

[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 in response to LOHS leads to core damage. This sequence is addressed in the Section 5.1.4.2.

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 pressure 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

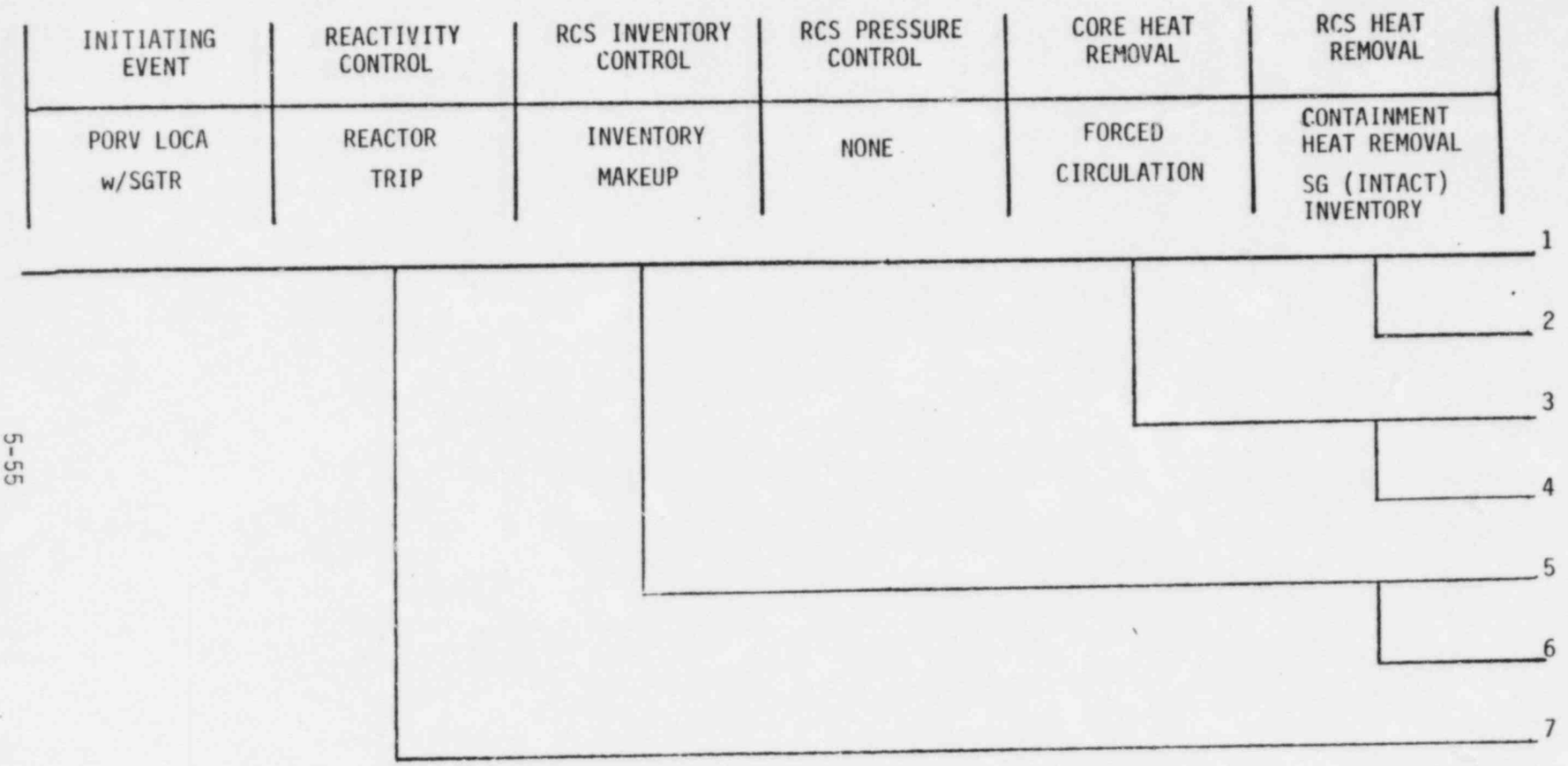


TABLE 5.3.3.2-1

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
	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 or Transient Induced 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 or a transient induced 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 or transient induced 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 OR TRANSIENT INDUCED
PORV LOCA
FUNCTIONAL EVENT TREE

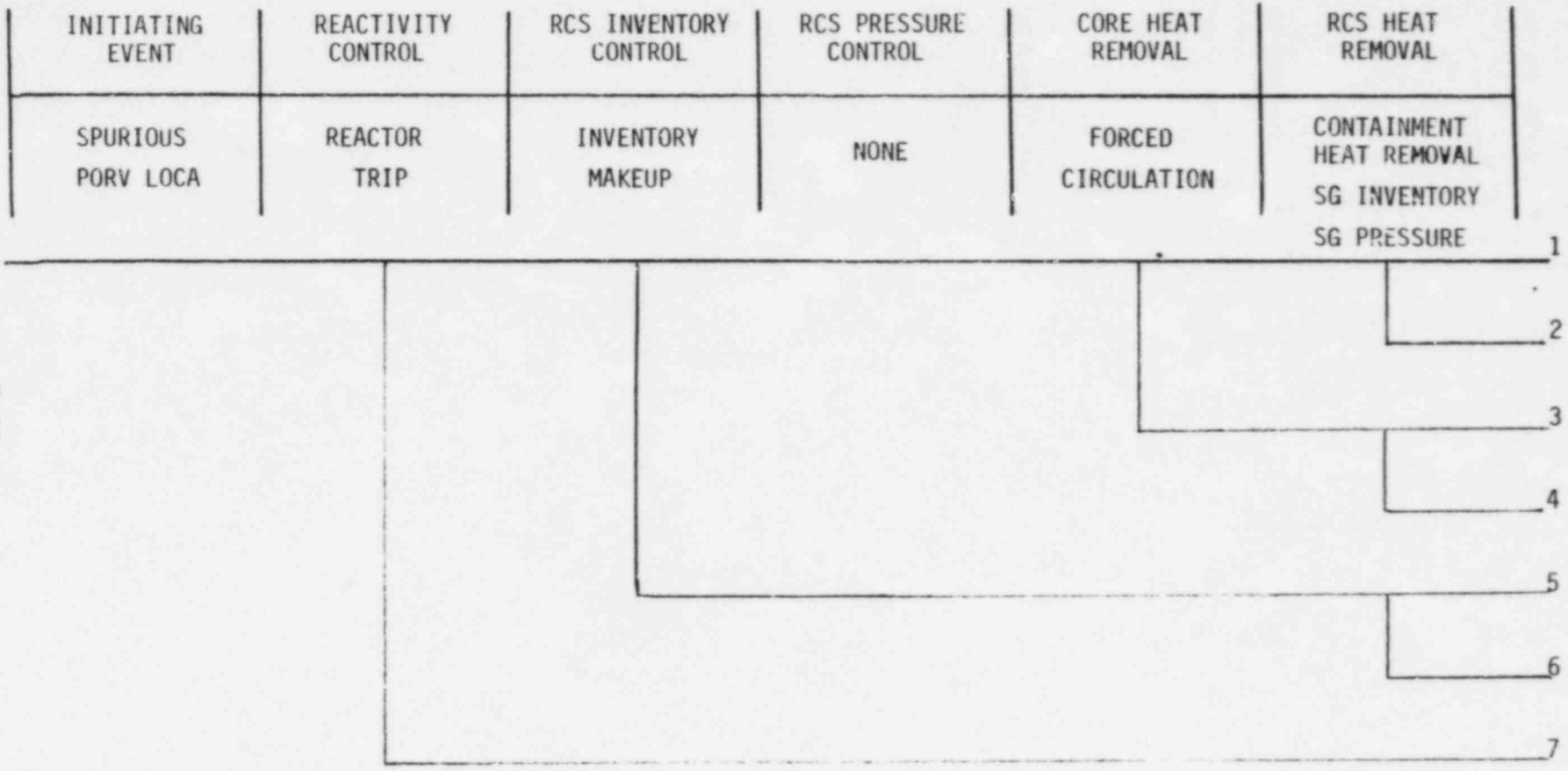


TABLE 5.3.3.3-1

SPURIOUS OR TRANSIENT INDUCED 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
	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. 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 times 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
P4	Initiating Event	Transient induced opening of both PORV flowpaths
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.
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 8 turbine bypass valves
W_2	Failure to Open MSSVs	Failure to control steam generator pressure by not opening at least 1 of 10 MSSVs associated with each steam generator.
T	Failure to Open ADVs	Failure to control steam generator pressure by not opening at least 1 of 4 ADVs

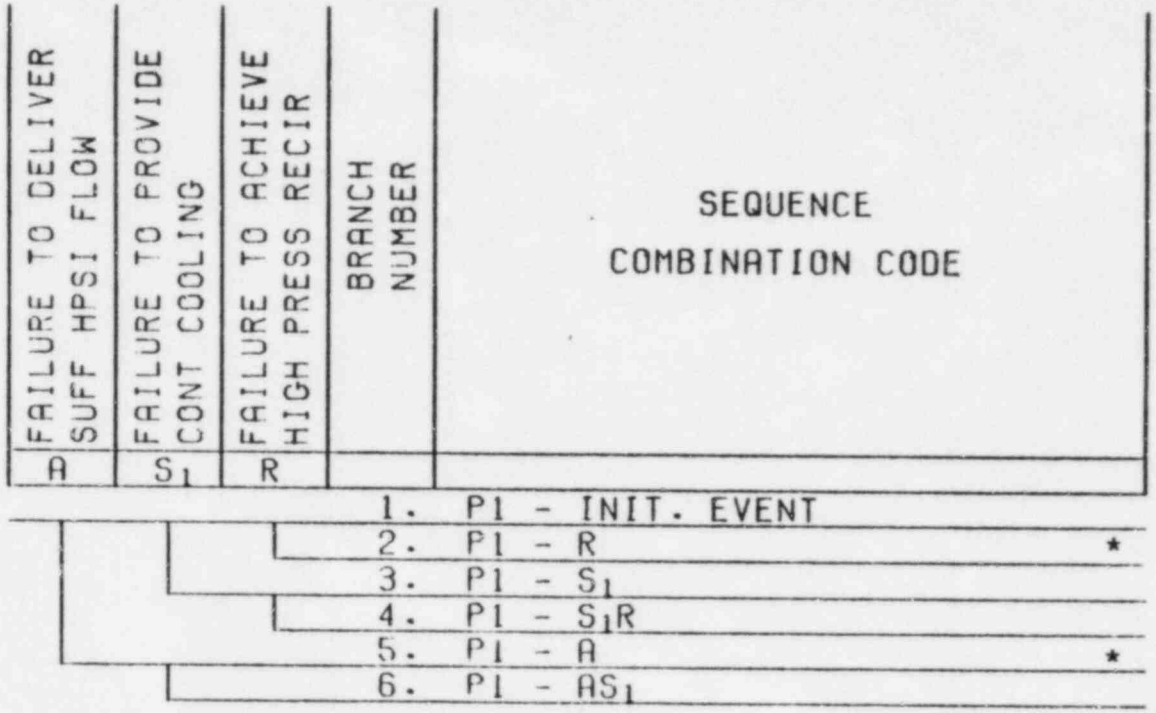


FIGURE 5.3.4.1-1

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. Additional information on the Containment Spray System 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 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 either PORV flow path following a tube rupture in one steam generator times the probability that the 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.

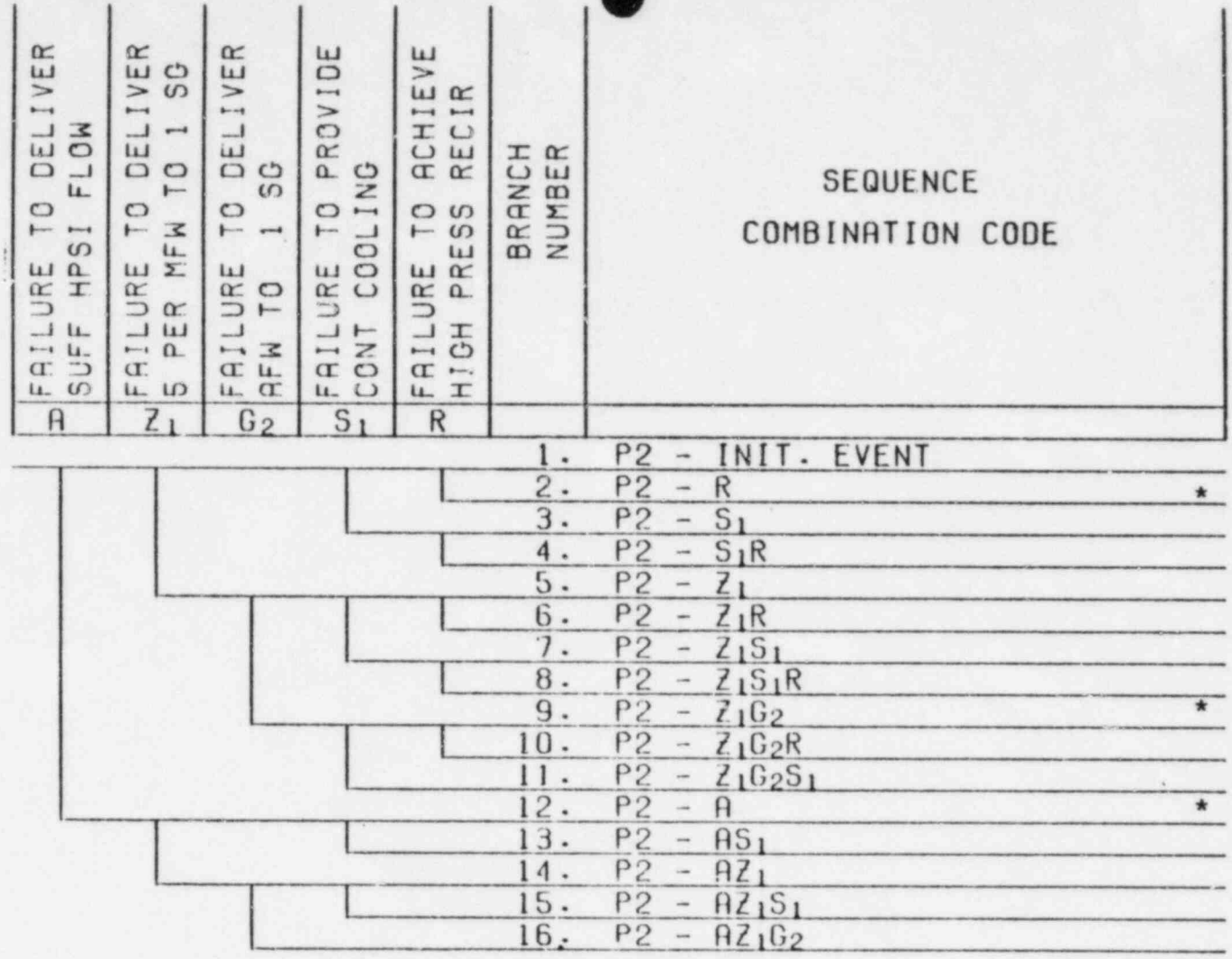


FIGURE 5.3.4.2-1

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 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.

5.3.4.3 Spurious or Transient Induced PORV LOCA Event Tree

The event tree for Spurious or Transient Induced 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 Core Heat Removal is high pressure

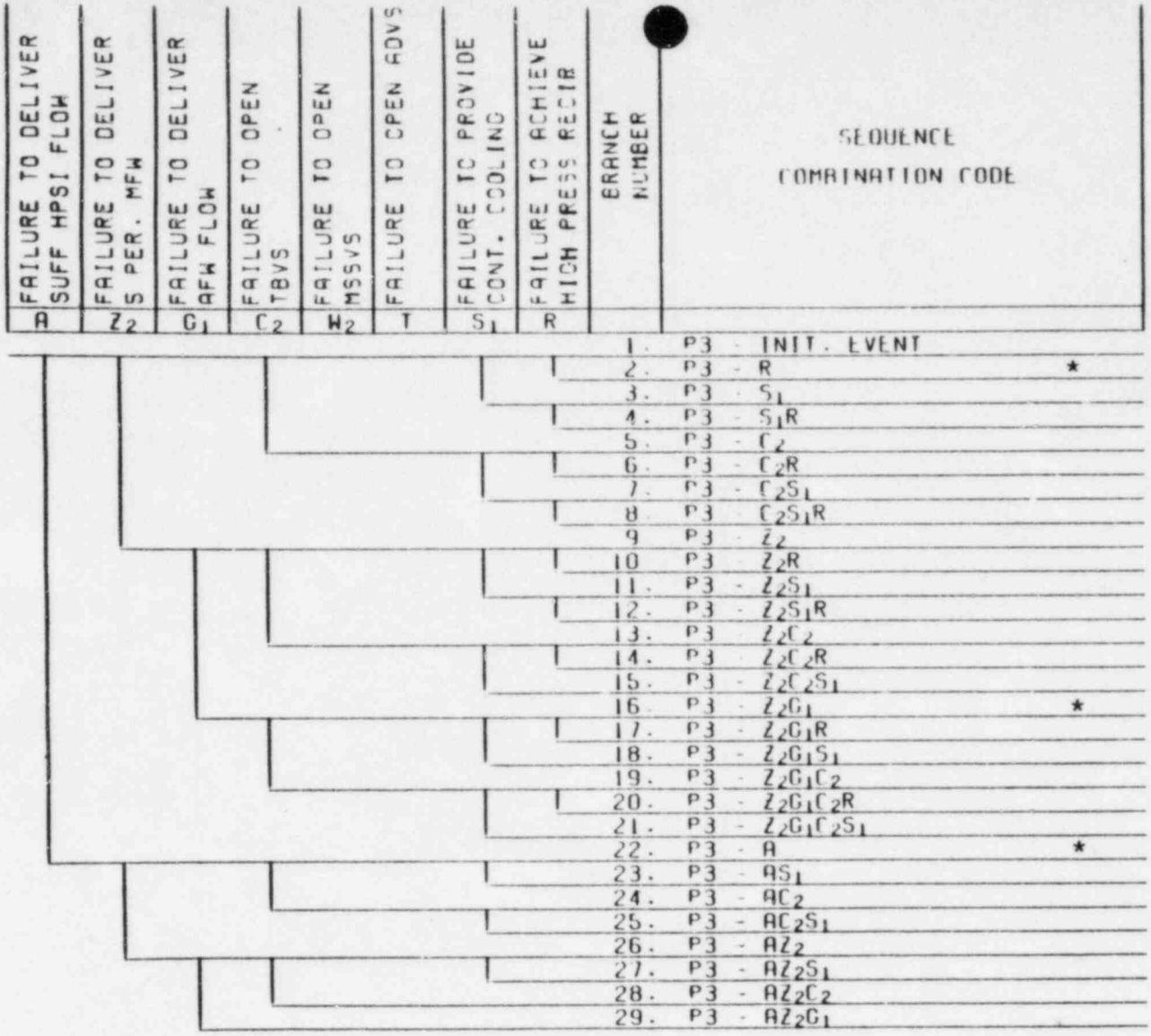


FIGURE 5.3.4.3-1
SPURIOUS OR TRANSIENT INDUCED PORV LOCA SYSTEMIC EVENT TREE

* The above minimal core damage sequences are identical for Spurious PORV LOCA and Transient Induced PORV LOCA. These 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 inSection 2.2.1.

recirculation and with RCS Heat Removal are containment sprays, 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 error induced or spurious openings of either PORV flow path times 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.

P4 The initiating event is defined as the frequency of high RCS pressure transient induced openings of the PORV flowpaths times the probability that the flowpaths 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. 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 either steam generator. 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 — 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 not opening at least one of the ten safety valves associated with each steam generator. 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 at least one of the four atmospheric dump valve flow paths to relieve secondary steam to the atmosphere. The atmospheric dump valves are used to dump secondary steam to the atmosphere when the turbine bypass 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 Cooling Water Systems 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 PVNGS 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 (<1700 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 the Refueling Water Tank (RWT) 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.

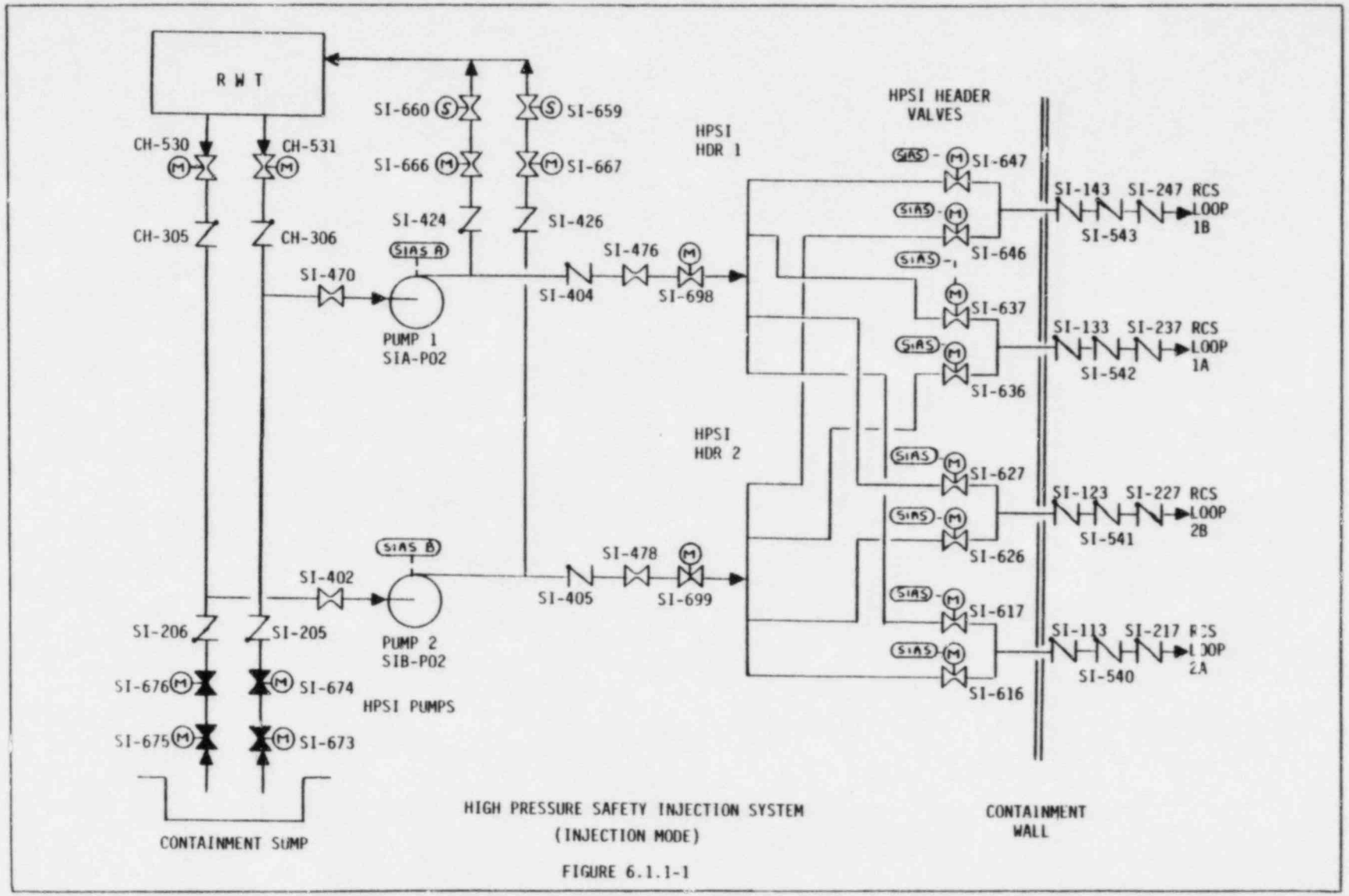

R W T
CH-530
CH-531
CH-305
CH-306
SI-660
SI-659
SI-666
SI-667
SI-424
SI-426
SIAS A
SI-470
SI-476
SI-404
SI-698
PUMP 1
SIA-P02
HPSI HEADER VALVES
HPSI HDR 1
SIAS
SI-647
SI-646
SI-637
SI-636
SI-143
SI-247 RCS LOOP 1B
SI-543
SI-133
SI-237 RCS LOOP 1A
SI-542
HPSI HDR 2
SI-627
SI-626
SI-617
SI-616
SI-123
SI-227 RCS LOOP 2B
SI-541
SI-113
SI-217 RCS LOOP 2A
SI-540
SIAS B
SI-402
SI-478
SI-405
SI-699
PUMP 2
SIB-P02
SI-206
SI-205
SI-676
SI-674
SI-675
SI-673
HPSI PUMPS
CONTAINMENT SUMP
HIGH PRESSURE SAFETY INJECTION SYSTEM
(INJECTION MODE)
CONTAINMENT WALL

FIGURE 6.1.1-1

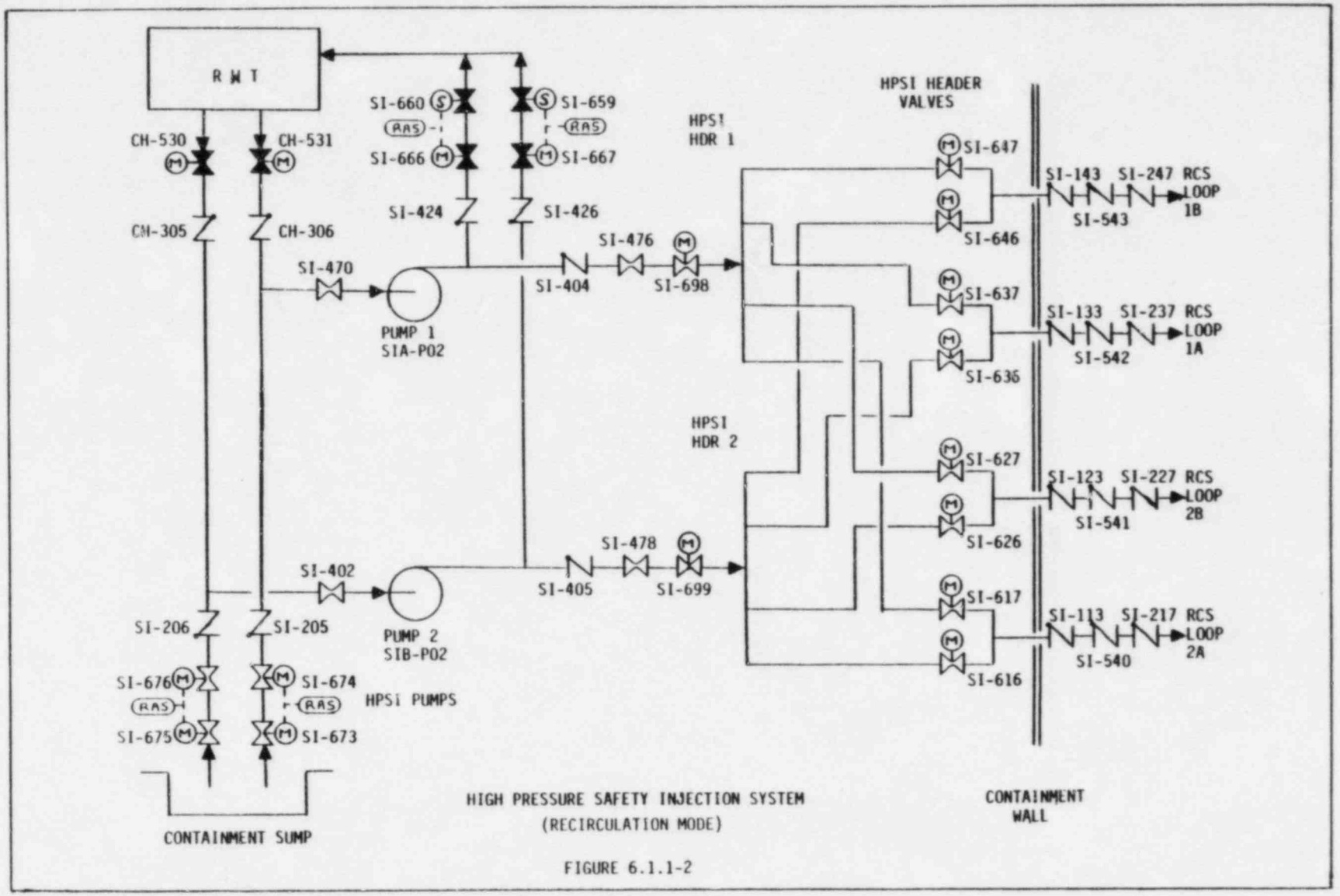

R W T
CH-530
CH-531
CH-305
CH-306
SI-660
SI-659
RAS
SI-666
SI-667
SI-424
SI-426
SI-470
SI-476
SI-404
SI-698
PUMP 1
SIA-P02
HPSI HEADER VALVES
HPSI HDR 1
SI-647
SI-646
SI-637
SI-636
SI-143
SI-247
SI-543
RCS LOOP 1B
SI-133
SI-237
SI-542
RCS LOOP 1A
HPSI HDR 2
SI-627
SI-626
SI-123
SI-227
SI-541
RCS LOOP 2B
SI-478
SI-405
SI-699
SI-402
SI-206
SI-205
PUMP 2
SIB-P02
SI-617
SI-616
SI-113
SI-217
SI-540
RCS LOOP 2A
SI-676
SI-674
SI-675
SI-673
HPSI PUMPS
CONTAINMENT SUMP
HIGH PRESSURE SAFETY INJECTION SYSTEM
(RECIRCULATION MODE)
CONTAINMENT WALL

FIGURE 6.1.1-2

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

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

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. The only operator action considered was manual backup of SIAS from the control room.

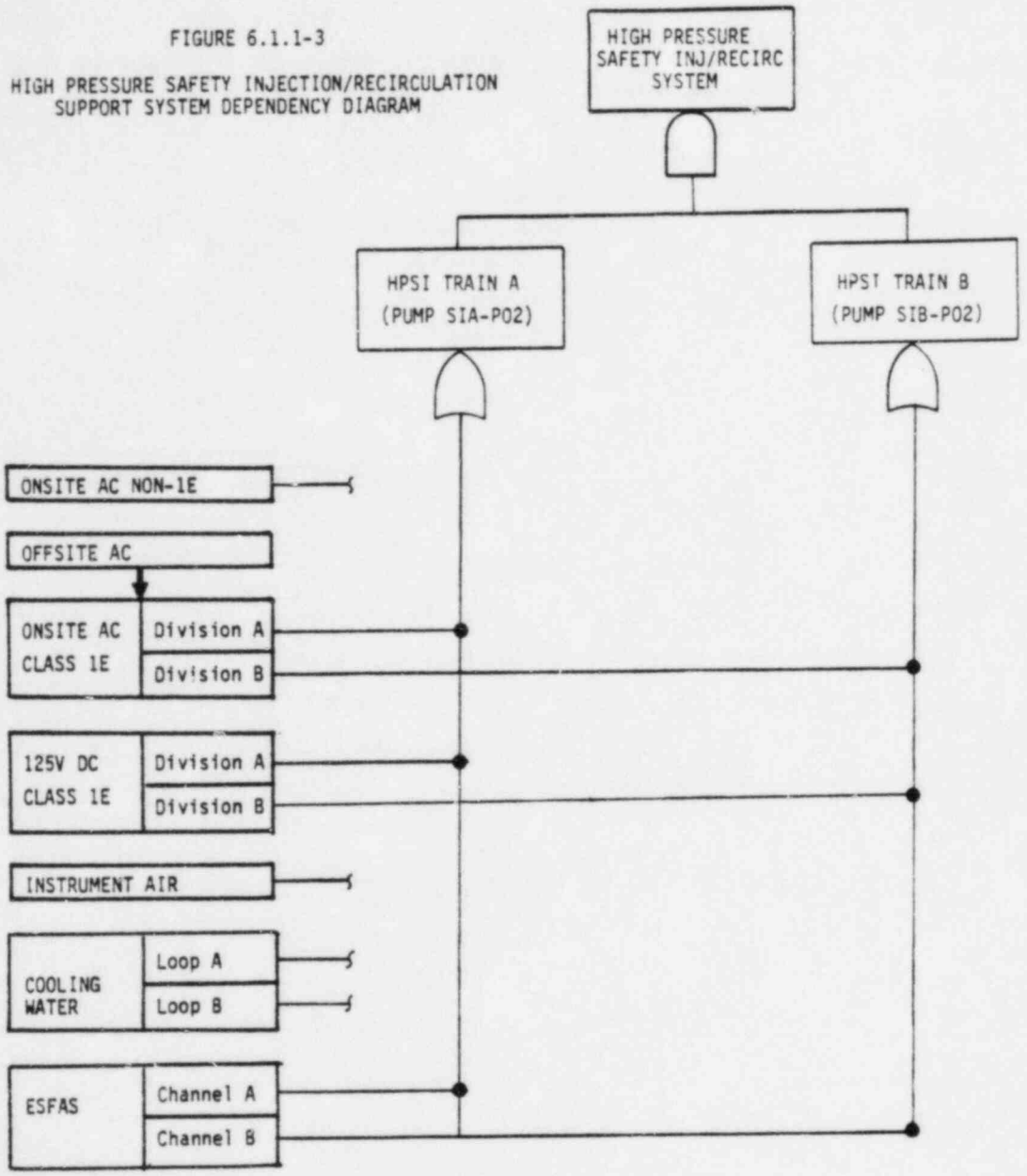
   The operator is allowed 20 minutes to backup the SIAS.

4. The containment sump isolation valves are closed.

5. The HPSI system is tested at start-up and once each eighteen months. If pump maintenance is required, manual valves SI-470, SI-476, SI-402 or SI-478 may be closed and inadvertently left in the wrong position. The probability of this maintenance error is included in the analysis. However, all other normally open valves are required to remain open during plant operation. Therefore, the only failure mode considered for these valves is plugging.

FIGURE 6.1.1-3

HIGH PRESSURE SAFETY INJECTION/RECIRCULATION
SUPPORT SYSTEM DEPENDENCY DIAGRAM



6. It is assumed that components on train A receive SIAS-A and components on train B receive SIAS-B.

7. Cooling Water Systems are not required for successful HPSI pump operation.

8. Since maintenance can only be performed on one HPSI pump during plant operation, unavailability contributions due to pump maintenance are included only for HPSI pump SIA-P02.

9. Motor operated valves CH-530 CH-531
SI-666 SI-667
SI-698 SI-699
are all FAI (fail as is) and are normally open, therefore, loss of power to these components is not considered in the fault tree model.

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. Both HPSI pumps are assumed to be operating.

4. The generation of the RAS closes the mini-flow line series isolation valves. Failure of these valves to close does not significantly impact HP recirculation flow; therefore, failure to isolate the miniflow lines is not considered in the fault tree model.

5. The RWT isolation valves are manually closed from the control room. Failure to close these valves does not impede recirculation flow; therefore, these valves are not included in the fault tree model.

6. If loss of offsite power occurs as an initiating event or as a result of turbine trip, power is restored prior to realignment for high pressure recirculation.

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). It was noted that the unreliability of the HPSI system became a significant

contributor 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 Five 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 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 dominant 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 PVNGS 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	5.4E-5	10
Two	Fail to Deliver Sufficient HPSI Flow-System Unavailability given offsite power is unavailable at the time of the initiating event	2.3E-3	6
Three	Failure to Deliver Sufficient HPSI Flow - System Unavailabilty given PORV LOCA	2.4E-4	6
Four	Fail to Deliver Sufficient HPSI Flow-System Unavailability	5.9E-5	8
Five	Fail to Maintain Sufficient HPSI Flow-System Unreliability at 8 hours given offsite power is unavailable at the time of the initiating event	9.2E-4	16
Six	Failure to Achieve HP Recirculation-System Unavailability	7.1E-5	23
Seven	Fail to Throttle HPSI	2.5E-1	3

TABLE 6.1.3-2

DOMINANT CUTSETS FOR PVNGS HPSI SYSTEM

Case Number	Cutset	Description	% of Total Failure Probability
One	1. FSSR2003 FSSR2004 FSSO2005	SIAS A not generated and SIAS B not generated and Operator fails to generate SIAS	15%
	2. HBCB2093 HBCB2100	HPSI Pump 1 Breaker fails to close and HPSI Pump 2 Breaker fails to close	4.8%
	3. HBCB2093 HPMJ2101	HPSI Pump 1 Breaker fails to close and HPSI Pump 2 fails to start	4.8%
	4. HPMJ2094 HBCB2100	HPSI Pump 1 fails to start and HPSI Pump 2 Breaker fails to close	4.8%
	5. HPMJ2094 HPMJ2101	HPSI Pump 1 fails to start and HPSI Pump 2 fails to start	4.8%
Two	1. EDDJ2816 EDDJ2817	DG E-PEA-G01 fails to start and DG E-PEB-G02 fails to start	65%
	2. EBTB2820 EDDJ2817	DG E-PEA-G01 Breaker fails to close and DG E-PEB-G02 fails to start	2.2%
	3. EDDJ2816 EBTB2821	DG E-PEA-G01 fails to start and DG E-PEB-G02 Breaker fails to close	2.2%
Three	1. EBGP2680 EDDJ2816 EDDJ2817	Spurious grid collapse and DG E-PEA-G01 fails to start and DG E-PEB-G02 fails to start	34%
	2. EBGP2680 EDDJ2816 EDDK2819	Spurious grid collapse and DG E-PEA-G01 fails to start and DG E-PEB-G02 fails to operate	9%
	3. EBGP2680 EDDJ2817 EDDK2818	Spurious grid collapse and DG E-PEB-G02 fails to start and DG E-PEA-G01 fails to operate	9%

TABLE 6.1.3-2
(Continued)
DOMINANT CUTSETS FOR PVNGS HPSI SYSTEM

Case Number	Cutset	Description	% of Total Failure Probability
Four	1. FSSR2003 FSSR2004 FSSO2005	SIAS A not generated and SIAS B not generated and Operator fails to generate SIAS	14%
	2. HBCB2093 HBCB2100	HPSI Pump 1 Breaker fails to close and HPSI Pump 2 Breaker fails to close	4.3%
	3. HBCB2093 HPMJ2101	HPSI Pump 1 Breaker fails to close and HPSI Pump 2 fails to start	4.3%
	4. HPMJ2094 HBCB2100	HPSI Pump 1 fails to start and HPSI Pump 2 Breaker fails to close	4.3%
	5. HPMJ2094 HPMJ2101	HPSI Pump 1 fails to start and HPSI Pump 2 fails to start	4.3%
Five	1. EDDJ2816 EDDK2819	DG E-PEA-G01 fails to start and DG E-PEB-G02 fails to operate	21%
	2. EDDJ2817 EDDK2818	DG E-PEB-G02 fails to start and DG E-PEA-G01 fails to operate	21%
	3. EDDK2818 EDDK2819	DG E-PEA-G01 fails to operate and DG E-PEB-G02 fails to operate	11%
Six	1. FSRR2015 FSRR2016 FSRO2017	RAS A not generated and RAS B not generated and Operator fails to generate RAS	11%
	2. HVMA2324 HVMA2328	Containment Sump Valve SI-673 FTO and Containment Sump Valve SI-676 FTO	4.0%
	3. HVMA2324 HVMA2330	Containment Sump Valve SI-673 FTO and Containment Sump Valve SI-675 FTO	4.0%

TABLE 6.1.3-2
(Continued)
DOMINANT CUTSETS FOR PVNGS HPSI SYSTEM

Case Number	Cutset	Description	% of Total Failure Probability
	4. HVMA2326	Containment Sump Valve SI-674 FTO and	4.0%
	HVMA2328	Containment Sump Valve SI-676 FTO	
	5. HVMA2326	Containment Sump Valve SI-674 FTO and	4.0%
	HVMA2330	Containment Sump Valve SI-675 FTO	
Seven	1. HZZ02338	Operator fails to throttle HPSI	100%

6.2 AUXILIARY SPRAY SYSTEM

6.2.1 System Description

Figure 6.2.1-1 provides a schematic of the Auxiliary Spray System. To initiate auxiliary spray, the spray valves HV-203 and HV-205 are manually opened from the control room. The charging line valves PVD-240 is then closed to divert flow to the pressurizer. Figure 6.2.1-2 provides a schematic of the charging supply modelled in the fault tree.

Figure 6.2.1-3 provides the Auxiliary Spray Support System dependency diagram.

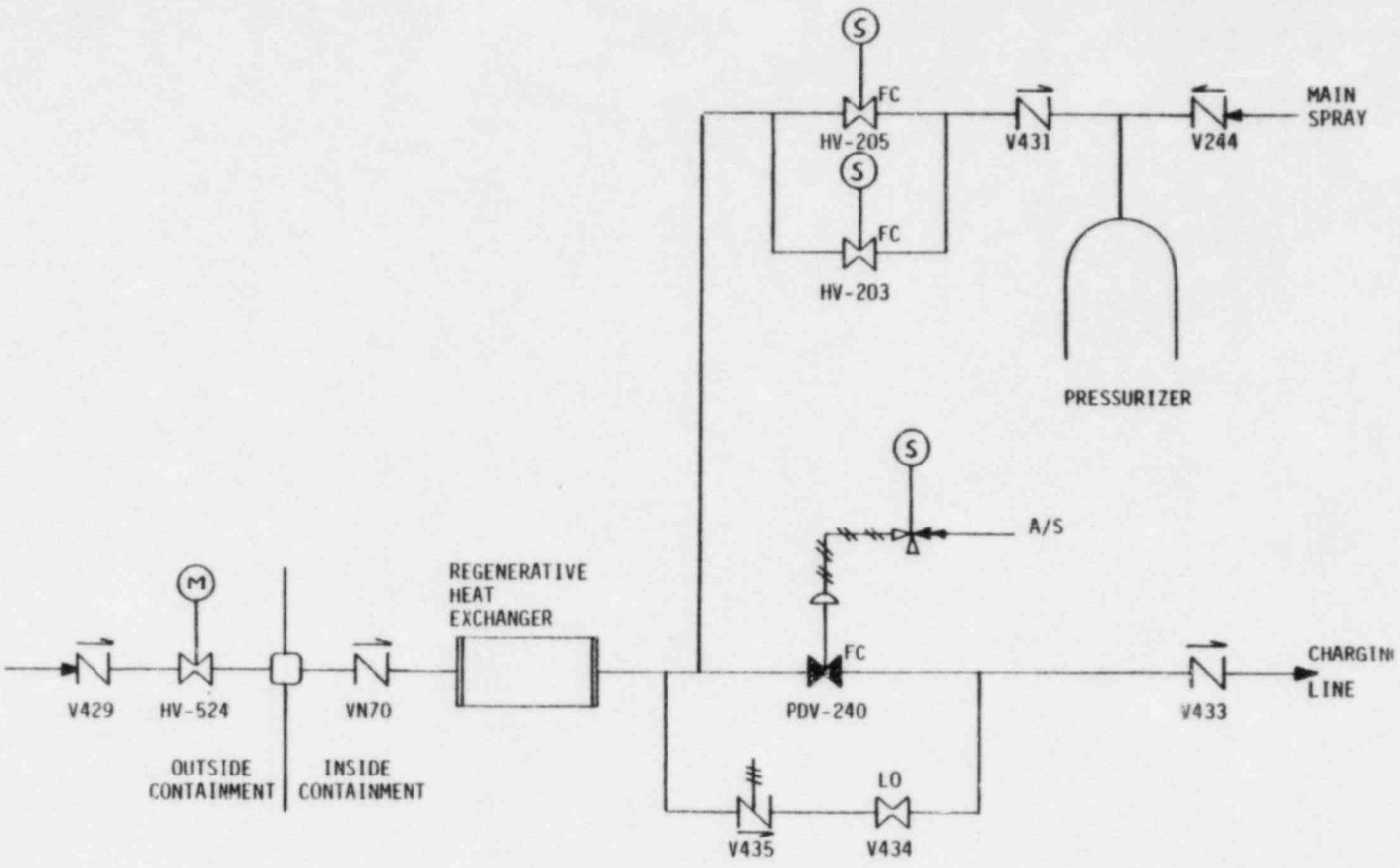
6.2.2 Assumptions

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

1. System failure is defined as the inability to deliver sufficient auxiliary spray to the pressurizer. Sufficient flow is defined as the flow from at least one charging pump.

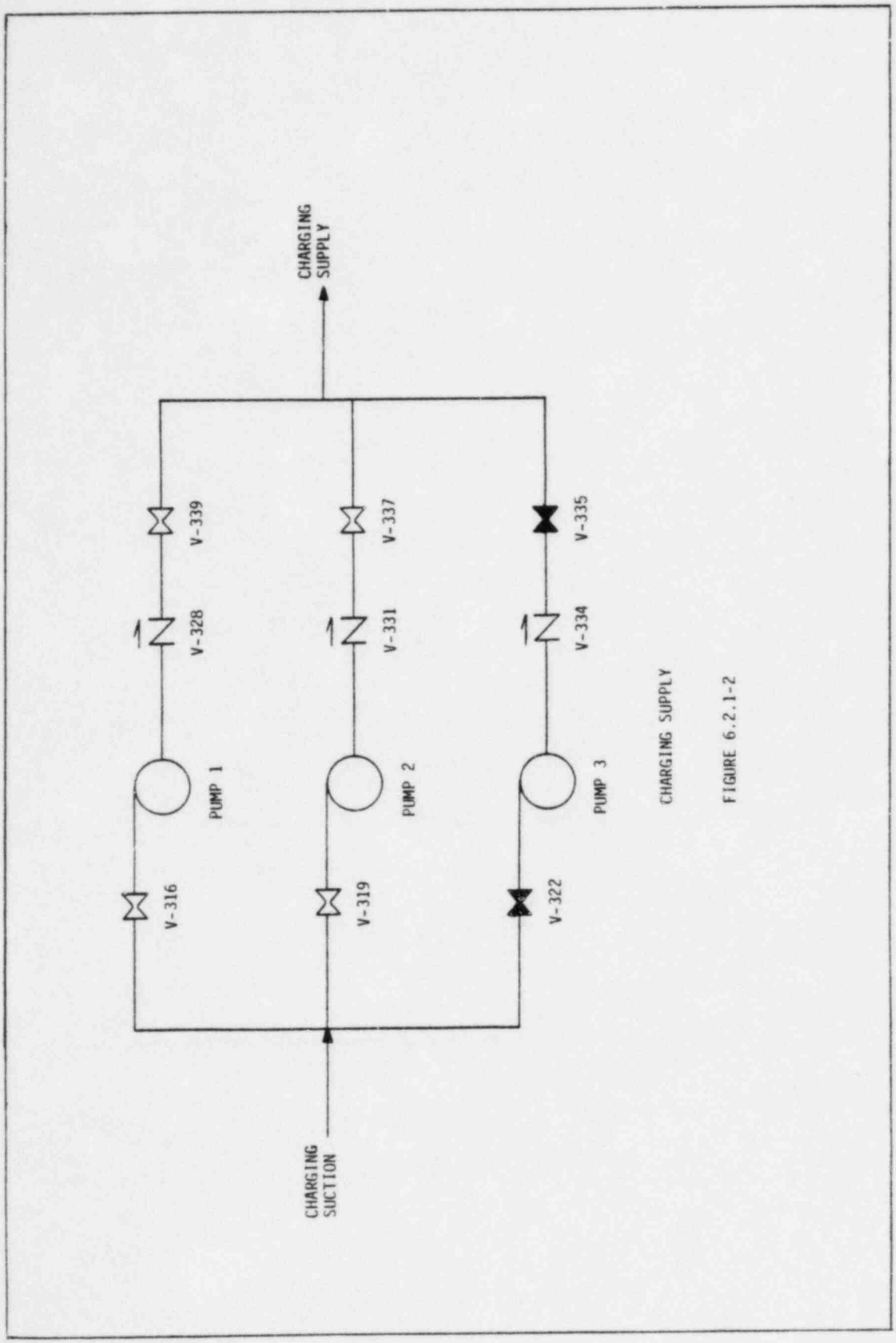
2. The operator is allowed 30 min. to establish auxiliary spray flow from the time auxiliary spray flow is first desired. The operator action to initiate the spray flow is defined as opening of the two auxiliary spray valves (HV-205 and HV-203) and closing of the charging line valve (PVD-240).

3. It is assumed that none of the auxiliary spray flow is diverted back through the main spray valves to the RCS cold legs. This is because the check valve (V244) in the main spray line will prevent any back flow. Also, the main spray valves provide a back-up to the check valves as they are normally closed and are of failed closed (FC) design.



AUXILIARY SPRAY SYSTEM

FIGURE 6.2.1-1

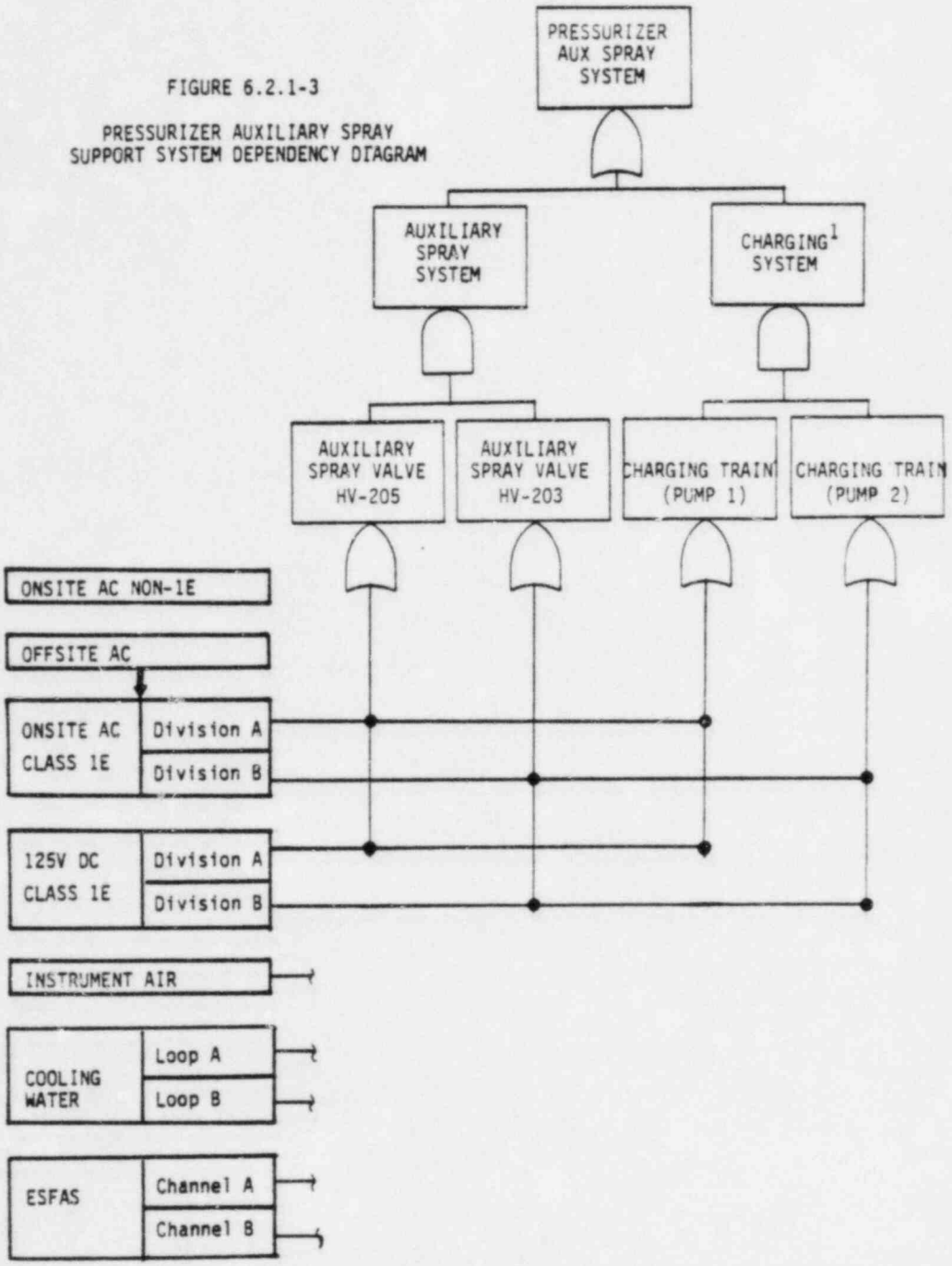


CHARGING SUPPLY

FIGURE 6.2.1-2

FIGURE 6.2.1-3

PRESSURIZER AUXILIARY SPRAY
SUPPORT SYSTEM DEPENDENCY DIAGRAM



[1]Charging pump 3 is assumed to be down for maintenance.

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

   a. Charging pumps 1 and 2 are operating at the time of transient.

   b. Charging pump 3 is down for maintenance.

5. Only one auxiliary spray valve (HV-205 or HV-203) is needed to provide sufficient spray flow.

6. Spring loaded check valve V435 is not in the failed open position at the time the auxiliary flow is initiated. It is also assumed that after the auxiliary spray is initiated, the pressure drop across the check valve remains less than the setpoint (to open the check valve).

7. The spray valves HV-205 and HV-203 and the charging line valve PDV-240 fail close on loss of power. The normally open motor operated charging line valve HV-524 will remain open on loss of power.

8. On loss of offsite power, the charging pumps require operator action to load them on the diesel generators.

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 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. 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 PVNGS 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	3.8E-3	4
Two	Fail to Deliver Auxiliary Spray Flow-System Unavailability given offsite power is unavailable at the time of the initiating event	1.1E-2	3
Three	Fail to Deliver Auxiliary Spray Flow-System Unavailability given loss of MFW and AFW	4.2E-3	3

TABLE 6.2.3-2

DOMINANT CUTSETS FOR PVNGS AUXILIARY SPRAY SYSTEM

Case Number	Cutset	Description	% of Total Failure Probability
One	1. PVSO2470	Operator fails to initiate aux. sprays	62%
	2. UVDB2477	Charging line valve PDV-240 fails to close (Mechanical Malfunction)	35%
	3. PVCA2474	Aux. spray line check valve V431 fails to open (Mechanical Malfunction)	3%
Two	1. PVSO2471	Operator fails to load charging pumps on Diesel Generator.	37%
	2. PVSO2470	Operator fails to initiate aux. sprays	27%
	3. UVDB2477	Charging line valve PDV-240 fails to close (Mechanical Malfunction)	15%
	4. EDDJ2816	Diesel Generator E-PEA-GO1 fails to start and	13%
	EDDJ2817	Diesel Generator E-PEB-GO2 fails to start	
Three	1. PVSO2470	Operator fails to initiate aux. sprays.	58%
	2. UVDB2477	Charging line valve PDV-240 fails to close (Mechanical Malfunction)	32%
	3. EBGP2680	Spurious grid collapse and	
	PVSO2471	Operator fails to load charging pumps on diesel generators and	4%

6.3 CONTAINMENT SPRAY SYSTEM

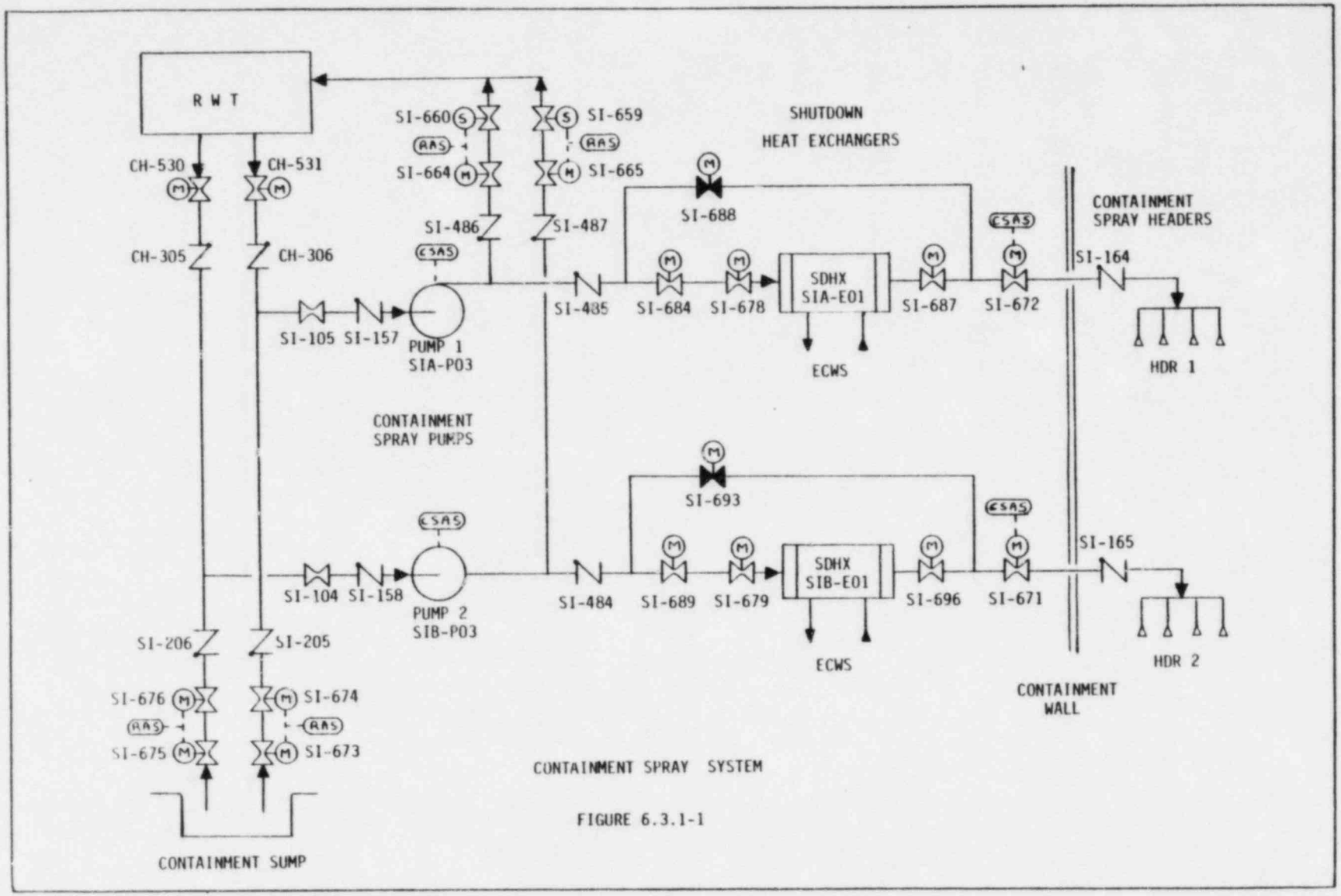
6.3.1 System Description

The objectives of the Containment Spray 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. This cooling system also serves to limit offsite radiation levels by reducing the pressure differential between the containment atmosphere and the external environment. The Containment Spray System consists of two 100% capacity trains.

The Containment Spray System utilizes the refueling water tank, 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) on high containment pressure. The CSAS starts the containment spray pumps and opens the spray control valves to the containment. The Essential Cooling Water System (ECWS) and the Essential Spray Pond System (ESPS) are required to provide coolant to the shutdown heat exchangers and are actuated by the Safety Injection Actuation Signal (SIAS) on high containment pressure. The SIAS starts the ECW pumps and the ESP pumps.

During the injection mode the actuated spray pumps take suction from the refueling water tank and discharge through the shutdown heat exchangers 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 10% of its minimum allowed volume, a recirculation actuation signal (RAS) is generated. Generation of RAS opens the containment sump isolation valves to allow



CONTAINMENT SPRAY SYSTEM

FIGURE 6.3.1-1

automatic transfer of the containment spray pumps suction from the refueling water tank to the containment sump. Transfer of pump suction ensures that containment cooling is maintained.

The RAS also closes the containment spray pumps miniflow isolation lines.

The containment heat removal support system dependency diagram is provided in Figure 6.3.1-2.

6.3.2 Assumptions

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

1. System failure is defined as the inability to remove sufficient containment heat. Sufficient Containment heat removal is provided by one 100% capacity CSS train.

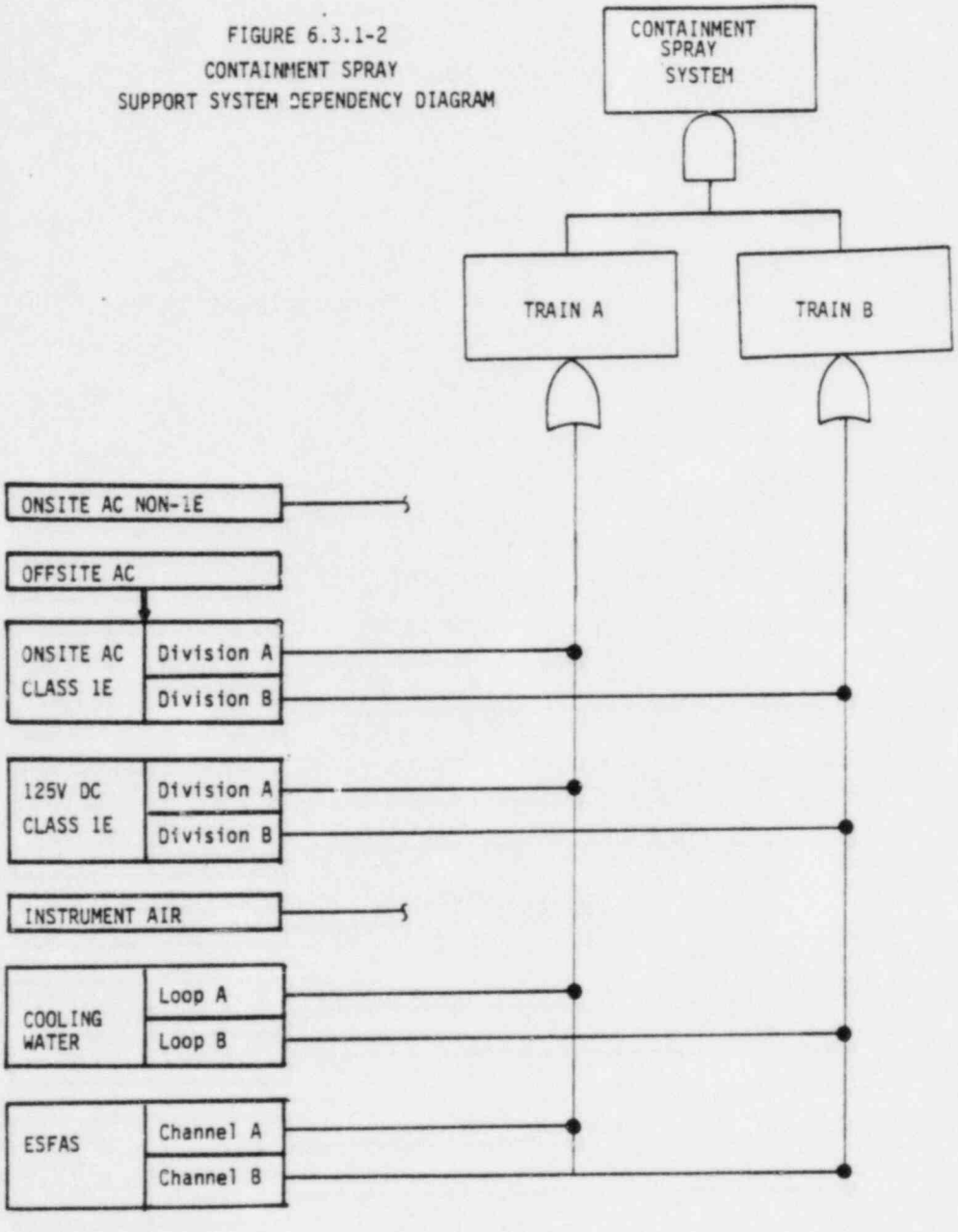
2. Isolation of the spray pump mini-flow lines during injection mode could result in dead headed operation and damage to the pumps.

3. The only operator actions considered were manual backup of the CSAS, SIAS and RAS from the control room.

4. The RAS closes the containment spray pumps mini-flow line series isolation valves at 10% level in the RWT. Failure of these valves to close does not significantly impact the containment spray recirculation mode; therefore, failure to isolate the mini-flow lines is not considered in the fault tree model.

5. Since maintenance can only be performed on one CS pumps during plant operation, unavailability contributions due to pump maintenance are included only for CS pump SIA-P03.

FIGURE 6.3.1-2
CONTAINMENT SPRAY
SUPPORT SYSTEM DEPENDENCY DIAGRAM



6.3.3 Results

The fault tree logic diagram for Failure of Containment Sprays was used to evaluate the probability of failing to provide sufficient containment heat removal for the PORV LOCA event trees. The result is presented as Case One in Table 6.3.3-1. For the LOHS with Feed and Bleed Operation event tree, the Containment Spray System logic diagram was also 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 and the dependencies which exist between these three systems have been incorporated into the Containment Spray System failure probability. These results are presented as Case Two 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 PVNGS CONTAINMENT SPRAY SYSTEM

Case Number	Description	Failure Probability (Median Value)	Error Factor
One	Failure of Containment Sprays - System Unavailability	1.5E-3	18
Two	Failure of Containment Sprays - System Unavailability given loss of MFW and loss of AFW	2.7E-3	14

TABLE 6.3.3-2

DOMINANT CUTSETS FOR PVNGS CONTAINMENT SPRAY SYSTEM

Case Number		Cutset	Description	% of Total Failure Probability
One	1.	FSSR2003	SIAS A not generated and	.88%
		FSSR2004	SIAS B not generated and	
		FSS02005	Operator fails to generate SIAS	
	2.	FSAR2009	CSAS A not generated and	.88%
		FSAR2010	CSAS B not generated and	
		FSA02011	Operator fails to generate CSAS	
	3.	FSRR2015	RAS A not generated and	.88%
		FSRR2016	RAS B not generated and	
		FSR02017	Operator fails to generate RAS	
Two	1.	EBGP2680	Spurious Grid collapse and	6.8%
		EDDJ2816	DG E-PEA-G01 fails to start and	
		EDDJ2817	DG E-PEB-G02 fails to start	
	2.	EBGP2680	Spurious Grid collapse and	5.5%
		EDDJ2816	DG E-PEA-G01 fails to start and	
		EDDK2819	DG E-PEB-G02 fails to operate	
	3.	EBGP2680	Spurious Grid collapse and	5.5%
		EDDJ2817	DG E-PEB-G02 fails to start and	
		EDDK2818	DG E-PEA-G01 fails to operate	
	4.	EBGP2680	Spurious Grid collapse and	4.4%
		EDDK2818	DG E-PEA-G01 fails to operate	
			and	
		EDDK2819	DG E-PEB-G02 fails to operate	

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 either PORV flowpath following a tube rupture in one steam generator. The unaffected steam generator is available to remove RCS heat.

- Spurious or Transient Induced PORV LOCA. This type of PORV LOCA refers to the opening of either or both PORV flowpaths. For the manual PORV design, this type of PORV LOCA includes error (test, maintenance, or operator) induced openings. For the automatic PORV design, this type of PORV LOCA includes high RCS pressure transient induced openings. 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 was used along with an assumed valve testing frequency that varies from two weeks to quarterly to evaluate the Spurious PORV LOCA (manual design) occurrence frequency.

In order to evaluate the unavailability of the PORVs 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 Power Operated Relief Valve (PORV) design for PVNGS is presented in Figure 6.4.1-1. Both the manual and the automatic PORV designs considered feature two 50% capacity flow paths. Each path contains a motor operated block valve and a PORV. For the manual PORV design, the motor operated block valves and the PORVs are closed during power operation. 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". For the manual PORV design, the PORVs are not opened by signals that are generated automatically, therefore, they do not prevent or minimize challenges to the primary safety valves. For the automatic PORV design, the motor operated block valves are opened and the PORVs are closed during power operation. In the event of a high RCS pressure transient the PORVs open automatically to 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:

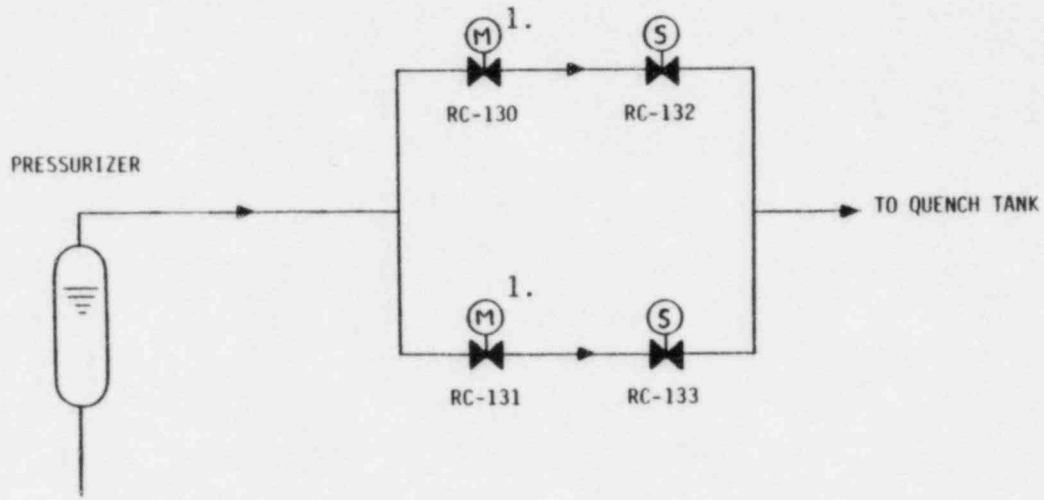
1. Both PORV flowpaths are required following a loss of secondary heat sink event.

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 may be required to establish or terminate flow through the PORVs.



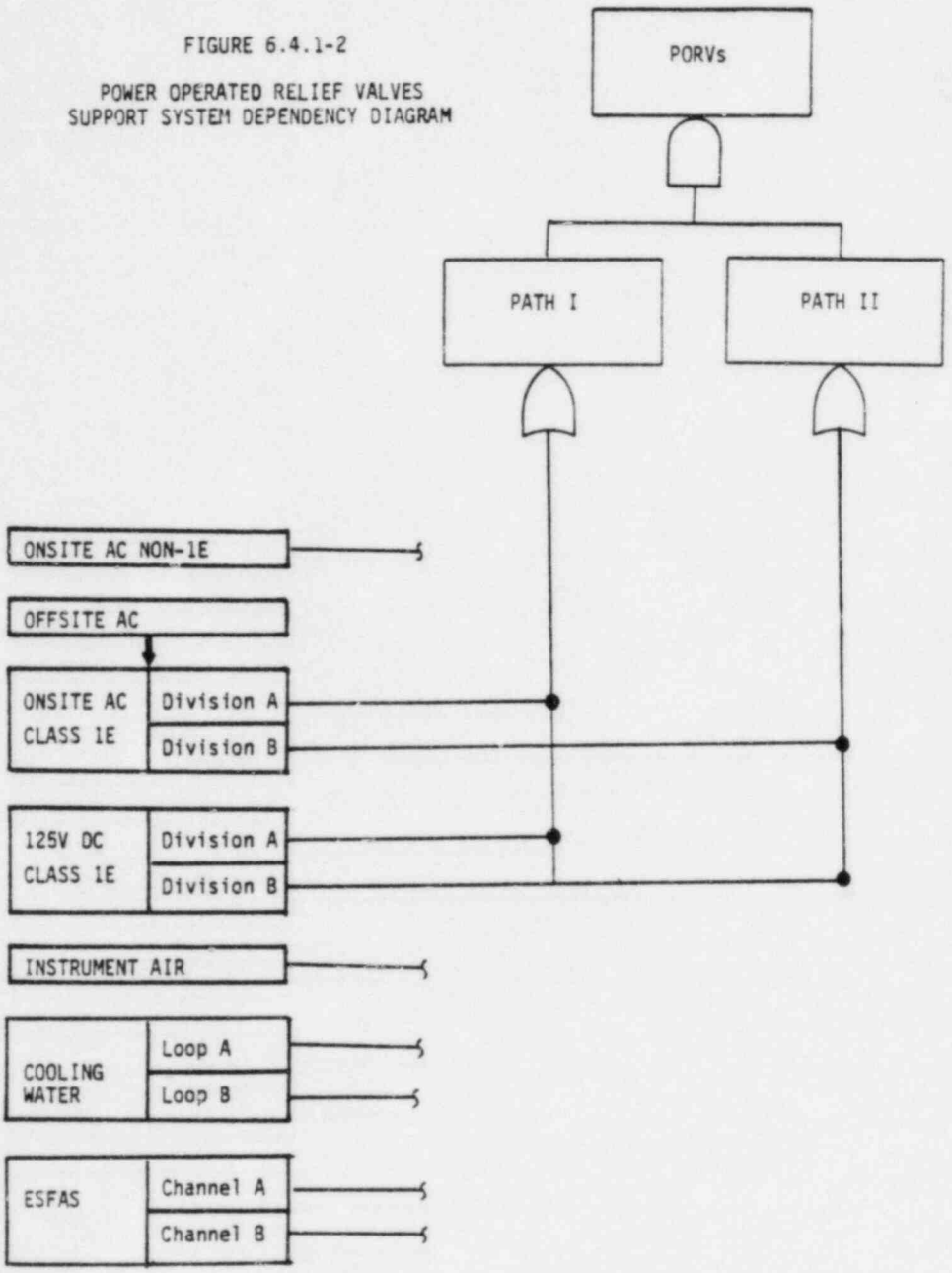
POWER OPERATED RELIEF VALVES

FIGURE 6.4.1-1

[1] For the manual design, plant operates with block valves closed and for the automatic design, plant operates with block valves open.

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 E-PHA-M33 and E-PHB-M34 respectively.

3. PORV RC-132 and RC-133 are loaded on 125 VDC buses E-PKA-M41 and E-PKV-M42 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 or Transient Induced 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).

- 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 best estimate ratio.

TABLE 6.4.3-1

INITIATING EVENT FREQUENCIES AND FAILURE PROBABILITIES FOR PVNGS PORVs

Case Number	Description	Failure Probability (Median Value)	Error Factor
One	PORV LOCA Following LOHS - Initiating Event Frequency	1.8E-5	16
Two	PORV LOCA Following SGTR - Initiating Event Frequency	1.3E-4	7
Three	Spurious or Transient Induced PORV LOCA - Initiating Event Frequency		
	(a) Manual Design	3.2E-5[1]	16
	(b) Automatic Design	5.0E-3[1]	13
Four	Failure to Establish Flow through One PORV - System Unavailability given offsite power is available at the time of the initiating event	1.1E-3	4
Five	Failure to Establish Flow through One PORV - System Unavailability	1.1E-3	4
Six	Failure to Establish Flow through One PORV - System Unavailability given offsite power is unavailable at the time of the initiating event	3.5E-3	4

1. This value excludes challenges to the PORVs due to malfunction of the turbine runback feature. Operating experience shows that C-E NSSS supplied plants with turbine runback feature experience more challenges to the PORVs. Therefore, the affected plants are currently operating with the turbine runback feature overridden. If challenges to the PORVs due to malfunction of the turbine runback feature were included, the PORV LOCA initiating event frequently would increase by approximately 15%.

TABLE 6.4.3-2

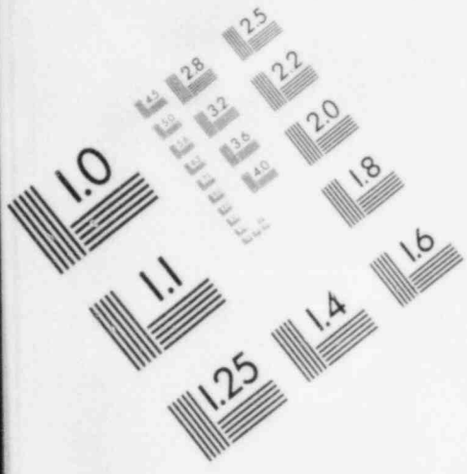
DOMINANT CUTSETS FOR PVNGS PORVS

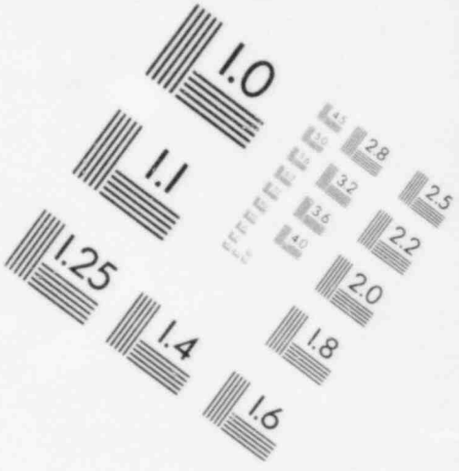
Case Number		Cutset	Description	% of Total Failure Probability
One	1.	ZZZZ2928 ZZZZ2927 VVX02937	Loss of MFW and Loss of AFW and Operator fails to isolate the PORV flow paths	99%
Two	1.	ZZZZ2926 VVX02937	Tube rupture in one SG and Operator fails to isolate the PORV flow paths	99%
Three (a) Manual Design	1.	VVMV2945 ZZZZ2936 VVX02938	Pre-existing error on valve RC-133 and Valve RC-131 opens for testing and Operator fails tc isolate the PORV flow path	23%
	2.	VVMV2944 ZZZZ2934 VVX02938	Pre-existing error on valve RC-131 and Valve RC-133 opens for testing and Operator fails to isolate the PORV flow path	23%
	3.	VVMV2940 ZZZZ2932 VVX02938	Pre-existing error on valve RC-132 and Valve RC-130 opens for testing and Operator fails to isolate the PORV flow path	23%
	4.	VVMV2939 ZZZZ2930 VVX02938	Pre-existing error on valve RC-130 and Valve RC-132 opens for testing and Operator fails to isolate the PORV flow path	23%
(b) Automatic Design	1.	ZZZZ2979 VVMS2948	Valve RC-133 opens spuriously and Valve RC-131 electrical malfunction	43%
	2.	ZZZZ2978 VVMS2943	Valve RC-132 opens spuriously and Valve RC-130 electrical malfunction	43%

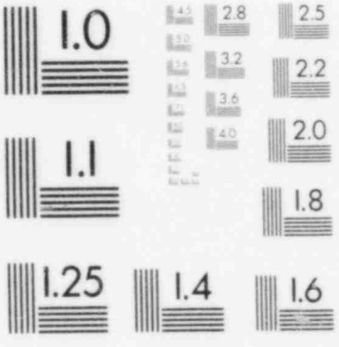
TABLE 6.4.3-2
(continued)
DOMINANT CUTSETS FOR PVNGS PORVS

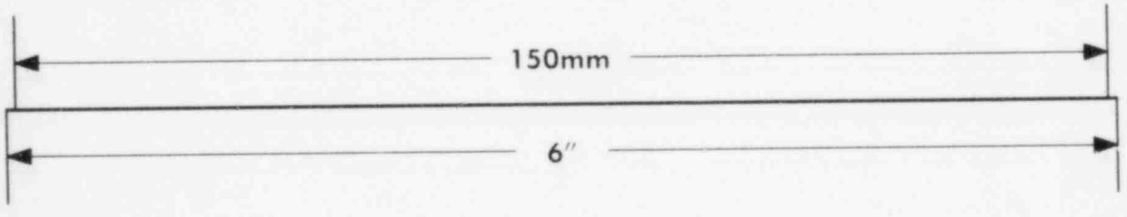
Case Number	Cutset	Description	% of Total Failure Probability
Four	1. VVZO2550	Operator fails to open one PORV and the associated block valve	>99%
Five	1. VVZO2550	Operator fails to open one PORV and the associated block valve	>99%
Six	1. VVZO2550	Operator fails to open one PORV and the associated block valve	43%
	2. EDDJ2816 EDDJ2817	DG E-PEA-G01 fails to start and DG E-PEB-G02 fails to start	39%
	3. VVMA2552	Valve RC-131 fails to open or the associated breaker fails to close and	2.6%
	EDDJ2816	DG E-PEA-G01 fails to start	
	4. VVMA2551	Valve RC-130 fail to open or the associated breaker fails to close and	2.6%
	EDDJ2817	DG E-PEB-G02 fails to start	

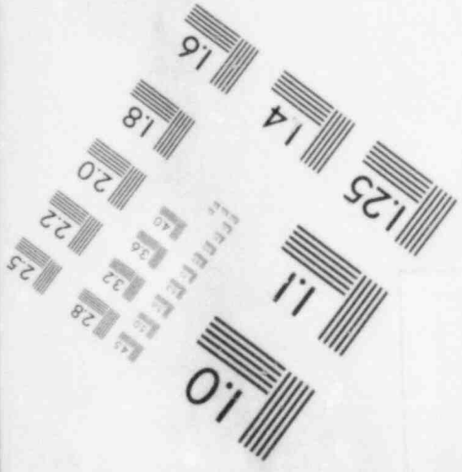
IMAGE EVALUATION TEST TARGET (MT-3)

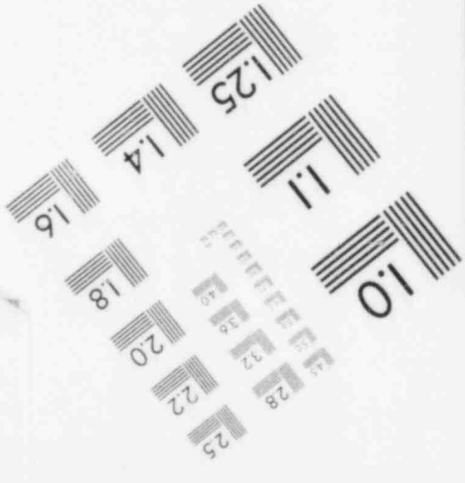












6.5 PRIMARY FEED AND BLEED SYSTEM

6.5.1 System Description

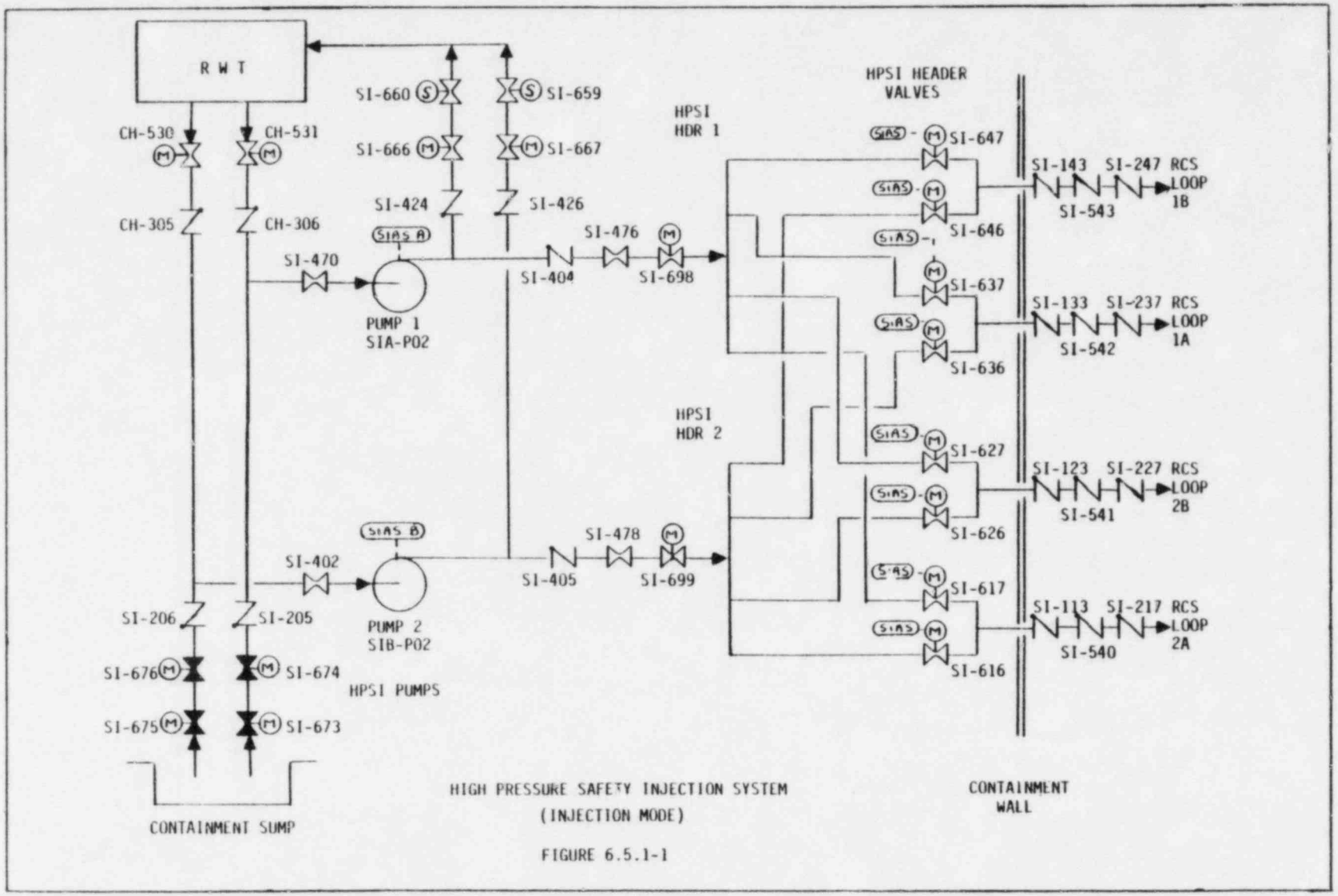
A conceptual Primary Feed and Bleed System for PVNGS consists of Power Operated Relief Valves (PORVs), the High Pressure Safety Injection System and the Charging System. A schematic of the PORVs is presented in Figure 6.5.1-2. It consists of two trains of a power-operated relief valve and a motor-operated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

A schematic of the PVNGS 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 the Refueling Water Tank (RWT) and discharge through the eight HPSI header isolation valves via two 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 of charging flow to the RCS loops is presented in Figure 6.5.1-3. The charging pumps take suction from the volume control tank and inject into the RCS during plant steady state operations. Normally two pumps are operating.

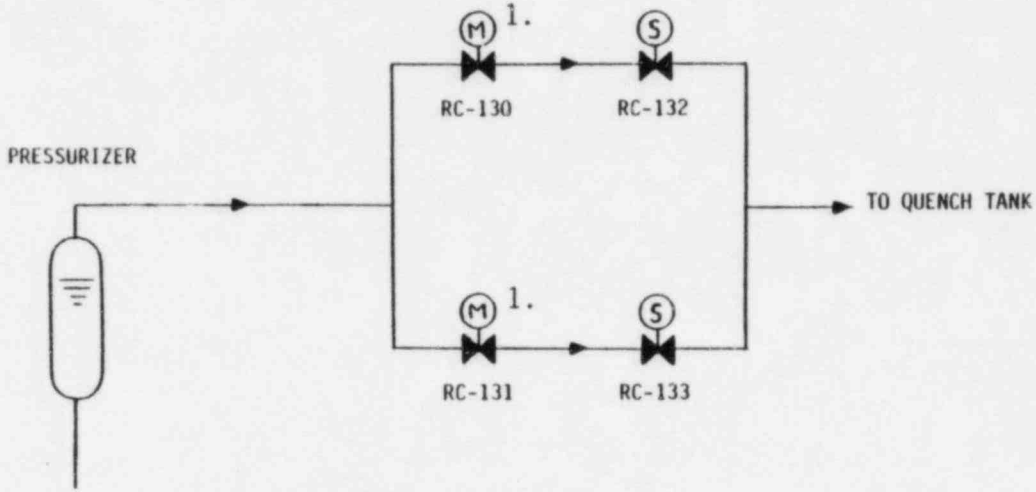
The Primary Feed and Bleed System is a manually actuated system. Following a loss of secondary heat sink (loss of main and auxiliary feedwater flow) the operator initiates feed and bleed by opening the PORVs for an automatic design or PORVs and associated block valves for a manual design system.[1] The 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. If the charging pumps are not already running, the operator also starts them. Primary pressure control and heat removal is accomplished by releasing

1. For a manual design, plant operates with block valves closed and for an automatic design, plant operates with block valves open. For both designs, Feed and Bleed is manually initiated.



HIGH PRESSURE SAFETY INJECTION SYSTEM
(INJECTION MODE)

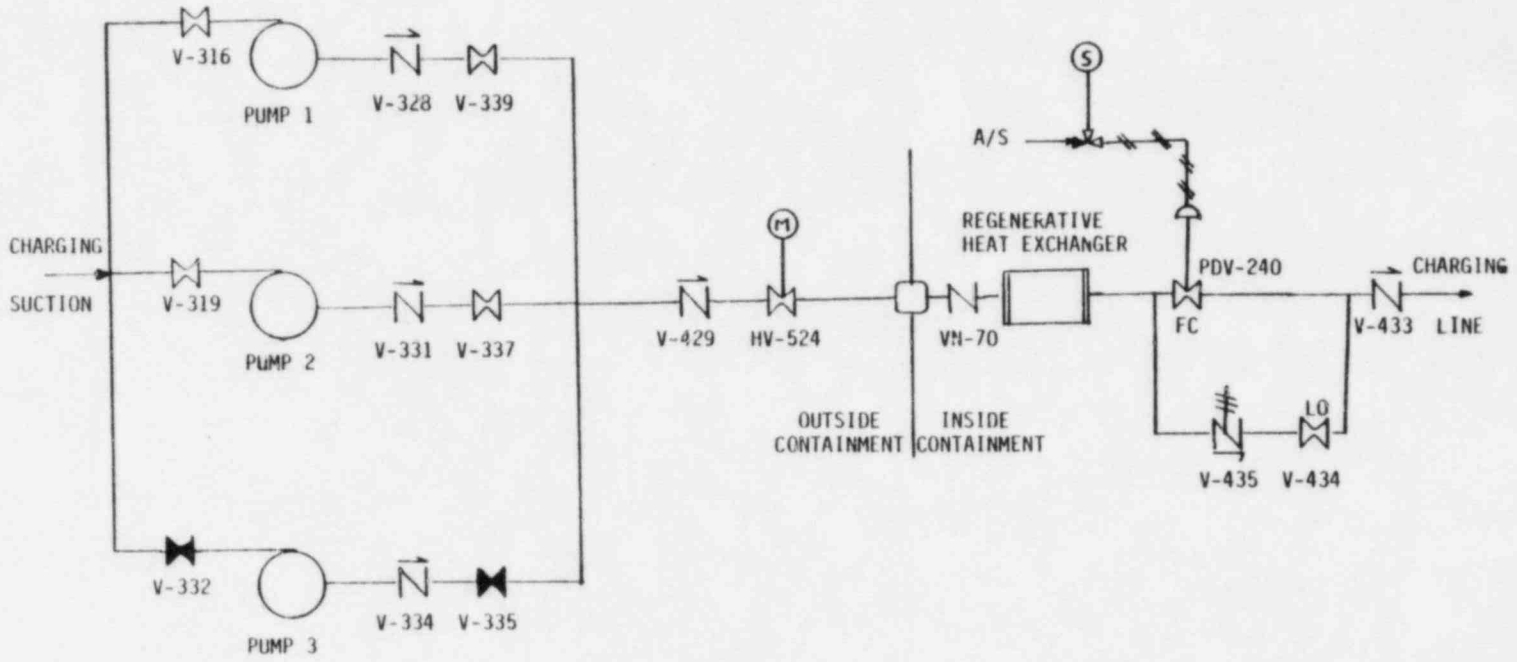
FIGURE 6.5.1-1



POWER OPERATED RELIEF VALVES

FIGURE 6.5.1-2

[1] For the manual design, plant operates with block valves closed and for the automatic design, plant operates with block valves open.



CHARGING SYSTEM

FIGURE 6.5.1-3

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 for successful Feed and Bleed operation.

3. Sufficient flow is defined as flow from at least one HPSI and one charging pump or flow from two HPSI pumps. For HPSI, at least two flow paths (i.e., injection into two cold legs) are required to deliver full flow.

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

5. Both HPSI pumps are available to start on SIAS.

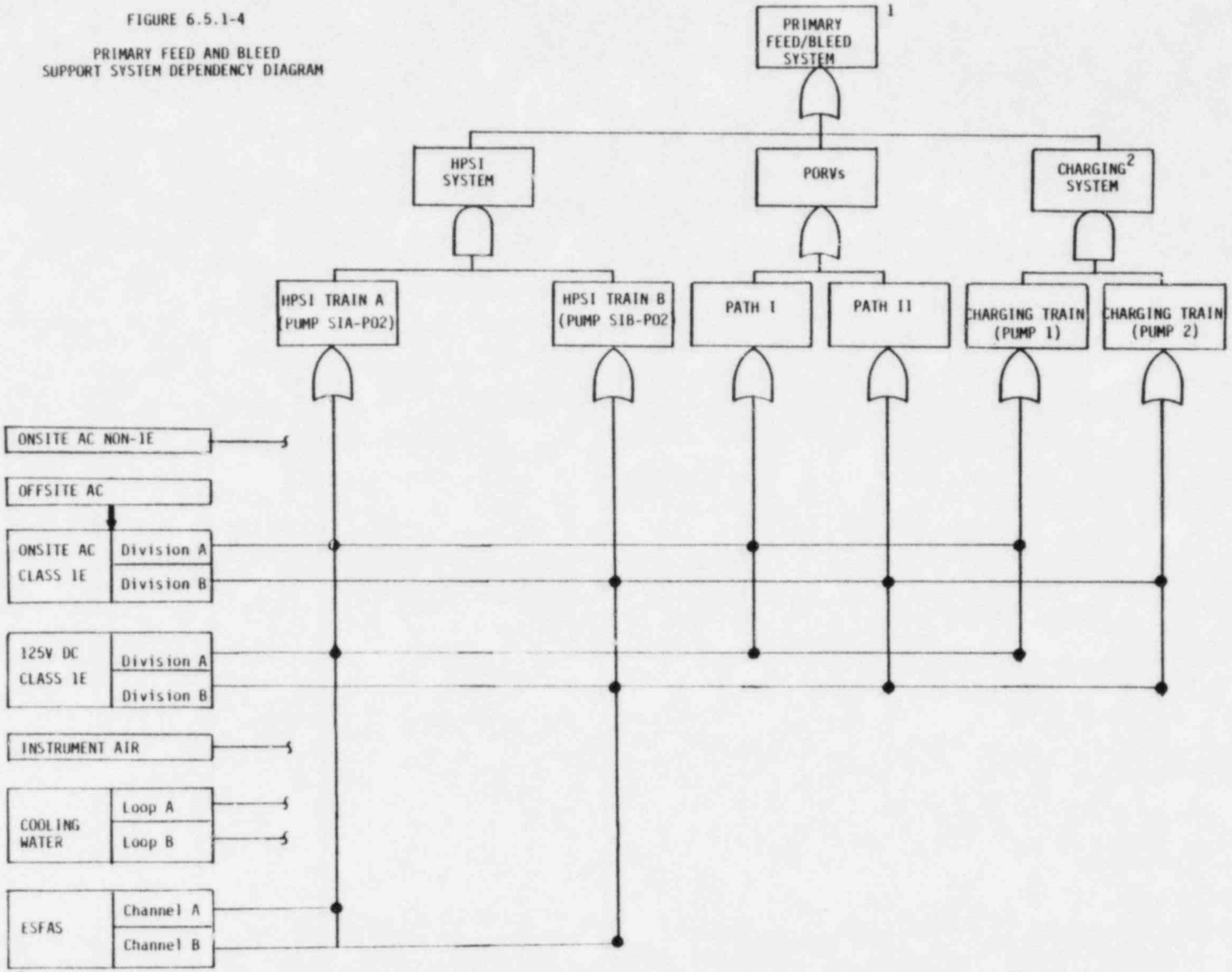
6. The following operator actions were considered:

    - Opening of the PORVs (and block valves for manual design) from the control room.

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

FIGURE 6.5.1-4

PRIMARY FEED AND BLEED
SUPPORT SYSTEM DEPENDENCY DIAGRAM



[1]This Support System Dependency Diagram does not represent the fault tree failure logic for Feed & Bleed.The Feed & Bleed success criteria is defined in Section 6.5.2

[2]Charging Pump 3 is assumed to be down for maintenance.

- If the charging pumps are not running, manual initiation of charging flow from the control room.

  The operator is allowed 25 minutes following a loss of heat sink to complete these three actions.

7. The containment sump isolation valves are closed.

8. Since maintenance can only be performed on one HPSI Pump during plant operation, unavailability contributions due to pump maintenance are included only for one of the pumps.

9. Two charging pumps (1 and 2) are operating at the time of the initiating event and charging pump 3 is in maintenance.

10. 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.

6.5.4 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 (manual design)

- (a) Failure of feed and bleed operation (manual design) given loss of MFW and loss of AFW.

  (b) Failure of feed and bleed operation (automatic design) 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. (In addition, the probability of restoration of AC power following the loss of AFW is incorporated into the Feed and Bleed System failure probability for Case Two.) 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 the two cases. 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 PVNGS PRIMARY FEED AND BLEED SYSTEM

Case Number		Description	Failure Probability (Median Value)	Error Factor
One		Failure of Feed and Bleed Operation (manual design)- System Unavailability	3.3E-2	4
Two[1]	(a)	Failure of Feed and Bleed Operation (manual design) - System Unavailability given loss of MFW and loss of AFW	4.0E-1	1.9
	(b)	Failure of Feed and Bleed Operation (automatic design) - System Unavailability given loss of MFW and loss of AFW	2.0E-1	2.4

1. For the manual design, plant operates with block valves closed and for the automatic design, plant operates with block valves open. For both designs, Feed and Bleed is manually initiated.

TABLE 6.5.3-2

DOMINANT CUTSETS FOR PVNGS FEED AND BLEED SYSTEM

Case Number	Cutset	Description	% of Total Failure Probability
One	1. VVZ02550	Operator fails tc open valves	86%
	2. VVMA2552	Block valve RC-131 fails to open	3.4%
	3. VVMA2551	Block valve RC-130 fails to open	3.4%
	4. VVSA2555	PORV RC-133 fails to open	3.4%
	5. VVSA2553	PORV RC-132 fails to open	3.4%
Two (a) Manual Design	1. EBGP2680 EDDJ2817	Spurious grid collapse and DG E-PEB-G02 fails to start	37%
	2. EBGP2680 ECBV2852	Spurious grid collapse and Battery E-PKA-F11 Unavailable	29%
	3. EBGP2680 EDDJ2816	Spurious grid collapse and DG E-PEA-G01 fails to start	25%
(b) Automatic Design	1. EBGP2680 ECBV2852	Spurious grid collapse and Battery E-PKA-F11 Unavailable	61%
	2. VVS02550	Operator fails to open valves	17%
	3. EBGP2680 EDDI2816 EDDJ2817	Spurious grid collapse and DG E-PEA-G01 fails to start and DG E-PEB-G02 fails to start	15%

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

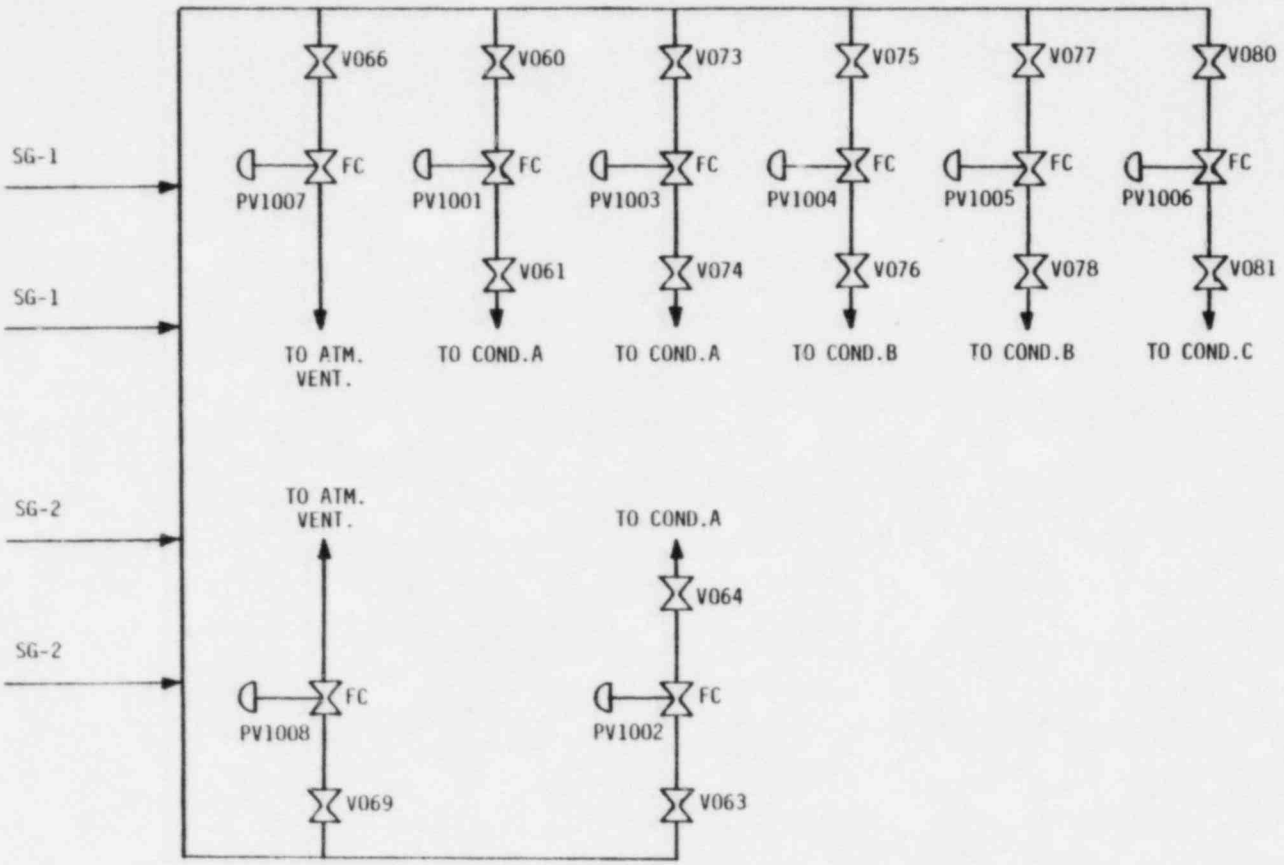
For the Spurious PORV LOCA event tree, a fault tree model was used to evaluate Failure to Open the TBVs.

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

Figure 6.6.1-1 provides a schematic of the Turbine Bypass System. The turbine bypass system (TBS) consists of eight air-operated globe valves and associated instruments and controls. These valves branch from each main steam line downstream of tne Main Steam Isolation Valves. Six of these valves direct steam to the condenser and the remaining two vent directly to the atmosphere. The TBS provides a maximum steam dump capacity of 55% rated main steam flow.

The valves are designed to fully open or close within 1 second or to modulate full open or closed in a minimum of 15 seconds and a maximum of 20 seconds. The valves are equipped with remote-operated handwheels to permit manual operation at the valve location.



TURBINE BYPASS SYSTEM

FIGURE 6.6.1-1

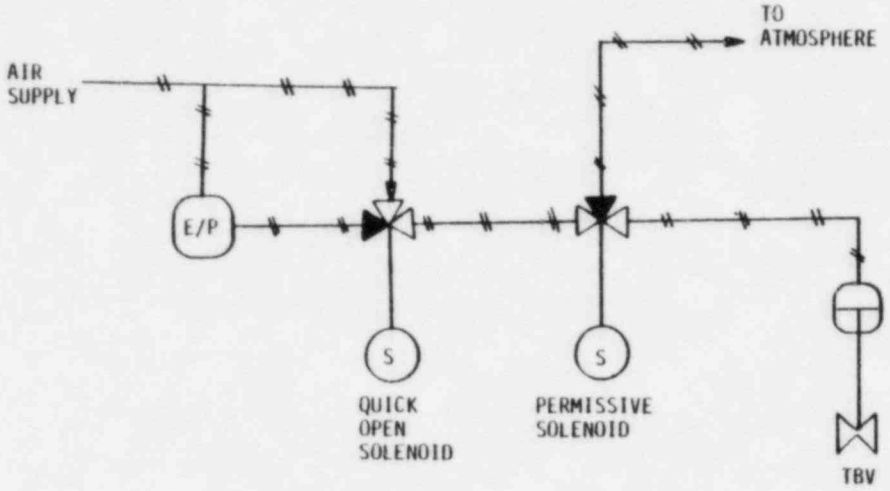
The two valves which exhaust to the atmosphere are the last to open and the first to close during load rejections, thus minimizing the quantity of steam discharged to the environment. The valves and piping for the system are located in the turbine building.

During normal operation, the TBVs are under the control of the Steam Bypass Control System. The main function of the TBVs is to limit the pressure rise in the steam generator, following a reactor trip, to a level which prevents opening of the main steam line safety valves. The bypass valves also open to the condenser to remove decay heat following a reactor shutdown or during hot standby conditions.

During plant shutdown, one turbine bypass valve is remotely or manually positioned to remove Reactor Coolant System sensible heat to reduce the reactor coolant temperature. Since steam pressure decreases as the system temperature is reduced, bypass valve flow capacity becomes limited at low pressures and other bypass valves are opened to complete the cooldown at the design rate until shutdown cooling is initiated. All turbine bypass valves can be remotely operated from the main control room. These valves are pneumatically operated.

The valves in the turbine bypass system are designed to fail closed to prevent uncontrolled bypass of system.

A simplified schematic of a turbine bypass valve is presented in Figure 6.6.1-2. An excess of energy in the NSSS caused by a load reduction transient or other conditions will result in an increase in the main steam header pressure. If that pressure increases above a programmed setpoint value, the SBCS will sequentially modulate the turbine bypass valves open to limit the main steam header pressure to the setpoint value (modulating mode). However, the rate of change of excess NSSS energy that may be dissipated by the modulating mode is limited due to the 15-20 second stroke time required for the valves.



SCHEMATIC OF A TYPICAL TBV

FIGURE 6.6.1-2

When a decrease in load is detected so large that it cannot be accommodated by the Modulation control of the valves, 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 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. TBVs are designed to fail closed on loss of instrument air or loss of offsite power. TBVs PV1001 through PV1006 also require a condensor available signal for them to open.

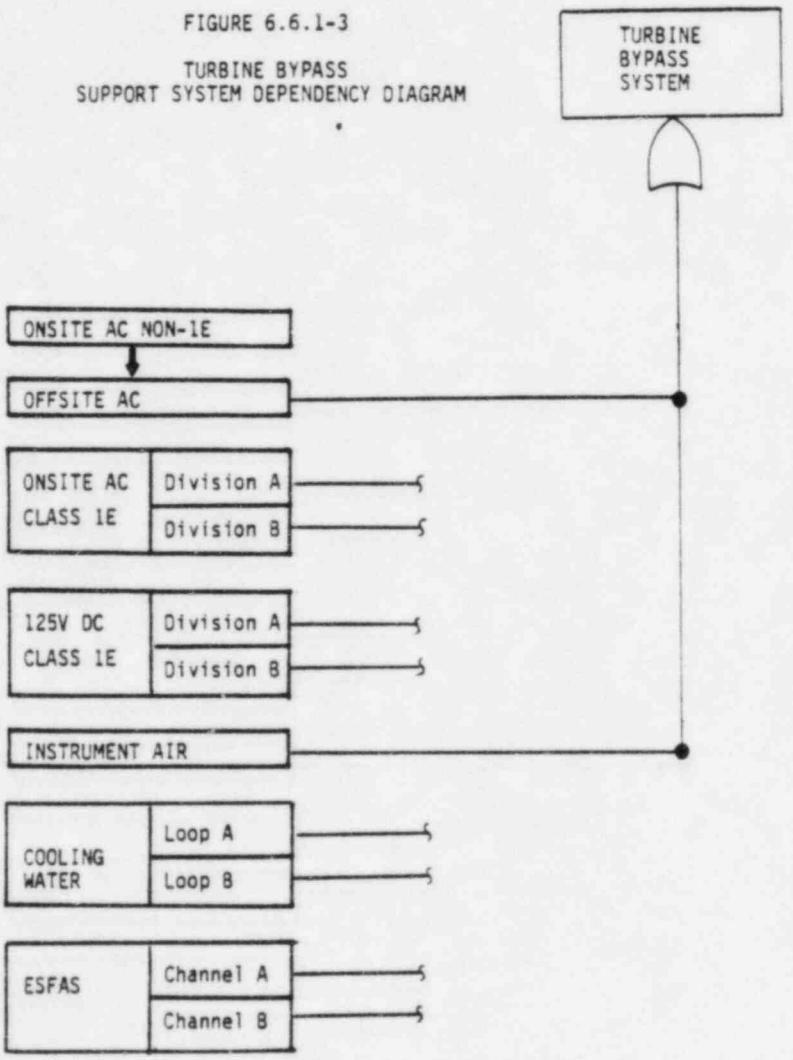
2. Two redundant Quick Opens Signals (Channel 1 and Channel 2) are required to open a bypass valve in the Quick Open mode of operation.

3. The SBCS receives power from 120V AC Instrument and Control Panel E-NNN-D11.

4. 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

FIGURE 6.6.1-3

TURBINE BYPASS
SUPPORT SYSTEM DEPENDENCY DIAGRAM



probability of losing them 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".

5. During plant cooldown, only one TBV is initially used to reduce the RCS temperature. At low pressure, when the valve flow capacity becomes limiting, the second valve is opened. Therefore, the fault tree 'Failure to close all TBVs after Quick Open or during Cooldown' is defined as follows: one out of eight valves fails to close after Quick Open or one out of two valves fails to close during cooldown.

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
- One TBV 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 TBVs 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. 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 PVNGS TURBINE BYPASS SYSTEM

Case Number	Description	Failure Probability (Median Value)	Error Factor
One	TBVs Fail to Quick Open - System Unavailability	3.5E-3	7
Two	One TBV Fails to Reclose after Quick Open or During Cooldown - System Unavailability	2.1E-2	4
Three	Loss of TBV Flow Prior to Isolation of the Affected (or Most Affected) SG - System Unavailability	1.1E-2	4
Four	Loss of TBV Flow After Isolation of the Affected (or Most Affected) SG - System Unavailability	2.1E-2	3
Five	Fail to Open TBVs - System Unavailability	1.7E-2	3

TABLE 6.6.3-2

DOMINANT CUTSETS FOR PVNGS TURBINE BYPASS SYSTEM

Case Number	Cutset	Description	% of Total Failure Probability
One	1. EBFB2699	13.8 KV Bus E-NAN-S01 Fast Transfer Breaker Fails to Close	32%
	2. EBFA2697	Unit Auxiliary Transformer (13.8 KV Bus E-NAN-S01) Fast Transfer Breaker Fails to Open	32%
	3. ECBV2810	Battery E-NKN-F17 Unavailable	32%
Two	1. TVPO2291	Operator Fails to Close TBV During Cooldown	17%
	2. TVPB2263	TBV Mechanical Malfunction	13%
	3. TVPB2264	TBV Mechanical Malfunction	13%
Three	1. THSO2292	Early SG Isolation by Operator	100%
Four	1. TSMO2293	Operator Fails to Lower MSIS Setpoint	50%
	2. IZZX2063	Loss of Instrument Air - Demand Failure	45%
	3. TVSA2295	Permissive Solenoid Malfunction	5%
Five	1. IZZX2063	Loss of Instrument Air - Demand Failiure	66%
	2. ECBV2810	Battery E-NKN-F17 Unavailable	8%
	3. EBGP2682	Grid collapse on Turbine Trip	8%
	4. EBFA2697	UAT (13.8KV Bus E-NAN-S01) Fast Transfer Breaker Fails to open	8%
	5. EBFB2699	13.8KV Bus E-NAN-S01 Fast Transfer Breaker Fails to close	8%

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. Both St. Lucie 2 and PVNGS turbines have four steam inlet paths to the high pressure (HP) turbine; each path contains in series a stop valve and a governing control valve. Each valve has an individual actuator, controlled by E/H governing system. The dominant contributors to the failure to trip turbine are the mechanical malfunction of the stop and governing control valves or their actuator. Because of similarity of the inlet 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 governing control valves are initially fully open.

3. The reactor trip signal is generated.

4. An operator action from the control room is included as a back-up 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

Each of the Main Steam lines is equipped with one quick acting Main Steam Isolation Valve (MSIV). Figure 6.7.1-1 provides a schematic of these valves. Each valve has an actuation time of 5 seconds or less and operates automatically in the event of rupture in the main steam piping or associated components either upstream or downstream of the MSIV. They prevent blowdown of more than one steam generator (assuming a single active failure). The valves are designed to close upon loss of electric power. Once isolation is initiated, in response to a main steam isolation signal, the valves continue to close and cannot be opened until manually reset.

Each valve has two physically separate and electrically independent solenoid actuators in order to provide redundant means of valve operation.

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 to close the valve.

2. The MSIVs fail close on loss of power.

3. 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.

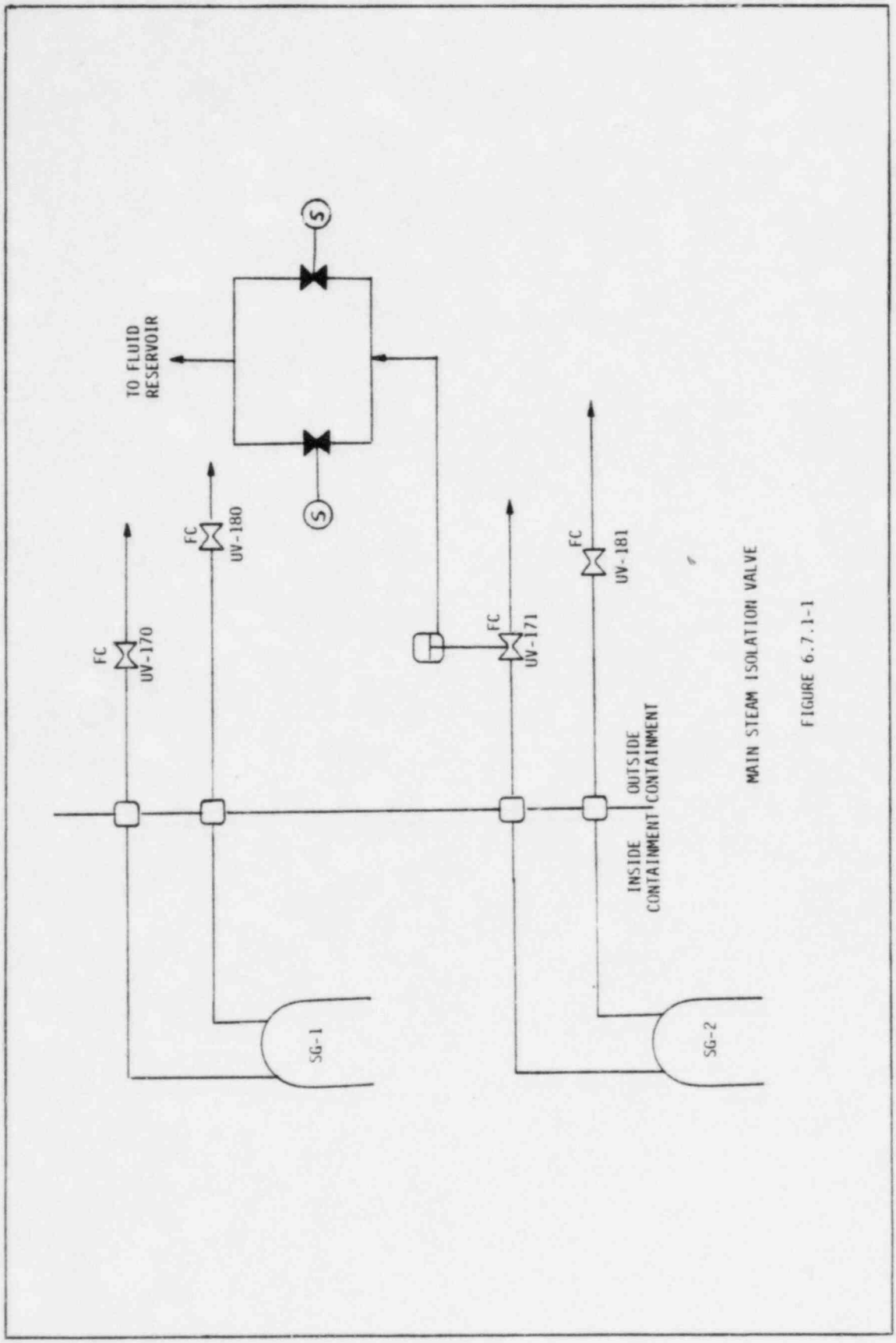
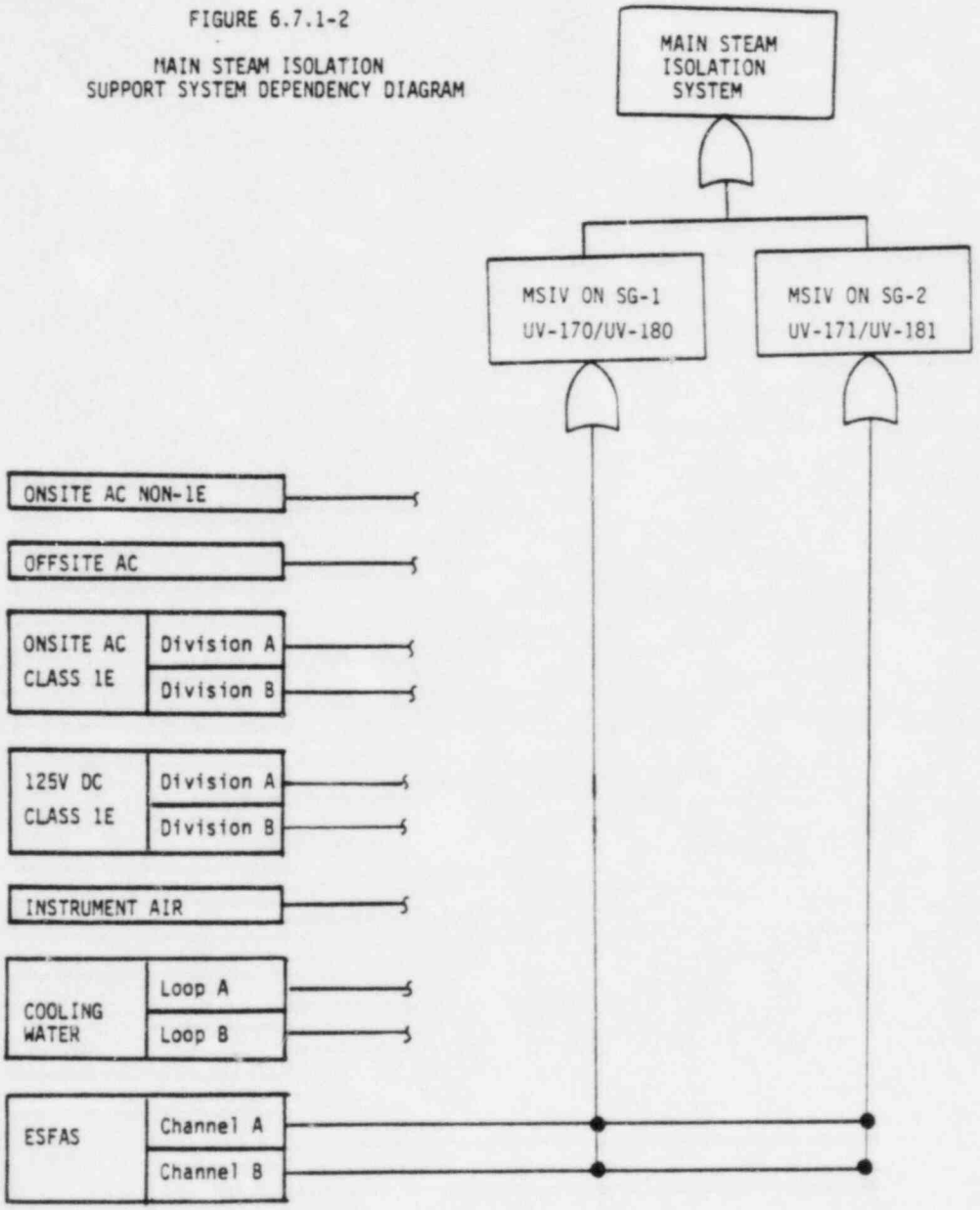

TO FLUID RESERVOIR
FC UV-170
FC UV-180
FC UV-171
FC UV-181
OUTSIDE CONTAINMENT
INSIDE CONTAINMENT
SG-1
SG-2
MAIN STEAM ISOLATION VALVE

FIGURE 6.7.1-1

FIGURE 6.7.1-2

MAIN STEAM ISOLATION
SUPPORT SYSTEM DEPENDENCY DIAGRAM



4. The MSIV bypass valves remain close. This is because the bypass valves are normally closed and they fail close on loss of power.

6.7.3 Results

Fault tree logic diagrams were used to evaluate the probability of failing to close both MSIVs on a steam generator. 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 for the two steam generators 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 the two cases. 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 PVNGS MSIVs

Case Number	Description	Failure Probability (Median Value)	Error Factor
One	Fail to close MSIVs UV-170 and UV-180 on SG-1 - System Unavailability	1.8E-3	3
Two	Fail to close MSIVs UV-171 and UV-181 on SG-2 - System Unavailability	1.8E-3	3

TABLE 6.7.3-2

DOMINANT CUTSETS FOR PVNGS MSIVs

Case Number	Cutset	Description	% of Total Failure Probability
One	1. DVEB2065A	MSIV UV-170 Mechanical Malfunction	49.5%
	2. DVEB2066A	MSIV UV-180 Mechanical Malfunction	49.5%
	3. FSMR2000 FSMR2001 FSMO2002	MSIS A not generated and MSIS B not generated and Operator fails to generate MSIS.	0.2%
Two	1. DVEB2065	MSIV UV-171 Mechanical Malfunction	49.5%
	2. DVEB2066	MSIV UV-181 Mechanical Malfunction	49.5%
	3. FSMR2000 FSMR2001 FSMO2002	MSIS A not generated and MSIS B not generated and Operator fails to generate MSIS	0.2%

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 HV184 or ADV HV178 on SG-1
- Open ADV HV185 or ADV HV179 on SG-2
- Terminate flow through ADV HV184 and ADV HV178 on SG-1
- Terminate flow through ADV HV185 and ADV HV179 on SG-2

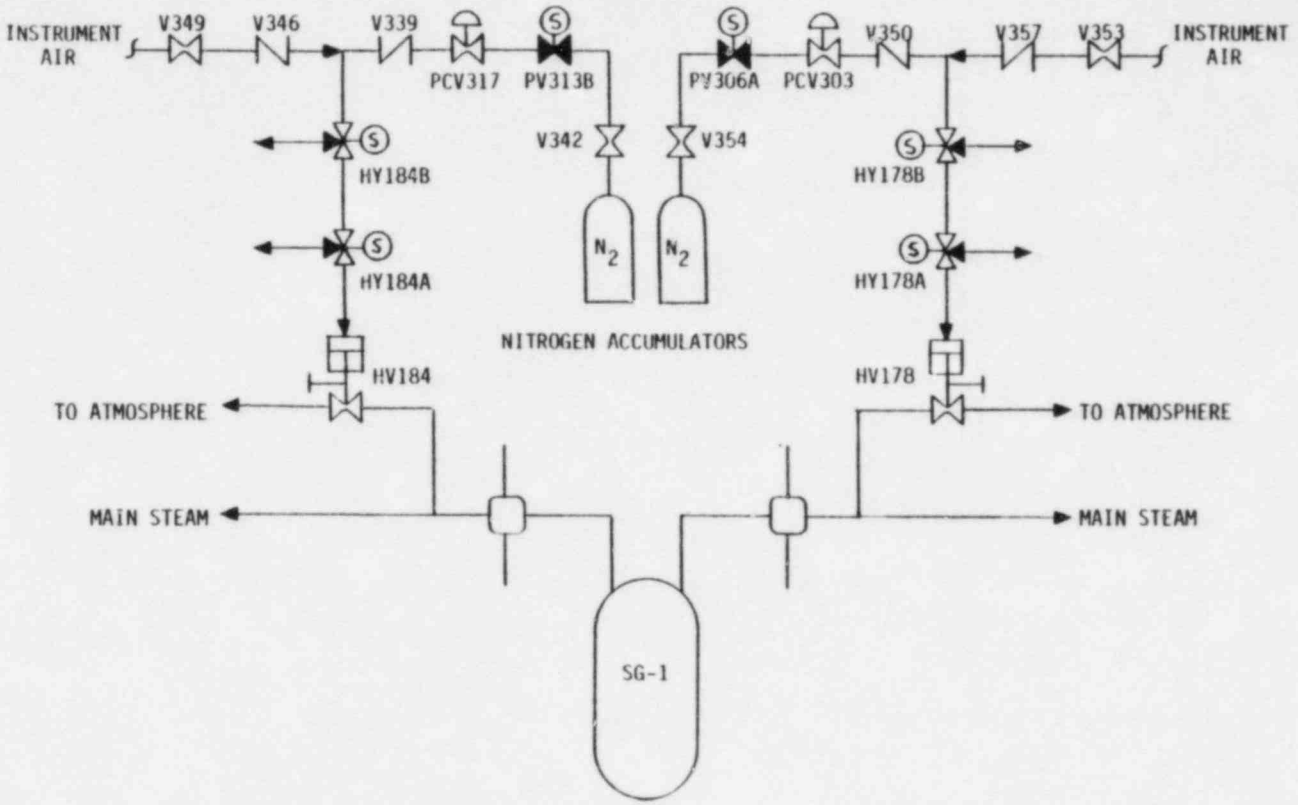
For the spurious PORV LOCA event tree, a fault tree model was used to evaluate Failure to Open One of Four ADVs.

6.8.1 System Description

The PVNGS Atmospheric Dump System consists of four Atmospheric Dump Valves (ADVs) and eight solenoid valves. Two redundant ADVs are provided for each steam generator, one per main steam line. The ADVs are pneumatically operated and can be controlled from the main control room. A handwheel is also provided with the atmospheric dump valve for local hand operation. Schematics of the ADS are presented in Figures 6.8.1-1 and 6.8.1-2.

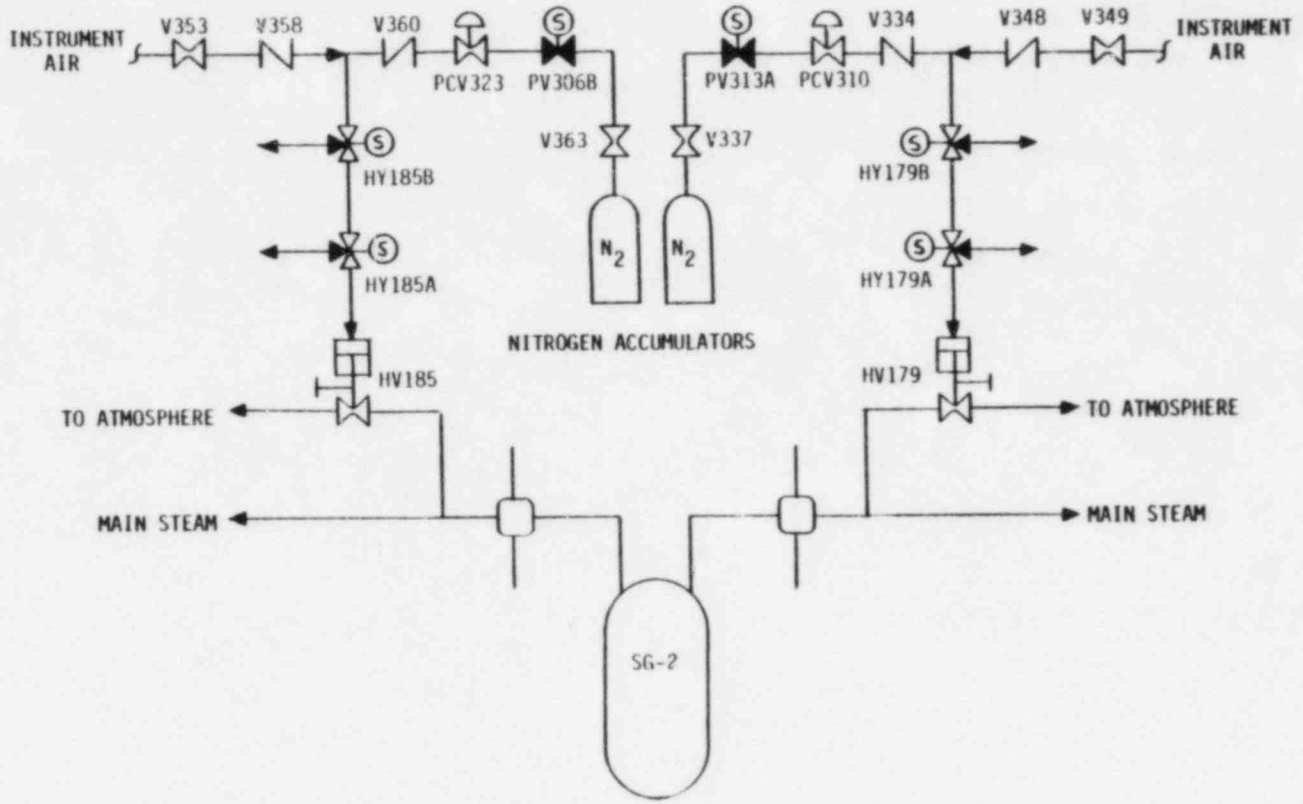
In the "open" mode, two solenoid valves (per ADV) open and align to supply air to the underside of the actuator piston. The air pressure under the actuator piston opposes the spring tension above the piston. An increased air pressure under the piston allows the actuator piston to move upward, raising the plug, and increasing flow through the valve dump.

In the "close" mode, the solenoid valves close and align to vent the air from the ADV to the atmosphere. The spring tension above the piston provides the driving force to close the valve.



ATMOSPHERIC DUMP SYSTEM ON SG-1

FIGURE 6.8.1-1



ATMOSPHERIC DUMP SYSTEM ON SG-2

FIGURE 6.8.1-2

The Class 1E 125 VDC power system provides power to the solenoid valves that control the ADVs. The solenoid valves are designed to fail "open" in the exhaust positior; therefore, ADVs are fail closed on loss of electrical power. Air supply to the ADVs is provided by the turbine building instrument air header. Should instrument air be lost, a nitrogen accumulator supplies backup pressure automatically. The ADVs are designed to fail closed on a loss of air pressure. 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.

The Atmospheric Dump support system dependency diagram is provided in Figure 6.8.1-3.

6.8.2 Assumptions

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

1. The operator is required to open or close the ADVs from the control room. (No automatic signal is assumed). The ADVs can also be manually open or closed with a handwheel.

2. The solenoid valves receive the following power supplies:

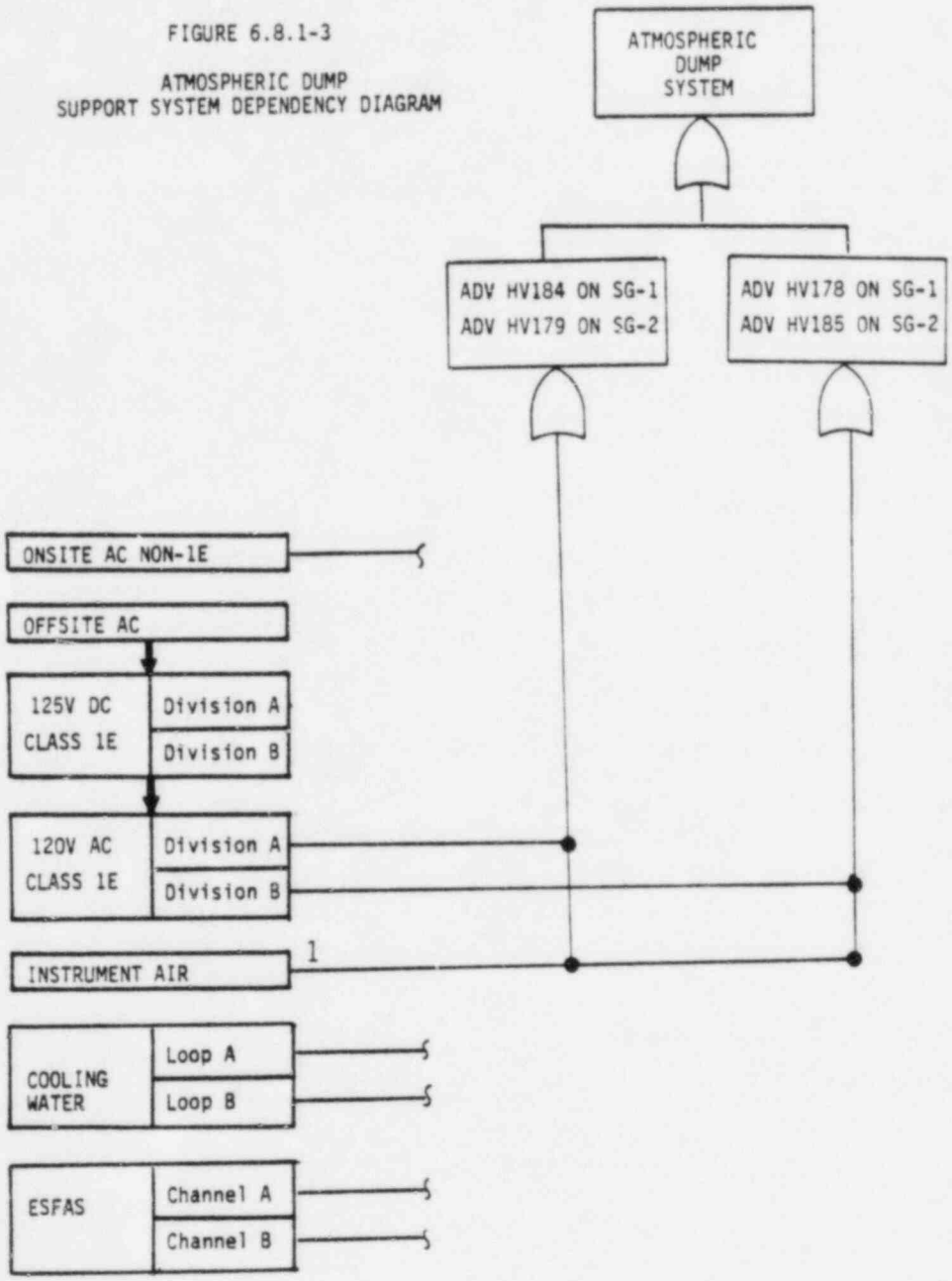
HY184A and HY179A	125 VDC Bus E-PKA-M41
HY178A and HY185A	125 VDC Bus E-PKB-M42
HY184B and HY179B	125 VDC Bus E-PKB-M43
HY178B and HY185B	125 VDC Bus E-PKD-M44

3. Air pressure to the ADVs can be supplied by either the Instrument Air System or a nitrogen accumulator of Instrument Air is unavailable.

4. The ADVs fail closed on loss of power or loss of instrument air.

FIGURE 6.8.1-3

ATMOSPHERIC DUMP
SUPPORT SYSTEM DEPENDENCY DIAGRAM



[1]For this system Instrument Air has a nitrogen backup.

5. The eight solenoid valves HY184A and B, HY178A and B, HY185A and B, and, HY179A and B fail open in the exhaust position on loss of power, thereby preventing air and nitrogen from opening the ADVs.

6. Nitrogen accumulator isolation valves PV313B, PV306A, PV306B and PV313A open on loss of Instrument Air and fail open on loss of Offsite Power.

7. The following operator actions were considered:

   - manually opening the solenoid valves from the control room.
   - manually closing the solenoid valves from the control room.
   - manually closing the ADVs with a handwheel.

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 one of two ADVs on SG-1
- Failure to open one of two ADVs on SG-2
- Failure to close both ADVs on SG-1
- Failure to close both ADVs on SG-2

For the SGTR event trees where offsite power is unavailable at the time of the initiating event, the above 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 four ADVs.

The quantitative results of the analyses are presented as Cases One through seven 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. The results of Cases Two and Four indicate that loss of offsite power is not a significant contributor to the unavailability of the ADVs.

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 PVNGS ATMOSPHERIC DUMP SYSTEM

Case Number	Description	Failure Probability (Median Value)	Error Factor
One	Failure to open ADV HV184 or ADV HV178 on SG-1. System Unavailability given offsite power available	1.6E-2	4
Two	Failure to open ADV HV184 or ADV HV178 on SG-1. System Unavailability given offsite power unavailable	1.6E-2	4
Three	Failure to open ADV HV185 or ADV HV179 on SG-2. System Unavailability given offsite power is available	1.6E-2	4
Four	Failure to open ADV HV185 or ADV HV179 on SG-2. System Unavailability given offsite power is unavailable	1.6E-2	4
Five	Failure to close ADV HV184 and ADV HV178 on SG-1. System Unavailability	3.4E-3	6
Six	Failure to close ADV HV185 and ADV HV179 on SG-2. System Unavailability	3.4E-3	6
Seven	Failure to open one of four ADVs. System Unavailability	1.6E-2	4

TABLE 6.8.3-2

DOMINANT CUTSETS FOR PVNGS ATMOSPHERIC DUMP SYSTEM

Case Number	Cutset	Description	% of Total Failure Probability
One	1. DVSO2173	Operator fails to generate open signal	>99%
Two	1. DVSO2173	Operator fails to generate open signal	>99%
Three	1. DVSO2196	Operator fails to generate open signal	>99%
Four	1. DVSO2196	Operator fails to generate open signal	>99%
Five	1. DVSO2155	Operator fails to generate close signal	33%
	2. DVPB2160	ADV HV178 mechanical malfunction (FTC)	33%
	3. DVPB2156	ADV HV184 mechanical malfunction (FTC)	33%
Six	1. DVSO2164	Operator fails to generate close signal	33%
	2. DVPB2169	ADV HV179 mechanical malfunction (FTC)	33%
	3. DVPB2165	ADV HV185 mechanical malfunction (FTC)	33%
Seven	1. DVSO2173	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.

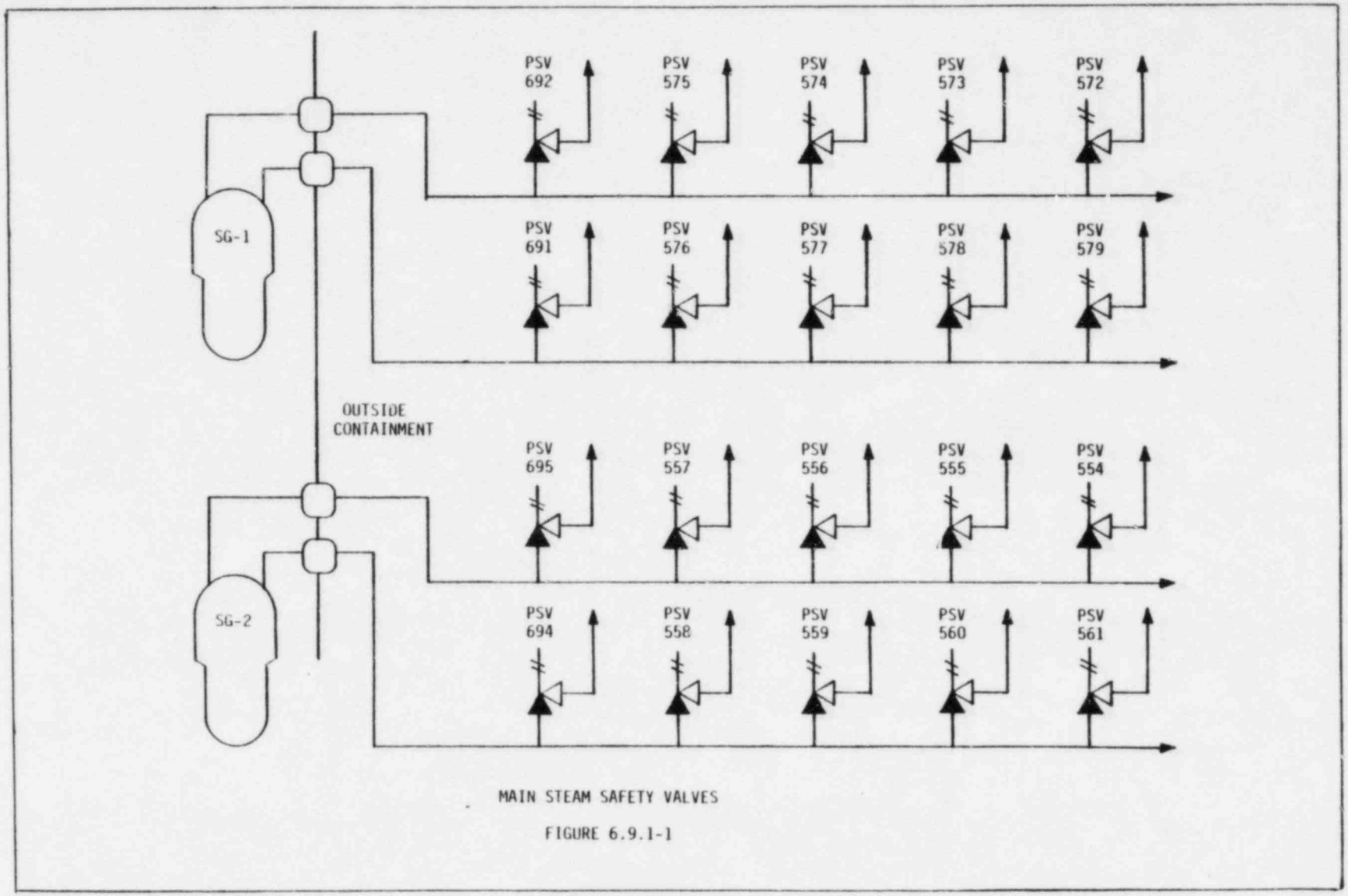
The MSSVs are modelled in the Spurious PORV LOCA event tree as the branch "Failure to Open MSSVs".

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
- six MSSVs open on the affected (or most or least affected) SG

6.9.1 System Description

A schematic of the PVNGS MSSVs is presented in Figure 6.9.1-1. The springloaded MSSVs provide over pressure protection for the secondary side of the steam generator and the main steam piping. Each main steam line is provided with five safety valves (ten valves per steam generator). The total receiving capacity of the safety valves is 11.13×10^6 lb./hr. per steam generator. The valve setpoints are as follows:



MAIN STEAM SAFETY VALVES

FIGURE 6.9.1-1

Lift Setting	
1250 psig	
1290 psig	Note: Two valves per SG at each setpoint.
1315 psig	
1315 psig	
1315 psig	

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 ten MSSVs on either steam generator.

2. The ten main steam safety valves on one steam generator are independent of the main steam safety valves on the other steam generator.

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, six 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 10 MSSVs on either SG was determined to be $<<10^{-9}$. Therefore, a probability of 10^{-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 PSV-692 on SG-1)
- One MSSV on the unaffected or least affected SG fails to reclose (MSSV PSV-695 on SG-2)
- One MSSV on the affected or most affected SG fails to reclose given the TBS is unavailable following turbine trip. (Six valves on SG-1 are assumed to open).
- One MSSV on the unaffected or least affected SG fails to reclose given the TBS is unavailable following turbine trip. (Six valves on SG-2 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 PVNGS 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-2 fails to re-close - System Unavailability	1.0E-2	3
Four	One MSSV on SG-1 fails to re-close - System Unavailability	1.0E-2	3
Five	One MSSV on SG-1 fails to re-close given TBS is unavailable following turbine trip - System Unavailability	6.1E-2	3
Six	One MSSV on SG-2 fails to re-close given TBS is unavailable turbine trip - System Unavailability	6.1E-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% 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% 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 post-trip 5% 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 PVNGS-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 post-trip 5% flow are treated directly in the fault tree logic diagram.

TABLE 6.10-1

LOSS OF MAIN FEEDWATER

PLANT TRIP EVENTS

Category 1:

Loss of 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
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
Partial 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 this analysis and are not addressed (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

INITIATORS 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

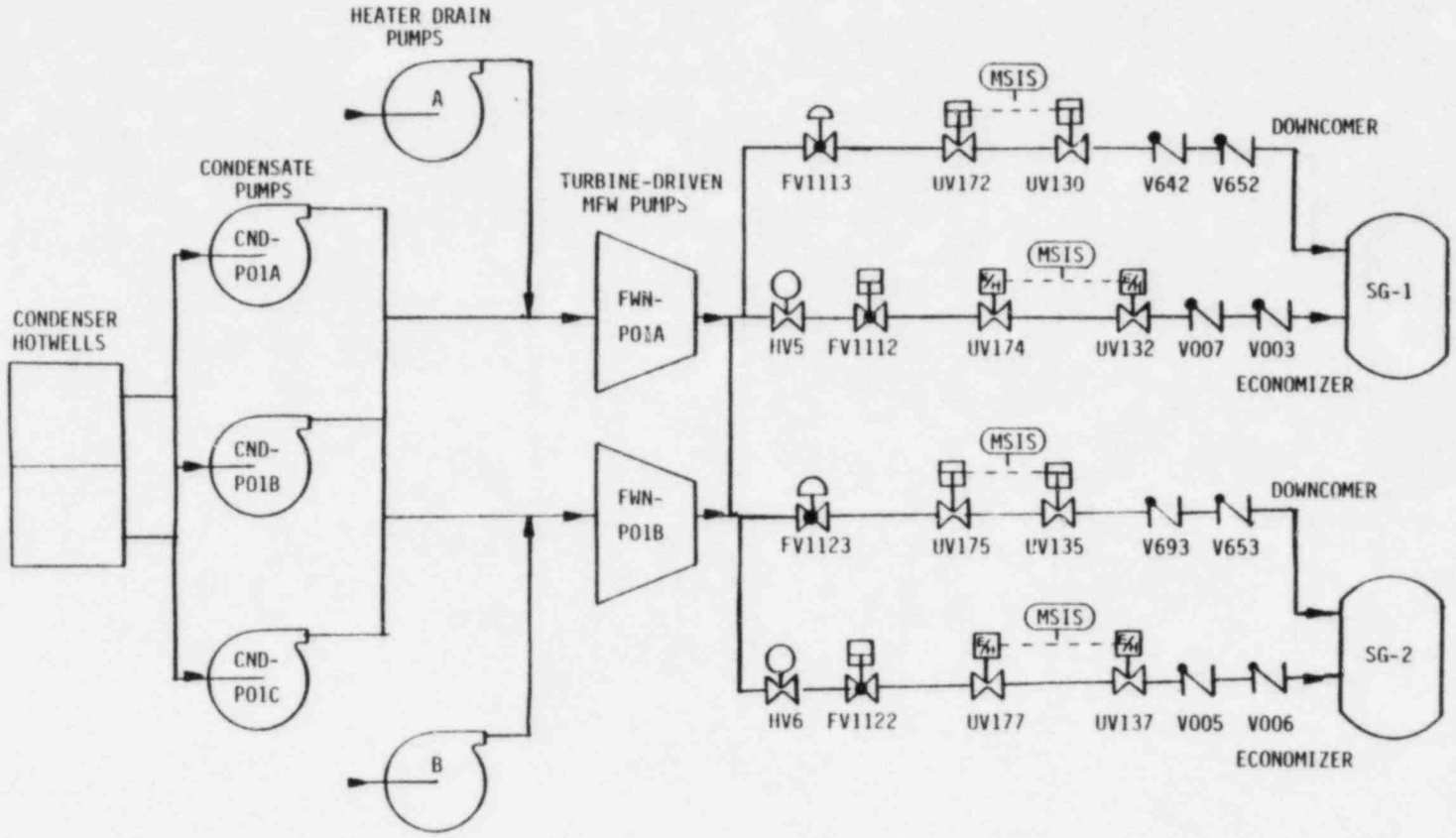
For the Spurious or Transient Induced PORV LOCA event tree, a fault tree logic diagram was used to evaluate the probability of failing to deliver 5% MFW flow to both steam generators. For the PORV LOCA following SGTR event tree, a fault tree model was used to determine the probability of failing to deliver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

6.10.1 System Description

A schematic of the PVNGS Condensate and Main Feedwater System is presented in Figure 6.10.1-1. The condensate and feedwater system consists of motor driven condensate pumps, low pressure feedwater heaters, heater drain tanks and pumps, feedwater pumps and drive turbines, and high pressure feedwater heaters. Three 50% capacity condensate pumps are provided, taking suction from the main condenser hotwells. The condensate pumps discharge into the low-pressure feedwater heaters. During abnormal condensate water chemistry the condensate is passed through the polishing demineralizers before going to the feedwater heaters. The system is designed to permit continued full-load operation of the plant with one of three condensate pumps unavailable.

The low-pressure feedwater heaters are mounted in the condenser neck. From the intermediate-pressure heaters the feedwater is pumped, by two 65% 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 into a common header which branches into two lines. The outlets of the heaters merge into a common line where the two feedwater streams are mixed to provide the SGs with feedwater of equal temperature. The feedwater flow again branches into two parallel lines which conduct feed flow to the SG system. The flow is then split into two streams with the great amount entering the steam generator economizer



MAIN FEEDWATER SYSTEM

FIGURE 6.10.1-1

section. The smaller amount of feedwater enters the downcomer section. The feedwater economizer and downcomer control valves and containment isolation valves are located outside the containment.

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

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 or load rejection event with the subsequent loss of post-trip 5% main feedwater flow to both steam generators.

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

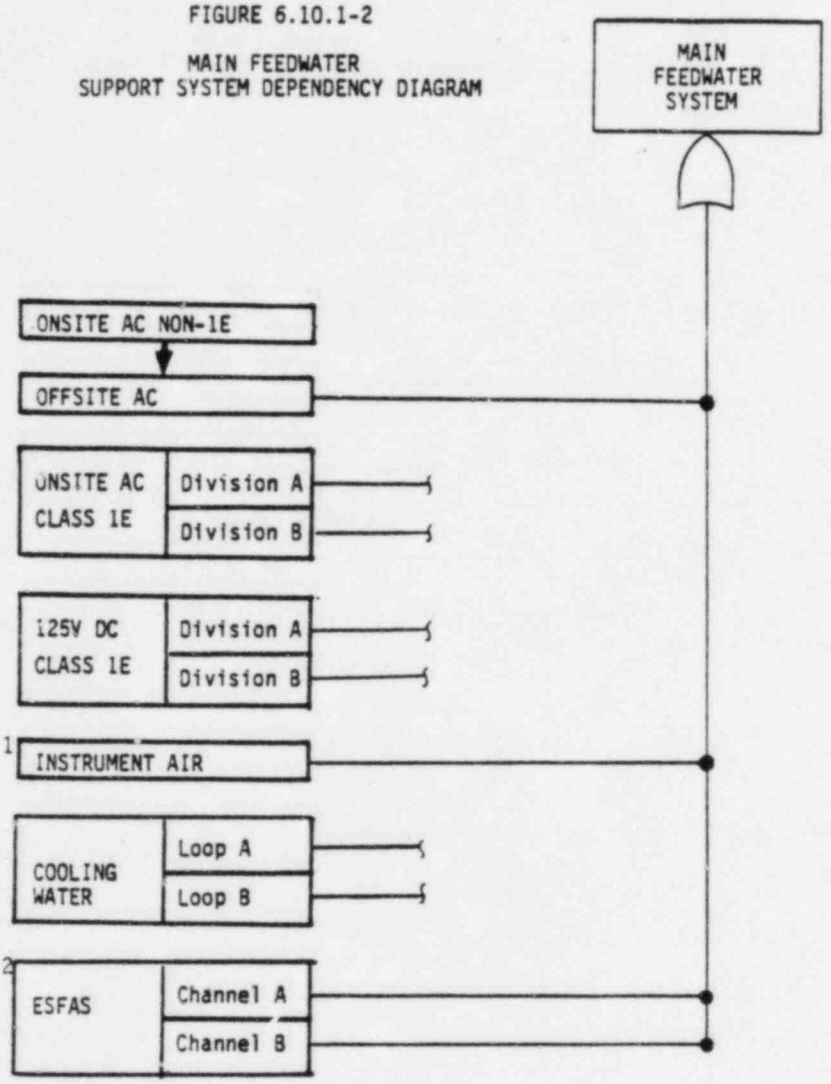
3. For the PORV LOCA following SGTR event tree, Failure to Deliver 5% MFW to One SG is defined as failing to deliver 5% MFW flow to the unaffected SG.

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

   2 Main Feedwater Pumps
   2 Heater Drain Pumps
   2 Condensate Pumps
   Circulating Water System
     Condenser

FIGURE 6.10.1-2

MAIN FEEDWATER
SUPPORT SYSTEM DEPENDENCY DIAGRAM



[1]For this system Instrument Air has a nitrogen backup.

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

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

   1 Main Feedwater Pump
   1 Condensate Pump
   1 Downcomer Bypass Feed Control Valve
   Condensate Hotwell

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 (Pump C) is unavailable due to maintenance.

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

10. Main Feedwater Pumps trip on

    High pump discharge pressure
    Low net positive suction head
    Low pump lube oil pressure
    Pump turbine driver overspeed
    Turbine driver exhaust low vacuum
    Turbine thrust-bearing wear excessive
    Low turbine lube oil pressure
    Turbine vibration high.

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

12. Condensate pumps will trip on low hotwell level.

13. Failure of the 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 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 6.10.3-2 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 PVNGS MAIN FEEDWATER SYSTEM

Case Number	Description	Failure Probability (Median Value)	Error Factor
One	Loss of Main Feedwater Initiating Event Frequency	1.12 per year	3
Two	Fail to deliver 5% MFW to the unaffected SG given PORV LOCA following SGTR - System Unavailability	1.4E-2	4
Three	Fail to deliver 5% MFW to at least one of two SGs given spurious or Transient Induced PORV LOCA - System Unavailability		
	(a) Manual PORV Design	1.4E-2	4
	(b) Automatic PORV Design	5.2E-2	2

TABLE 6.10.3-2

DOMINANT CUTSETS FOR PVNGS MAIN FEEDWATER SYSTEM

Case Number	Cutset	Description	% of Total Failure Probability
One	1. MPMC2365	Loss of Condenser Vacuum Pumps	33%
	2. FSMQ2351	Spurious MSIS	7.4%
	3. MZZZ2368	Loss of Circulating Water System System	7.4%
Two	1. EBGP2682	Grid Collapse Following TT	9.7%
	2. EBFA2697	Unit Auxiliary Transformer for E-NAN-S01 Transfer Breaker Fails to Open	9.7%
Three (a) Manual PORV Design	1. EBGP2682	Grid collapse Following TT	9.9%
	2. EBFA2697	Unit Auxiliary Transformer Transfer Breaker Fails to Open	9.9%
	3. EBFB2699	Bus E-NAN-S01 Fast Transfer Breaker Fails to Close	9.9%
(b) Automatic PORV Design	1. EBGP2680	Spurious Grid Collapse	81%
	2. ECBV2810	Battery E-NKN-F17 Unavailable	2%

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 or transient induced 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 following 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.

AFW motor-operated regulating and isolation valves are maintained only during 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 PVNGS, the maintenance unavailability of the different pump trains were determined based on generic values from WASH-1400 (16). From WASH-1400, the expected frequency of pump maintenance is one at 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 AFW System consists of surveillance and flow testing to satisfy the plant technical specifications and ASME requirements. Monthly testing is performed on each AFW pump. For each test, the pump is manually started and tested for a minimum flow and differential pressure on the bypass recirculation flow line. If the AFWS is required to operate, local operator action is required to align the train to provide AFW flow. The unavailability due to testing was determined by assuming an average test duration of 1.4 hours (7) and 12 tests per year. Failure to close the bypass recirculation flowline after pump testing was also considered.

The Auxiliary Feedwater motor-operated regulating and isolation valves are tested every 18 months. The test involves the operator verifying that each automatic valve actuating to its correct position upon receipt of an AFAS. The valves are also verified to be in the correct position every 30 days. Testing of the motor-operated valves does not contribute to AFW System unavailability since the valve is capable of responding to an AFAS or providing AFW flow to the SGs.

Monthly testing is also assumed to be performed separately on the AFAS. For each train, the actuation or control logic matrix and circuitry are tested. This testing does not impact the availability of the AFW System.

Human interaction with the AFW System that results in system unavailability has also been considered. Human error resulting in the misalignment of the AFW pumps manual valves (suction, discharge and bypass recirculation line) is included directly in the fault tree analysis. The AFW manual suction and discharge valves are normally open valves. The AFW pumps bypass recirculation line valves are normally closed and are opened for pump flow testing. It should be noted that the monthly flow test on the AFW pumps provides indication of the suction manual valves position.

Operator action to restore the Auxiliary Feedwater System as a response 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.

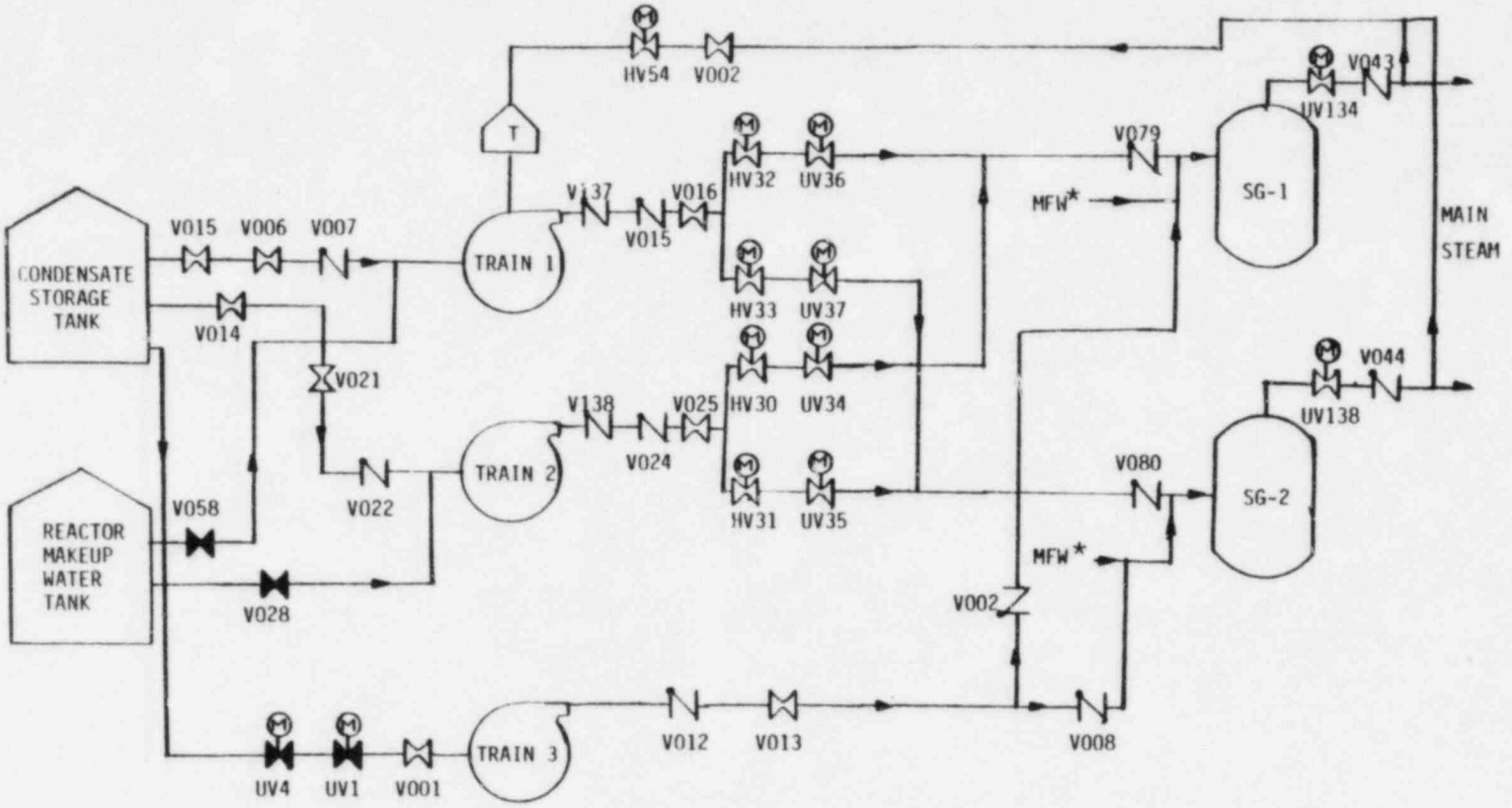
The method used to perform the common cause failure analysis is based on the system logic model. The fault tree logic diagram was used to determine the failure characteristics of the system. A search was then performed to identify potential common failure causes for the dominant failure characteristics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

Common cause contribution to system unavailability was found to be primarily due to common human facilities. 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 AFAS and was 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 PVNGS AFAS is a two train system with multiple channels.

6.11.1 System Description

A schematic of the PVNGS Auxiliary Feedwater System is presented in Figure 6.11.1-1. The AFW System 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 AFW System will start automatically on actuation of an auxiliary feedwater actuation signal (AFAS). The AFW System maintains flow control during system operation.



AUXILIARY FEEDWATER SYSTEM

FIGURE 6.11.1-1

* Pump train intersects Main Feedwater line upstream of the MFW isolation and control valves. Refer to Figure 6.17.4-1.

The AFWS consists of one Seismic Category I motor-driven pump, one Seismic Category I steam turbine-driven pump, one non-Seismic Category I motor-driven pump, associated valves, piping, controls, and instrumentation. The primary source of auxiliary feedwater is the condensate storage tank. The Seismic Category I motor-driven pump and all motor-operated valves receive power from both onsite and offsite power sources. In the event of a loss of offsite power, power to the motor driven pump is supplied by a standby diesel generator. The turbine-driven pump is supplied with steam from the main steam lines of either steam generator upstream of the MSIVs. Signals from the AFAS start the Seismic Category I motor-driven and turbine-driven pumps, shut all isolation valves, and opens the associated isolation valves to the downcomer nozzles of the steam generators. The non-Seismic Category I motor-driven pump is started manually. Its associated valves are powered from Class 1E sources and are opened manually from the control room. Operation of the non-Seismic Category I, non-essential pump is considered in the AFW Restoration Analysis, Section 6.17. The AFWS unavailability analysis includes only the Seismic Category I essential pumps and associated valves.

The Auxiliary Feedwater support system dependency diagram is provided in Figure 6.11.1-2.

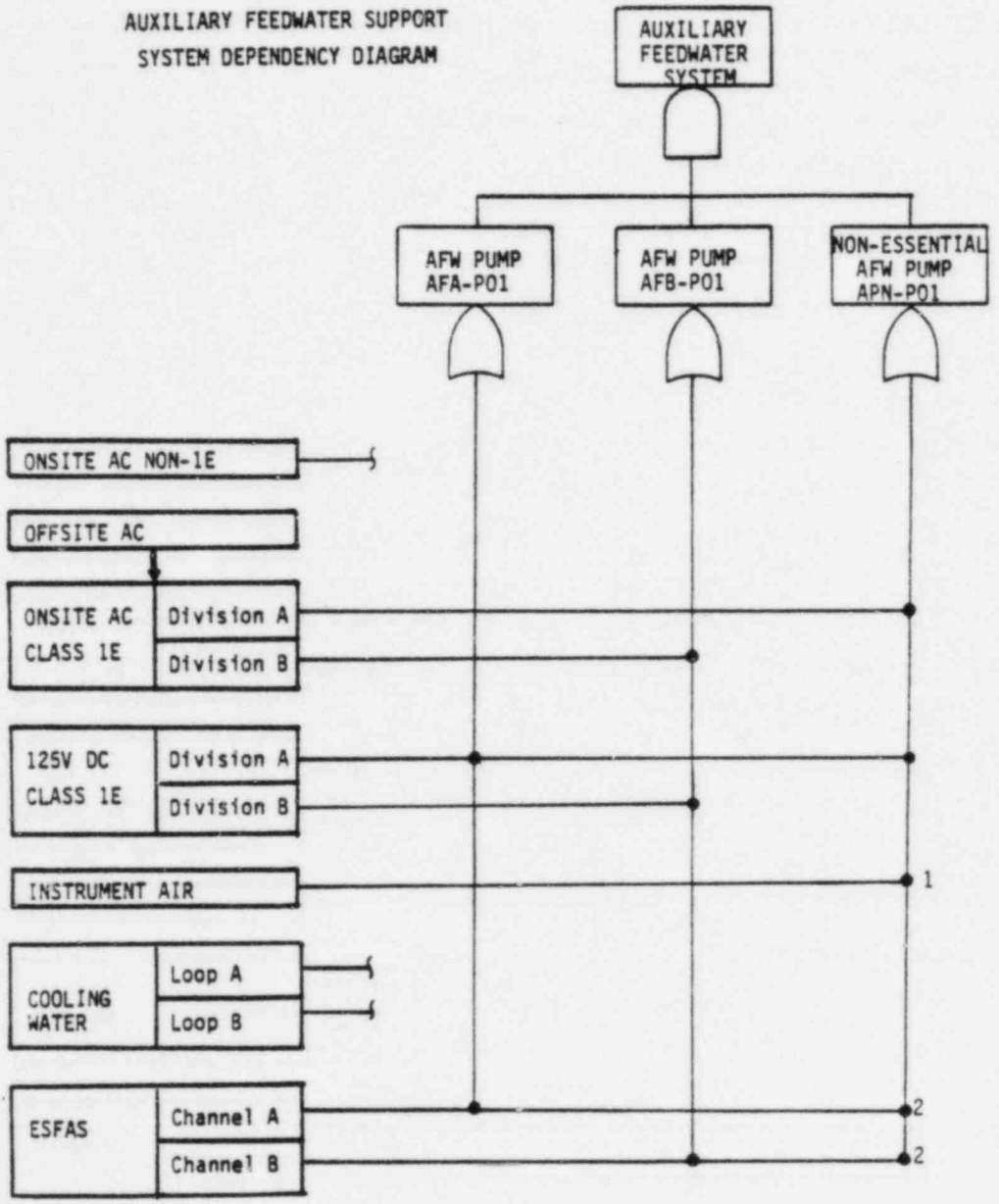
6.11.2 Assumptions

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. Operation of the none-essential motor-driven AFW pump is not included in the AFW unavailability analysis but is addressed in the AFW Restoration Analysis in Section 6.17. In addition, the AFW analysis does not credit the capability to transfer AFW flow from Units 2 or 3 to Unit 1.

2. For the Loss of Secondary Heat Sink and Spurious or Transient Induced PORV LOCA event trees, Failure to Deliver AFW is defined as failing to deliver sufficient AFW flow to at least one SG.

FIGURE 6.11.1-2
AUXILIARY FEEDWATER SUPPORT
SYSTEM DEPENDENCY DIAGRAM



[1]MFW Downcomer Isolation and Control Valves. For this system Instrument Air has a nitrogen backup.

[2]The AFAS closes valves UV4 and UV1.

3. For the PORV LOCA following SGTR event tree, Failure to Deliver AFW to One SG is defined as failing to deliver sufficient AFW flow to the unaffected SG.

4. Sufficient AFW flow is defined as flow from one AFW pump delivered to at least one SG.

5. Passive failures (breach of pressure boundary events) of the AFW system are not considered. Pipe rupture and missile evaluations are not within the scope of work.

6. Operator action to man lly actuate the AFW system or to re-establish AFW flow is not considered. Recovery of the AFW system is addressed in a separate analysis. (Section 6.17).

7. The startup suction strainers located in the suction line of each AFW pump have been removed.

8. System boundaries are defined to be the SG inlet nozzles to the condensate water storage tank.

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 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 or Transient Induced 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 following 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 Auxiliary Feedwater flow or operation of the non-essential auxiliary feedwater pump.

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 PVNGS
AUXILIARY FEEDWATER SYSTEM

Case Number	Description	Failure Probability (Median Value)	Error Factor
One	Failure to deliver AFW to at least one SG - System Unavailability	1.3E-3[1]	7
Two	Failure to deliver AFW to at least one SG given loss of MFW - System Unavailability	1.6E-3[1]	7
Three	Failure to deliver AFW to at least one SG given loss of 5% MFW to both SGs - System Unavailability		
	(a) Manual PORV Design	2.1E-3[1]	7
	(b) Automatic PORV Design	2.4E-3	6
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	2.9E-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 or operation of the non-essential AFW pump. See Section 6.17 for restoration analysis.

TABLE 6.11.3-2
DOMINANT CUTSETS FOR PVNGS AUXILIARY FEEDWATER SYSTEM

Case Number		Cutset	Description	% of Total Failure Probability
One	1.	APTA2414	Turbine pump fails to start	12.4%
		and		
		APMV2399	Motor pump in maintenance	
	2.	FSER2029	AFAS-2 failure and	10.5
		FSER2417	AFAS-1 failure	
	3.	APTV2398	Turbine pump in maintenance	6.5%
		and		
		AVNZ2427	Motor pump suction valve closed	
	4.	APMV2399	Motor pump in maintenance and	6.5%
		AVNS2410	Turbine pump suction valve closed	
Two	1.	APTA2414	Turbine pump fails to start and	9.7%
		APMV2399	Motor pump in maintenance	
	2.	FSER2029	AFAS-2 failure and	8.2%
		FSER2417	AFAS-1 failure	
	3.	APTV2398	Turbine pump in maintenance	5.0%
		and		
		AVNZ2427	Motor pump suction valve closed	
	4.	APMV2399	Motor pump in maintenance	5.0%
		and		
		AVNZ2410	Turbine pump suction valve closed	
Three (a) Manual PORV Design	1.	APTA2414	Turbine pump fails to start	6.6%
		and		
		APMV2399	Motor pump in maintenance	
	2.	FSER2029	AFAS-2 failure and	5.6%
		FSER2417	AFAS-1 failure	
	3.	APTA2414	Turbine pump fails to start	4.2%
		and		
		EDDJ2817	DG E-PEB-G002 fails to start	
		and		
		EBGP2682	Grid collapse on turbine trip	
(b) Auto-PORV Design	1.	APTA2414	Turbine pump fails to start and	8%
		APMV2399	Motor Pump in Maintenance	
	2.	FSER2029	AFAS-2 Failure and	6%
		FSER2417	AFAS-1 Failure	

TABLE 6.11.3-2
(Continued)
DOMINANT CUTSETS FOR PVNGS AUXILIARY FEEDWATER SYSTEM

Case Number	Cutset	Description	% of Total Failure Probability
Four	1. AVCA2397	Check valve V079 fails to open	8.8%
	2. APTA2414	Turbine pump fails to start	5.1%
	APMV2399	and Motor pump in maintenance	
	3. FSER2029	AFAS-2 failure and	4.3%
	FSER2417	AFAS-1 failure	
Five	1. AICP2970	AFW flow control system malfunction	100%
	AZZ02971	Operator fails to take action	
Six	1. AICP2972	AFW flow control system malfunction	97%
	AZZ02973	Operator fails to take action	
	2. MICP2974	Feedwater control system malfunction	3%
	MZZ02975	Operator fails to take action	
Seven	1. AICP2972	AFW flow control system malfunction	100%
	AZZ02973	Operator fails to take action	

6.12 STEAM GENERATOR BLOWDOWN SYSTEM

Fault tree logic diagrams were used to calculate various Steam Generator Blowdown System (SGBS) failure probabilities that were used as input to the SGTR event trees. The following fault tree models were developed for evaluation:

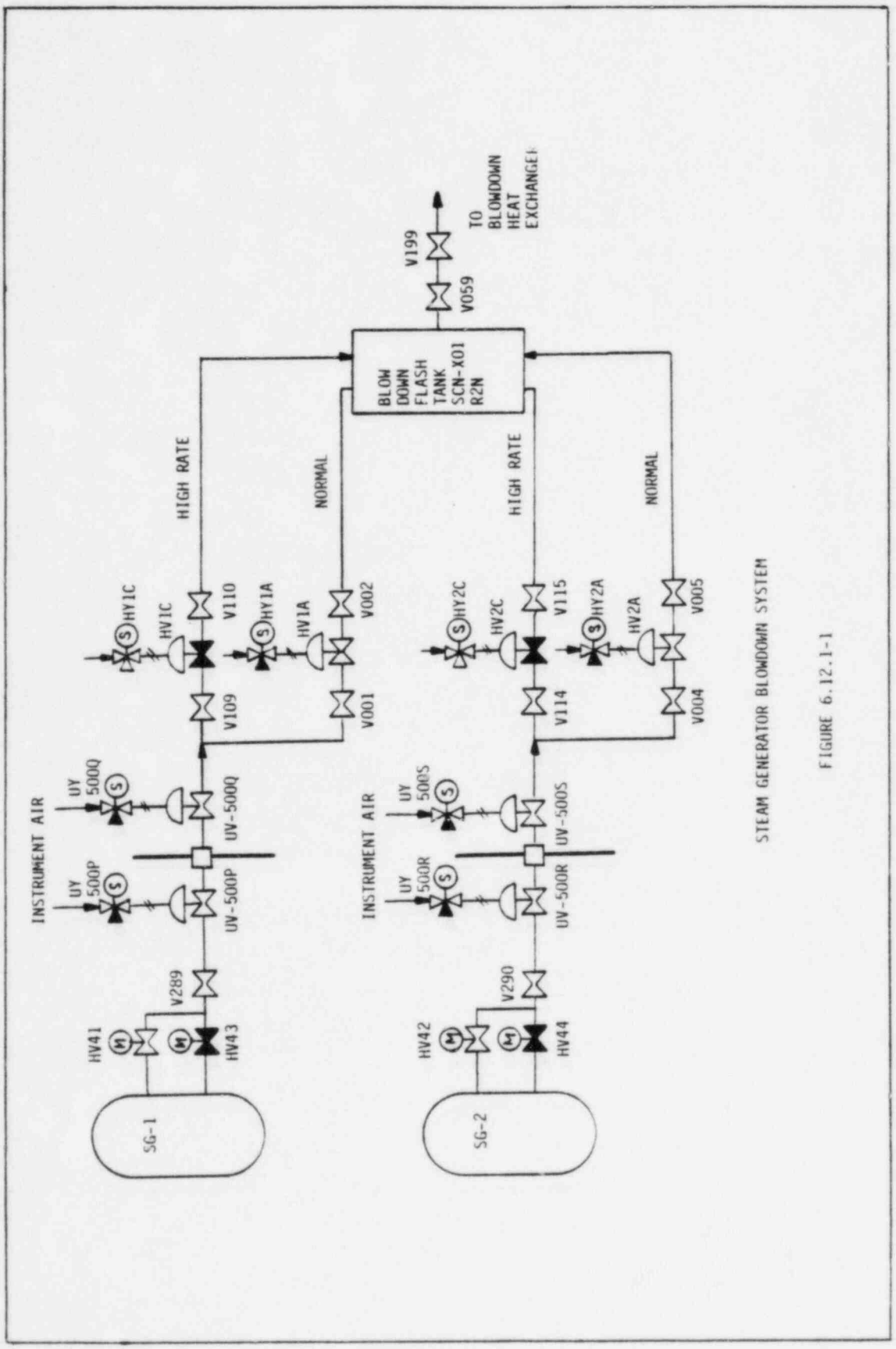
- Failure to Initiate Blowdown from the Affected SG (SG-2)
- Failure to Open Blowdown Isolation Valves on SG-2 (most affected SG)
- Failure to Open Blowdown Isolation Valves on SG-1 (least affected SG)
- Failure to Initiate Blowdown from Both Steam Generators (least affected and most affected SGs)

It should be noted that for SGTR with coincident LOOP, the SGBS is unavailable.

6.12.1 System Description

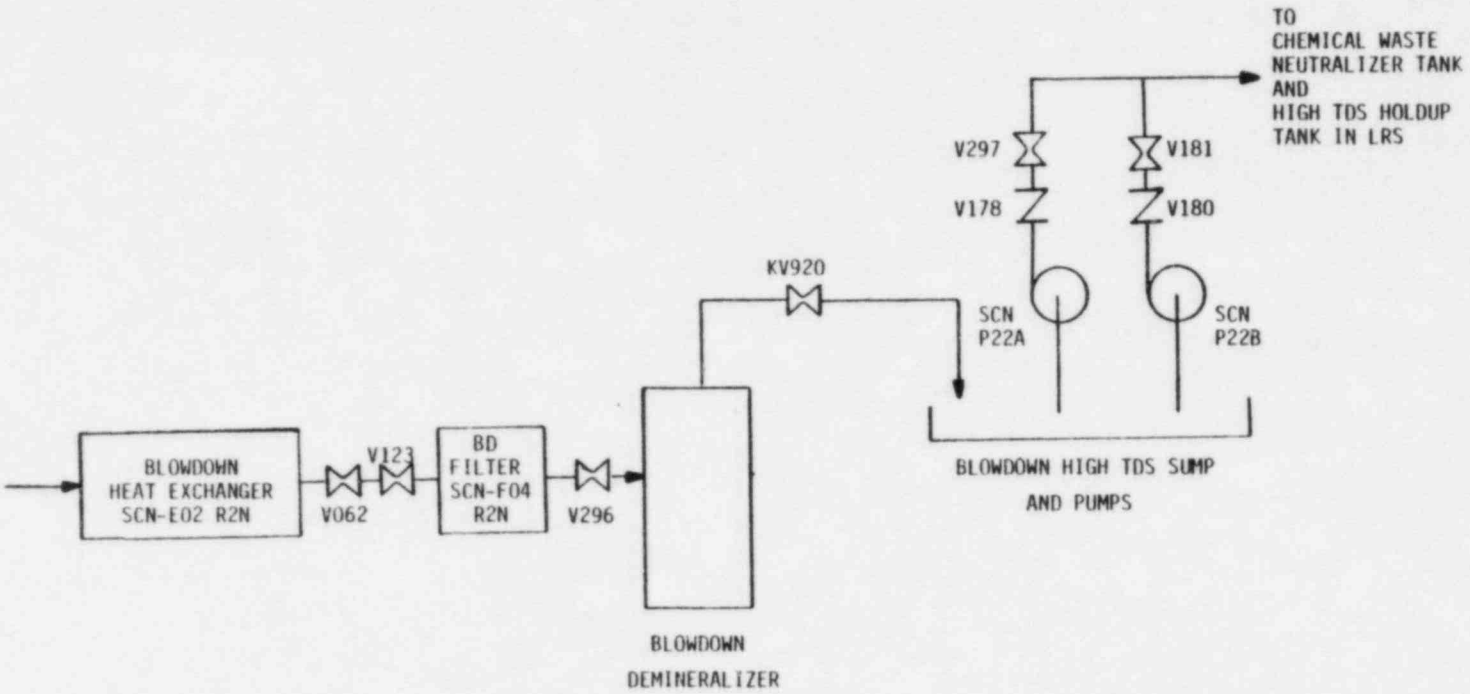
A schematic of the PVNGS Steam Generator Blowdown System (SGBS) is presented in Figures 6.12.1-1 and 6.12.1-2. The SGBS processes water from the tube bundle area of the steam generators. The blowdown water is filtered and purified to remove any impurities. Then, if meeting appropriate specifications, it is returned to the Condensate System for reuse. The SBCS is an integral part of the Secondary Chemistry Control System (SCCS).

Each SG is equipped with its own blowdown processing line with the capability of blowing down either the primary inlet or primary outlet regions of the SG shell side. Each blowdown line leaves the containment through its own penetration and discharges into the steam generator



STEAM GENERATOR BLOWDOWN SYSTEM

FIGURE 6.12.1-1



STEAM GENERATOR BLOWDOWN SYSTEM (continued)

FIGURE 6.12.1-2

blowdown flash tank. The liquid position flows through the blowdown heat exchanger to the blowdown filter where the major portion of suspended particles are removed. After filtration, the blowdown fluid is processed by the blowdown demineralizer.

The containment isolation valves are normally open and can be remotely operated from the main control room. These valves automatically close upon receipt of a Main Steam Isolation Signal (MSIS), an Auxiliary Feedwater Actuation Signal (AFAS) or a Safety Injection Actuation Signal (SIAS). Any of these signals will close the valves. The valves fail closed on loss of air.

The blowdown is measured for radioactivity in order to detect primary to secondary leakage. If significant steam generator tube leaks exist, blowdown flow from the demineralizer is routed to the Blowdown High Total Dissolved Solids (TDS) Sump and to the Chemical Waste Neutralizer Tank. From there, the liquid is processed by the Liquid Radwaste System (LRS) via the High TDS holdup tank.

The Blowdown support system dependency diagram is provided in Figure 6.12.1-3.

6.12.2 Assumptions

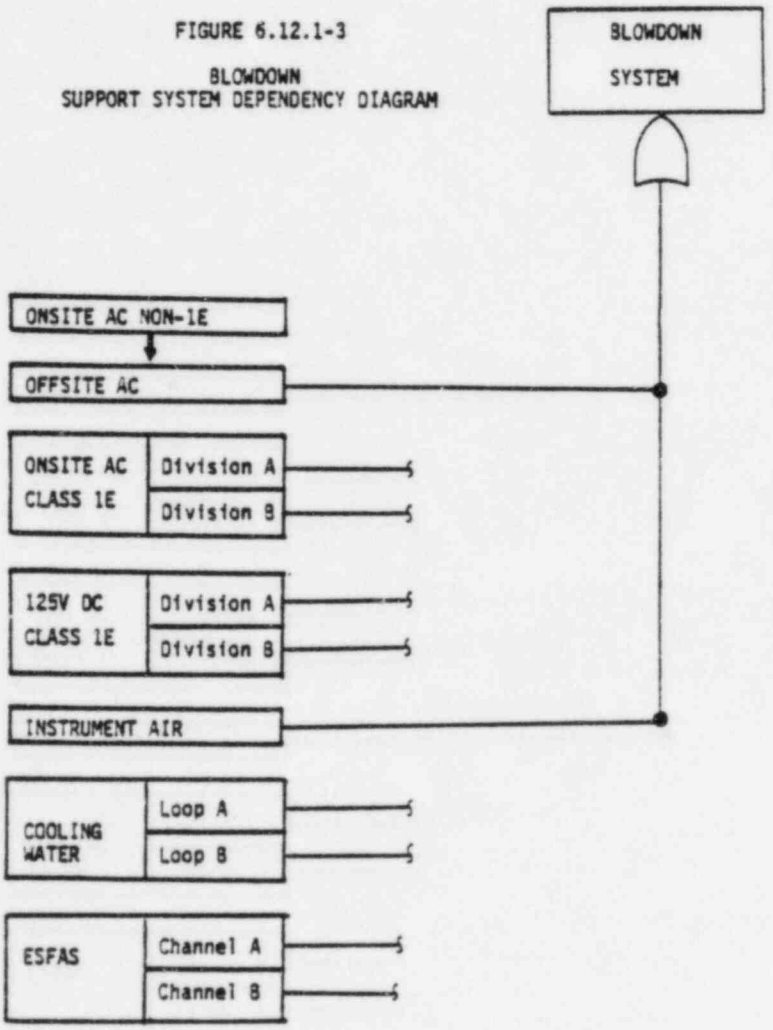
The following assumptions were made in performing the fault tree analyses:

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, blowdown system boundaries are assumed to include flow to the Chemical Waste Neutralizer Tank. Flow from the tank to the Liquid Radwaste System is not modelled in the fault tree. The LRS is assumed to have sufficient capacity to store the desired quantity of blowdown inventory for subsequent processing.

FIGURE 6.12.1-3

BLOWDOWN
SUPPORT SYSTEM DEPENDENCY DIAGRAM



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 SGBS operation.

4. The blowdown flowpath shown in Figures 6.12.1-1 and 6.12.1-2 is inferred from information available in Reference (7).

5. The flowpaths to the condenser have been isolated prior to initiation of flow to the Liquid Radwaste System, i.e., there will be no flow diversion to this area.

6. Flow to the Blowdown Flash Tank is aligned for the "normal rate".

7. Motor valves HV-41, HV-42, HV-43 and HV-44 are fail as is. HV-43 and HV-44 are assumed to be closed; HV-41 and HV-42 are assumed to be open.

8. One of the two BD High TDS sump pumps is sufficient to provide adequate flow to the Chemical Waste Neutralizer Tank.

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 2. This model is applicable for tube rupture(s) in one SG. (Assumed to be SG-2).

- The probability of failing to initiate blowdown flow from Steam Generator 2. This fault tree refers only to opening the blowdown isolation valves on the most affected SG (SG-2) assuming tube ruptures have occurred in two steam generators.

- The probability of failing to initiate blowdown flow from Steam Generator 1. This fault tree refers only to opening the blowdown isolation valves on the least affected SG (SG-1) 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 PVNGS
STEAM GENERATOR BLOWDOWN SYSTEM

Case Number	Description	Failure Probability (Median Value)	Error Factor
One	Failure to Initiate Blowdown from SG-2 - System Unavailability	7.2E-2	3
Two	Failure to Open Blowdown Isolation Valve on SG-2 - System Unavailability	1.7E-2	3
Three	Failure to Open Blowdown Isolation Valve on SG-1 - System Unavailability	1.7E-2	3
Four	Failure to initiate Blowdown from Both Steam Generators - System Unavailability	5.1E-2	3

TABLE 6.12.3-2

DOMINANT CUTSETS FOR PNVGS STEAM GENERATOR BLOWDOWN SYSTEM

Case Number	Cutset	Description	% of Total Failure Probability
One	1. BVNO2907	Operator fails to open manual valve KV-920	56%
	2. BVZO2902	Operator fails to open blow-down containment isolation valves	17%
Two	1. BVZO2902	Operator fails to open blow-down containment isolation valves on SG-2	69%
	2. BVDA2901	UV-500R fails to open	7.7%
	3. BVDA2904	UV-500S fails to open	7.7%
Three	1. BVZO2920	Operator fails to open blow-down containment isolation valves on SG-1	69%
	2. BVDA2918	UV-500P fails to open	7.7%
	3. BVDA2921	UV-500Q fails to open	7.7%
Four	1. BVNO2907	Operator fails to open manual valve KV-920	73%

6.13 ALTERNATE SECONDARY HEAT REMOVAL CAPABILITY

6.13.1 System Description

In the event of a total loss of all feedwater, an alternate method for decay heat removal involves the rapid depressurization of the steam generators and the use of low head pumps for cooling. The preferred source of low pressure feedwater is the condensate system. The condensate pumps (differential head of 1030 feet) can use water from the condenser hotwell and through the use of the feed pump bypass line, deliver makeup directly to each steam generator. The Alternate Secondary Heat Removal Capability will refer to the use of the Condensate System provide feed flow following a loss of main and auxiliary feedwater. (The analysis does not consider the capability to transfer condensate flow from Units 2 or 3 to Unit 1.)

The Condensate System is composed of a surface condenser, three 50% capacity pumps, low pressure feedwater heaters and the required piping and valves. A simplified flow diagram of the condensate feedwater system is given in Figure 6.13.1-1. The condensate system can supply water directly to each steam generator via the condensate pumps following depressurization of the secondary system to below the pump shutoff head. The condensate flow bypasses the feedwater pumps and the high pressure feedwater heaters and deliver flow to the downcomer MFW lines.

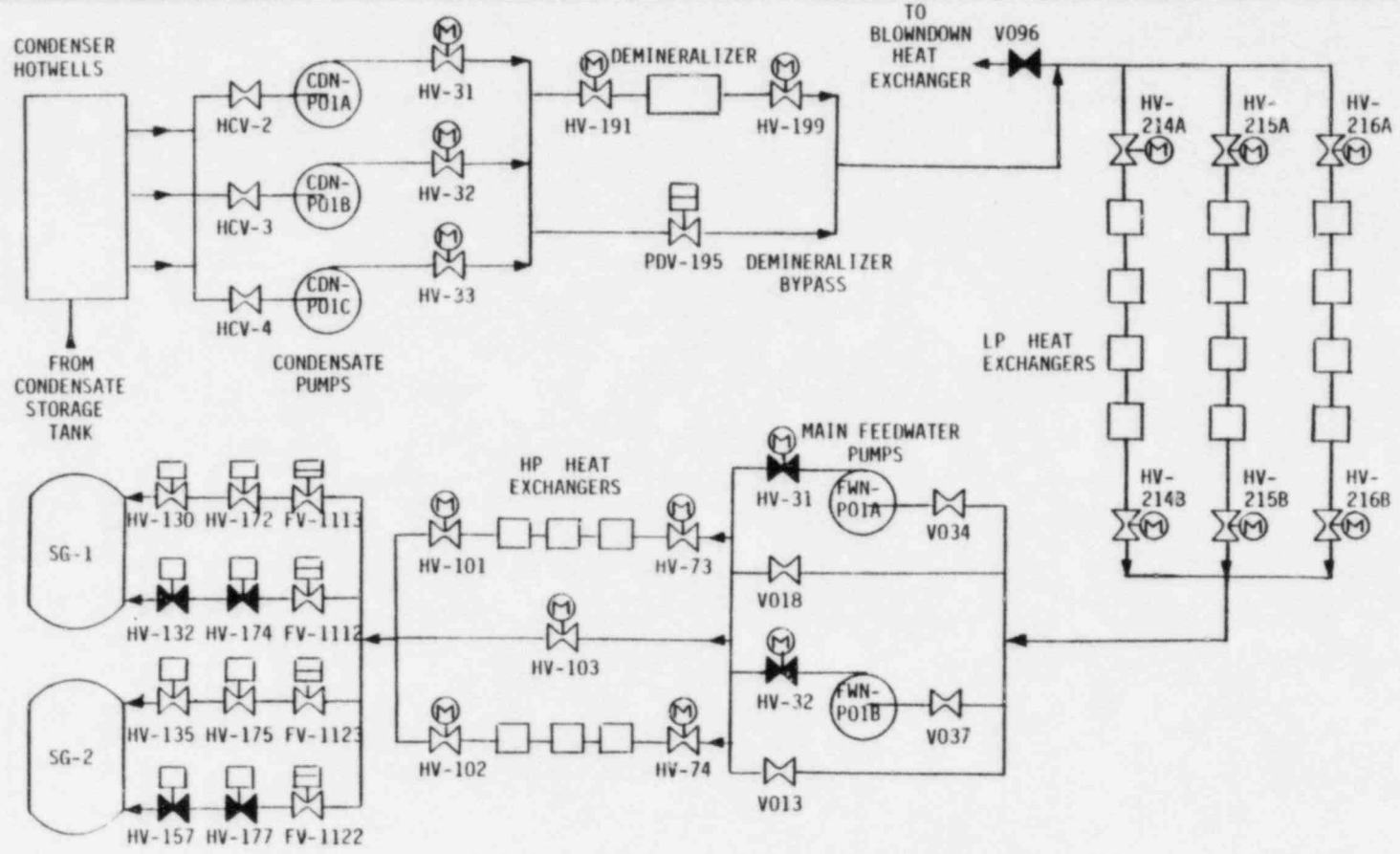
The Alternate Secondary Heat Removal support system dependency diagram is provided in Figure 6.13.1-2.

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 pumps.

2. Sufficient flow is defined as the flow from one condensate pump delivered to one steam generator.



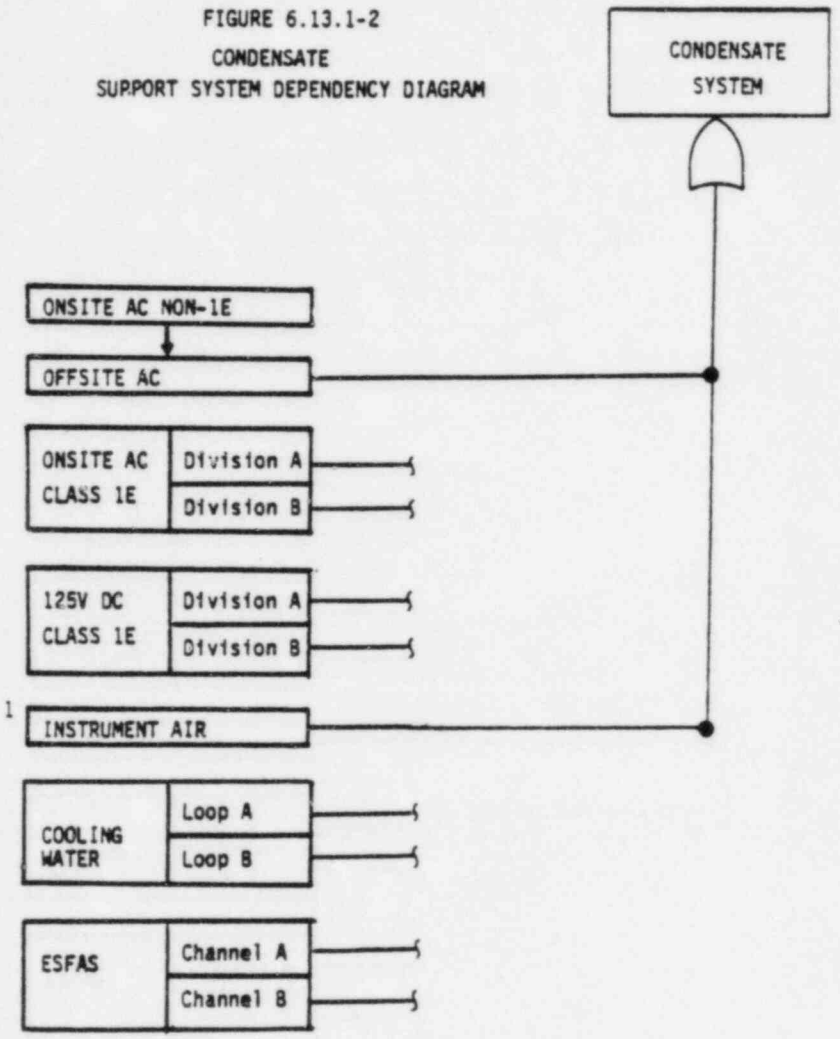
ALTERNATE SECONDARY CAPABILITY-CONDENSATE PUMP ALIGNMENT

FIGURE 6.13.1-1

FIGURE 6.13.1-2

CONDENSATE

SUPPORT SYSTEM DEPENDENCY DIAGRAM



[1]Downcomer MFW Isolation and Control Valves include Nitrogen backup to Instrument Air.

3. Both steam generators are intact for secondary flow delivery.

4. Pressure on the secondary side will be reduced using the atmospheric dump system.

5. The operator has a written procedure detailing the necessary actions to establish the alternate flow from the condensate pumps.

6. One condensate pump (CDN-POIC) is unavailable due to maintenance.

7. Failure of the condensate pump recirculation line will result in condensate pump failure.

8. Failure to bypass the main feedwater pumps and high pressure feedwater heaters and close the line to the blowdown heat exchanger results in failure to deliver sufficient condensate flow.

9. The following operator actions to align the condensate system to deliver flow directly to the steam generators are considered:

   - Operator action to bypass the main feedwater pumps and feedwater heaters.

Open Motor Valves	HV-103
Open Manual Valves	V018
	V013
Close Manual Valve	V096

     The Motor-operated valve may be operated from the control room.

   - Operator action to assure correct positioning of the feedwater economizer and downcomer control valves and isolation valves.

The operator will have approximately 60 minutes to align the system.

6.13.3 Results

The fault tree logic diagram for Failure of the Alternate Secondary Heat Removal 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 capability - condensate pump alignment

- Failure of the alternate secondary system - condensate pump alignment given loss of MFW and 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. In addition, the probability of restoration of AC power following the loss of AFW is incorporated into the system 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 PVNGS
ALTERNATE SECONDARY HEAT REMOVAL CAPABILITY

Case Number	Description	Failure Probability (Median Value)	Error Factor
One	Failure of Alternate Secondary Capability - System Unavailability	5.8E-2	3
Two	Failure of Alternate Secondary Capability given loss of MFW and AFW - System Unavailability	5.5E-1	1.56

TABLE 6.13.3-2

DOMINANT CUTSETS FOR PVNGS ALTERNATE SECONDARY HEAT REMOVAL CAPABILITY

Case Number	Cutset	Description	% of Total Failure Probability
One	1. MPZ02953	Operator Fails to Align Condensate System	84.9%
	2. EBGP2682	Grid Collapse turbine trip	2.1%
	3. ECBV2810	Battery E-NKN-F17 Unavailable	2.1%
Two	1. EBGP2680	Spurious Grid Collapse	85%
	2. MPZ02953	Operator Fails to Align the Condensate System	8.1%

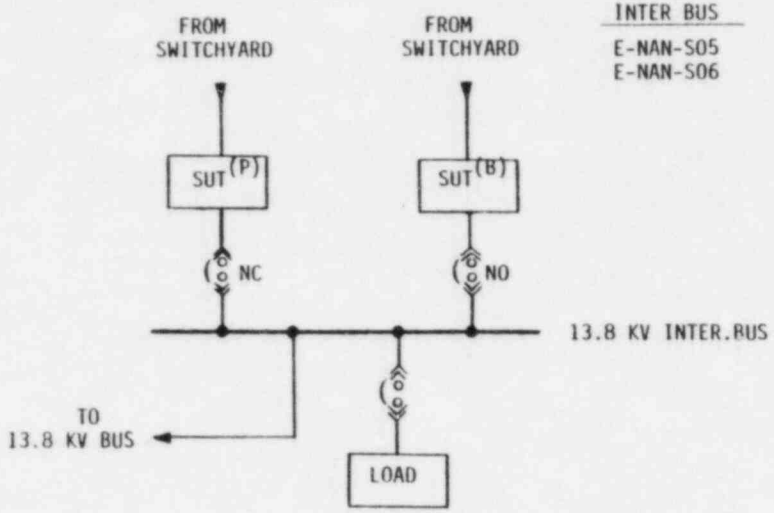
6.14 ELECTRICAL DISTRIBUTION SYSTEM

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 PVNGS EDS are provided in Figures 6.14.1-1 to 6.14.1-10. 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 13.8KV, 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 start up transformers. In the event of failure of the unit auxiliary



13.8 KV INTER BUS	13.8 KV BUS	SUT(P)	SUT(B)
E-NAN-S05	E-NAN-S03	E-NAN-X03	E-NAN-X01
E-NAN-S06	E-NAN-S04	E-NAN-X02	E-NAN-X01

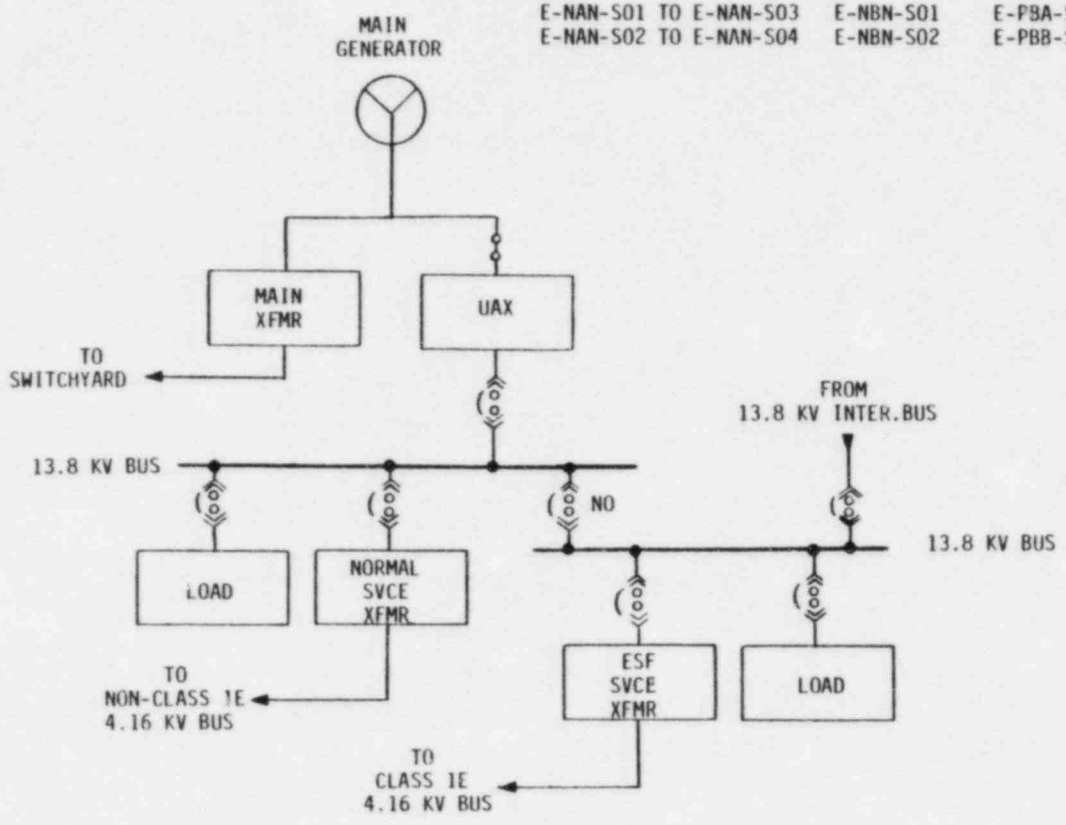
P... PREFERRED STARTUP TRANSFORMER

Q... ALTERNATE STARTUP TRANSFORMER

TYPICAL 13.8 KV INTERMEDIATE BUS SCHEMATIC

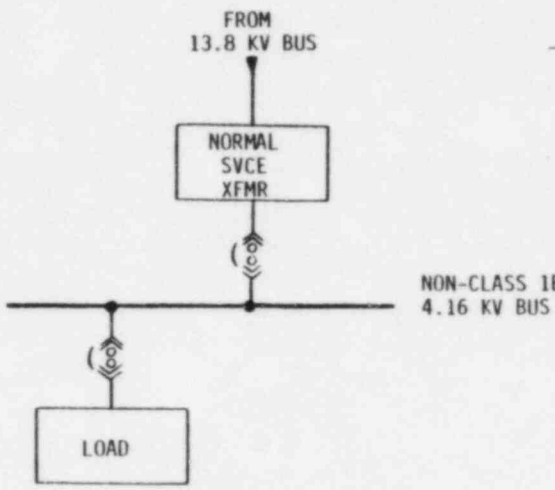
FIGURE 6.14.1-1

13.8 KV BUS	NON-CLASS 1E 4.16 KV BUS	CLASS 1E 4.16 KV BUS	NORMAL SVCE XFMR	ESF SVCE XFMR
E-NAN-S01 TO E-NAN-S03	E-NBN-S01	E-PBA-S03	E-NBN-X01	E-NBN-X03
E-NAN-S02 TO E-NAN-S04	E-NBN-S02	E-PBB-S04	E-NBN-X02	E-NBN-X04



TYPICAL 13.8 KV BUS SCHEMATIC

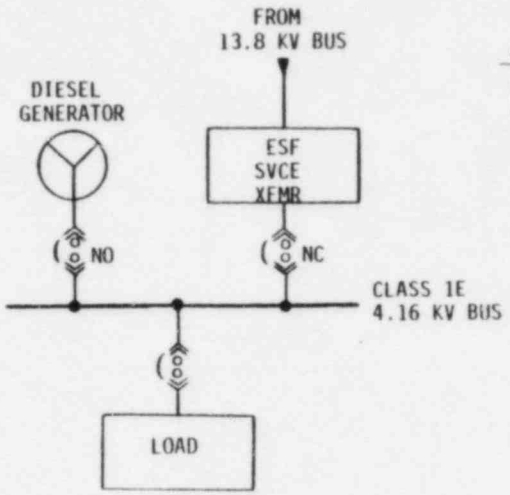
FIGURE 6.14.1-2



NON-CLASS 1E 4.16 KV BUS	NORMAL SVCE XFMR
E-NBN-S01	E-NBN-X01
E-NBN-S02	F-NBN-X02

TYPICAL NON-CLASS 1E 4.16 KV BUS SCHEMATIC

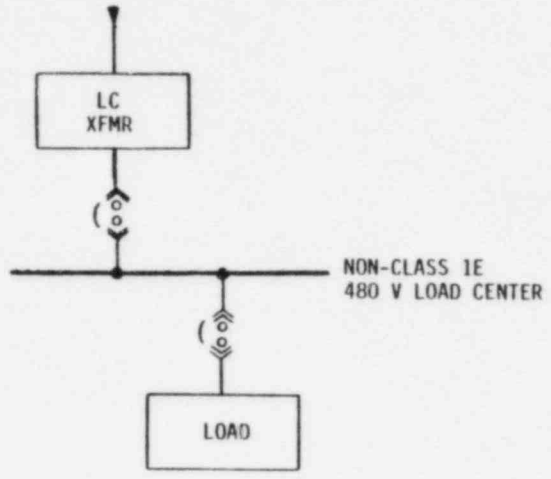
FIGURE 6.14.1-3



DIESEL GENERATOR	ESF SVCE XFMR	CLASS 1E 4.16 KV BUS
E-PEA-G01	E-NBN-X03	E-PBA-S03
E-PEB-G02	E-NBN-X04	E-PBB-S04

TYPICAL CLASS 1E 4.16 KV BUS SCHEMATIC

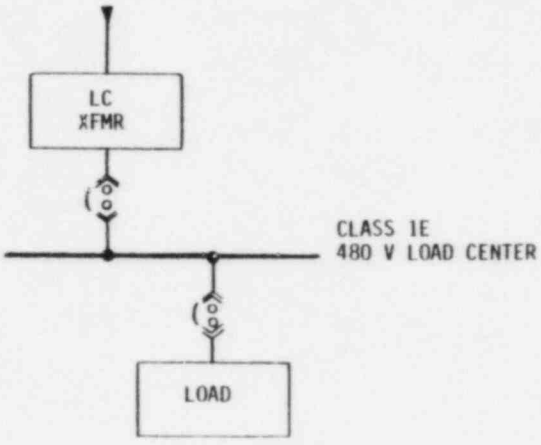
FIGURE 6.14.1-4



NON-CLASS 1E 480 V LC	13.8 KV BUS	NON-CLASS 1E 480 V LC	13.8 KV BUS
E-NGN-L13	E-NAN-S01	E-NGN-L20	E-NAN-S02
E-NGN-L19	E-NAN-S01	E-NGN-L26	E-NAN-S02
E-NGN-L05	E-NAN-S01	E-NGN-L14	E-NAN-S02
E-NGN-L21	E-NAN-S01	E-NGN-L22	E-NAN-S02
E-NGN-L15	E-NAN-S01	E-NGN-L28	E-NAN-S02
E-NGN-L23	E-NAN-S01	E-NGN-L08	E-NAN-S02
E-NGN-L09	E-NAN-S01	E-NGN-L24	E-NAN-S02
E-NGN-L07	E-NAN-S01	E-NGN-L30	E-NAN-S02
E-NGN-L01	E-NAN-S01	E-NGN-L18	E-NAN-S02
E-NGN-L25	E-NAN-S01	E-NGN-L04	E-NAN-S02
E-NGN-L11	E-NAN-S01	E-NGN-L10	E-NAN-S02
E-NGN-L17	E-NAN-S01	E-NGN-L12	E-NAN-S02
E-NGN-L03	E-NAN-S01	E-NGN-L02	E-NAN-S02
		E-NGN-L06	E-NAN-S02
		E-NGN-L16	E-NAN-S02

TYPICAL NON-CLASS 1E 480 V LOAD CENTER SCHEMATIC

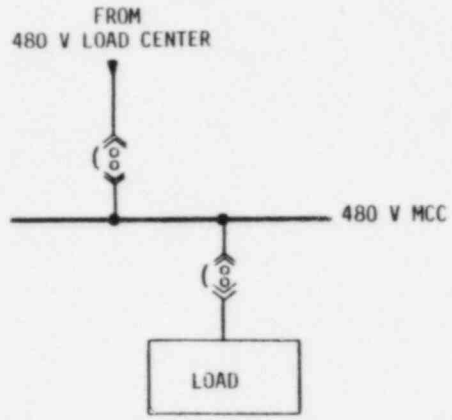
FIGURE 6.14.1-5



CLASS 1E 480 V LC	CLASS 1E 4.16 KV BUS
E-PGA-L31	E-PBA-S03
E-PGA-L33	E-PBA-S03
E-PGA-L35	E-PBA-S03
E-PGB-L36	E-PBB-S04
E-PGB-L34	E-PBB-S04
E-PGB-L32	E-PBB-S04

TYPICAL CLASS 1E 480 V LOAD CENTER SCHEMATIC

FIGURE 6.14.1-6

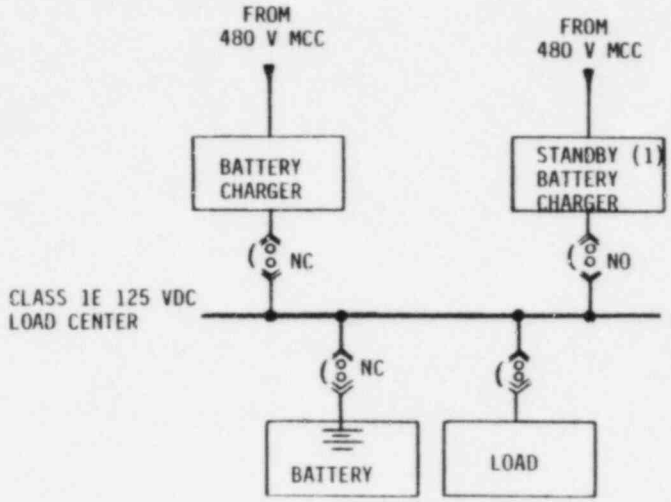


480 V MCC	480 V LC	480 V MCC	480 V LC
E-NHN-M21	E-NGN-L13	E-NHN-M18	E-NGN-L26
E-NHN-M11	E-NGN-L13	E-NHN-M06	E-NGN-L14
E-NHN-M27	E-NGN-L05	E-NHN-M24	E-NGN-L14
E-NHN-M19(1)	E-PGA-L35	E-NHN-M22	E-NGN-L08
E-NHN-M23	E-NGN-L15	E-NHN-M20(1)	E-PGB-L36
E-NHN-M17	E-NGN-L19	E-NHN-M16	E-NGN-L20
E-NHN-M15	E-NGN-L09	E-NHN-M04	E-NGN-L04
E-NHN-M01	E-NGN-L07	E-NHN-M30	E-NGN-L04
E-NHN-M09	E-NGN-L07	E-NHN-M10	E-NGN-L10
E-NHN-M05	E-NGN-L01	E-NHN-M08	E-NGN-L02
E-NHN-M07	E-NGN-L01	E-NHN-M02	E-NGN-L02
E-NHN-M13	E-NGN-L25	E-NHN-M26	E-NGN-L06
E-NHN-M03	E-NGN-L25	E-NHN-M28	E-NGN-L06
E-NHN-M25	E-NGN-L03	E-NHN-M50	E-NGN-L06
E-PHA-M31	E-PGA-L31	E-NHN-M14	E-NGN-L16
E-PHA-M37	E-PGA-L33	E-PHB-M36	E-PGB-L36
E-PHA-M33	E-PGA-L33	E-PHB-M34	E-PGB-L34
E-PHA-M35	E-PGA-L35	E-PHB-M32	E-PGB-L32
		E-PHB-M38	E-PGB-L32

1. MCC TRIPS ON SIAS

TYPICAL 480 V MCC SCHEMATIC

FIGURE 6.14.1-7

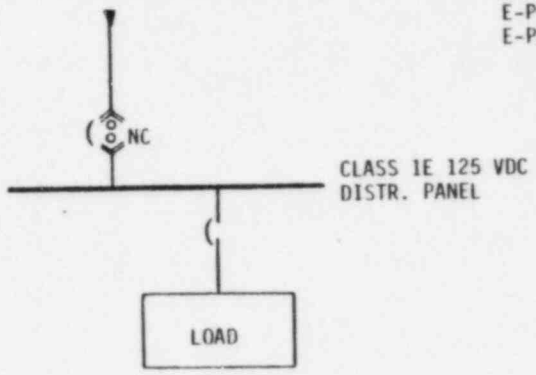


125 VDC LC	BATTERY	BATT.CHGR.	480 V MCC
E-PKA-M41	E-PKA-F11	E-PKA-H11	E-PHA-M35
		E-PKA-H15(1)	E-PHA-M33
E-PKC-M43	E-PKC-F13	E-PKC-H13	E-PHA-M31
		E-PKA-H15(1)	E-PHA-M33
E-PKB-M42	E-PKB-F12	E-PKB-H12	E-PHB-M36
		E-PKB-H16(1)	E-PHB-M34
E-PKD-M44	E-PKD-F14	E-PKD-H14	E-PHB-M32
		E-PKB-H16(1)	E-PHB-M34

1. THE STANDBY BATTERY CHARGER OUTPUT SWITCHES ARE MECHANICALLY INTERLOCKED TO OFFER THE POSSIBILITY OF EITHER BOTH OPEN OR ONE OPEN AND ONE CLOSED AT ANY TIME.

TYPICAL CLASS 1E 125 VDC LOAD CENTER SCHEMATIC

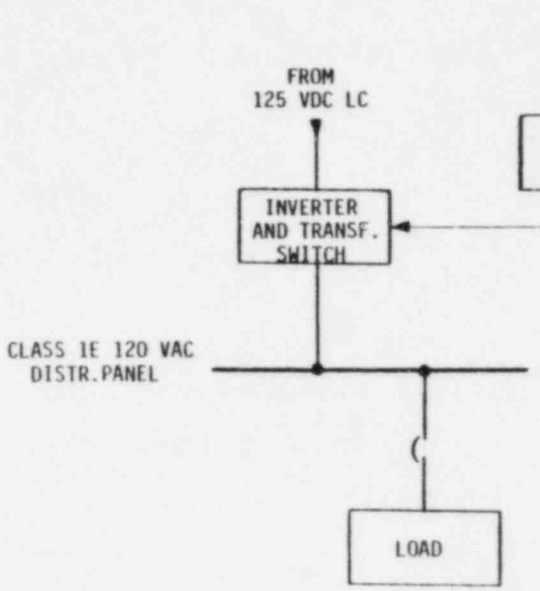
FIGURE 6.14.1-8



125 VDC DP	125 VDC LC
E-PKA-D21	E-PKA-M41
E-PKC-D23	E-PKC-M43
E-PKB-D22	E-PKB-M42
E-PKD-D24	E-PKD-M44

TYPICAL CLASS 1E 125 VDC DISTRIBUTION PANEL SCHEMATIC

FIGURE 6.14.1-9



120 VAC DP	125 VDC LC	INVERTER	VOLT. REG	480 V MCC
E-PNA-D25	E-PKA-M41	E-PNA-N11	E-PNA-V25	E-PHA-M35
E-PNC-D27	E-PKC-M43	E-PNC-N13	E-PNC-V27	E-PHA-M31
E-PNB-D26	E-PKB-M42	E-PNB-N12	E-PNB-V26	E-PHB-M36
E-PND-D28	E-PKD-M44	E-PND-N14	E-PND-V28	E-PHB-M32

TYPICAL CLASS 1E 120 VAC DISTRIBUTION PANEL SCHEMATIC

FIGURE 6.14.1-10

transformer, a generator trip, or backup protective trip, fast transfer to offsite power (switchyard) maintains continuity of power to the 13.8KV and 4.16KV non-class 1E buses.

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 powered from non-class 1E AC buses 13.8 KV E-NAN-S03 and E-NAN-S04. In the event of loss of the preferred power source, 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. The 13.8KV intermediate buses E-NAN-S05 and E-NAN-S06 are normally powered from the switchyard via start up transformers E-NAN-X03 and E-NAN-X02 respectively.

2. No credit was taken for powering the class 1E 4.16KV buses E-PBA-S03 and E-PBB-S04 from the same preferred power source i.e., 13.8KV bus E-NAN-S03.

3. No credit was taken for cross connecting the non-class 1E 4.16KV buses E-NBN-S01 and E-NBN-S02.

4. Spurious opening of normally closed circuit breakers is not considered.

5. The 125 VDC non-class 1E control power for normally operating loads is available.

6. Battery charger E-PKA-H15 and E-PKB-H16 output switches are mechanically interlocked; therefore, battery chargers E-PKA-H15 and E-PKB-H16 backup battery chargers E-PKA-H11 and E-PKB-H12 respectively.

7. Operator action is required to realign class 1E 120 VAC power supply to the 480 VAC source.

8. Operator action is required to realign the 13.8KV intermediate buses to their backup sources.

6.14.3 Results

The results of this evaluation are in terms of fault tree logic diagrams. EDS interactions can be modelled by utilizing these logic diagrams as support branches to other fault trees.

6.15 COOLING WATER SYSTEMS

The Cooling Water Systems 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 these logic diagrams as support branches to other fault trees provides a consistent method of modelling these interactions between mitigating systems. The Cooling Water Systems fault tree logic diagrams were not independently evaluated, therefore, no quantitative results are provided in this section.

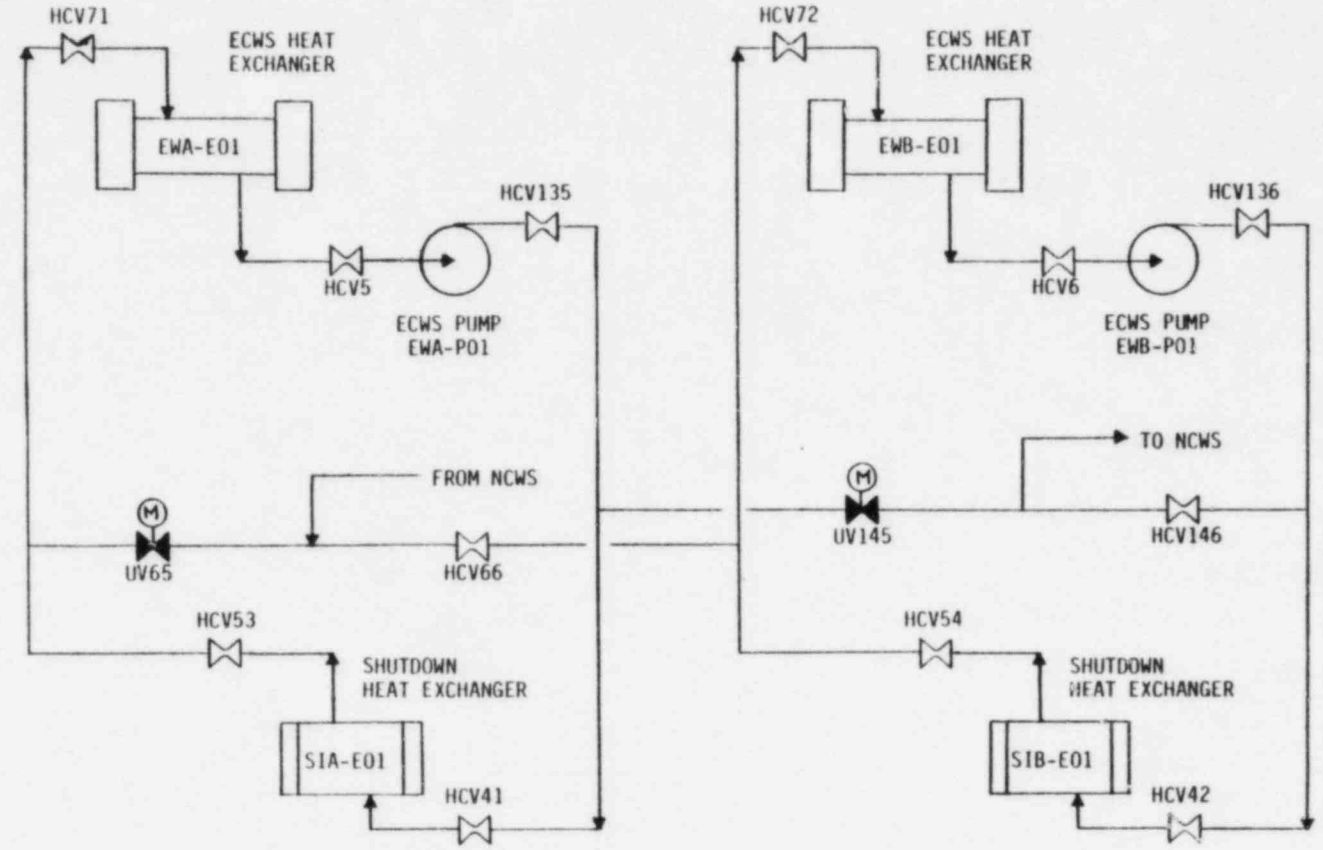
6.15.1 System Description

The Cooling Water Systems for the safety related and normal shutdwon components, as shown in Figure 6.15.1-1 and 6.15.1-2 are:

- Essential Cooling Water System (ECWS) and
- Essential Spray Pond System (ESPS).

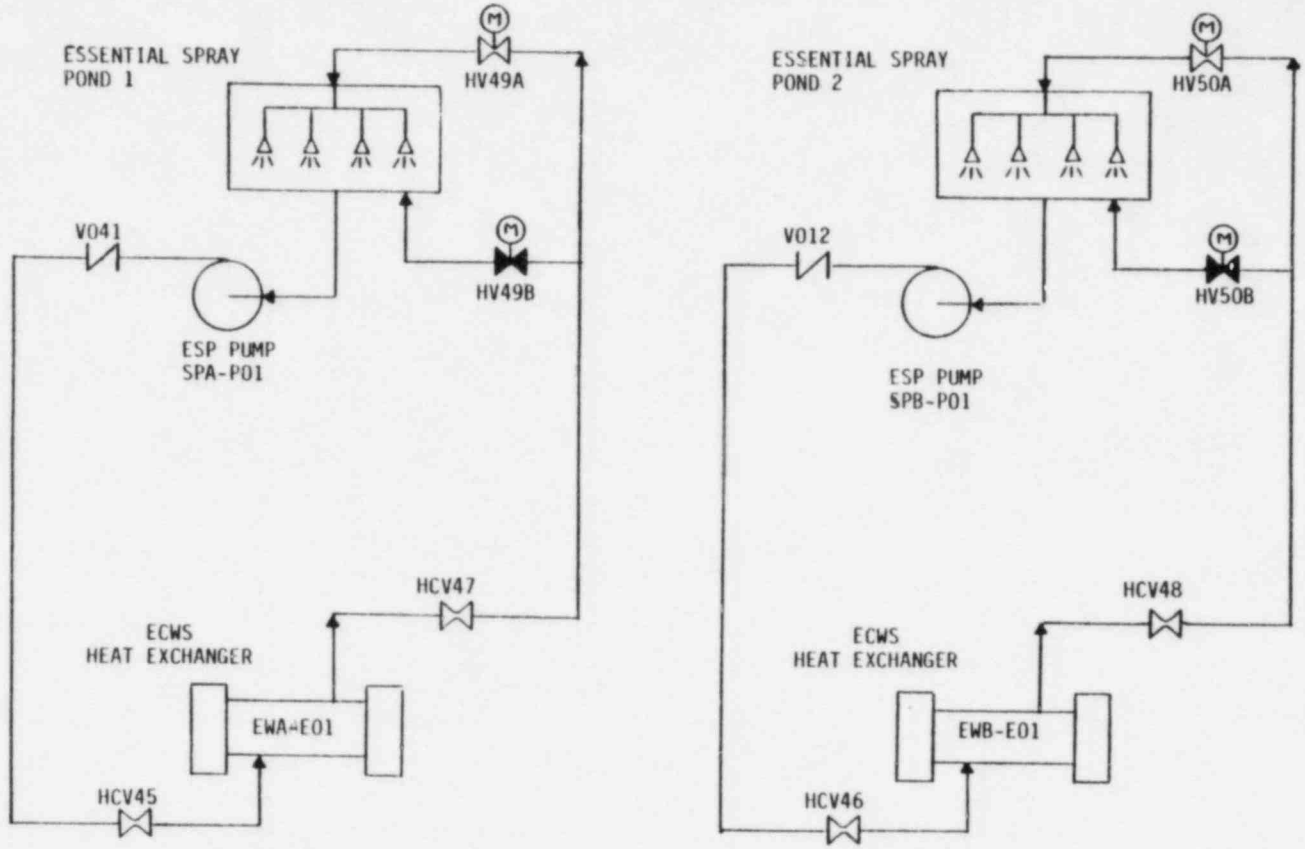
All heat absorbed by the systems through the nuclear components of the station is dissipated to the atmosphere via the essential spray ponds.

The ECWS consists of two independent, closed loop, safety-related trains. Either train of the ECWS is capable of supporting 100% of the cooling functions required for a safe reactor shutdown or required following an accident. Each train of the ECWS includes a 100 percent heat dissipation capacity heat exchanger (shell side), or 100 percent capacity pump, a surge tank and a chemical addition tank. The cooling water is pumped by the ECW pumps through the shell side of the ECWS heat exchangers, to the components being cooled and back to the pumps. The tube side of the heat exchangers is furnished with cooling water from the ESPS at a higher operating pressure than the shell side in order to prevent leakage into the ESPS from the ECWS.



ESSENTIAL COOLING WATER SYSTEM

FIGURE 6.15.1-1



ESSENTIAL SPRAY POND SYSTEM

FIGURE 6.15.1-2

Each train of the ECWS provides cooling for the following safety related components:

- Shutdown Cooling Heat Exchangers
- Essential Chillers

However, the ECWS can provide cooling water to the safety related

- Fuel Pool Heat Exchangers

and to the non-safety related following components:

- Reactor Coolant Pumps
- CEDM Coolers
- Normal Chillers
- Nuclear Sample Coolers

in the event the Nuclear Cooling Water System (NCWS), which normally cools these components, becomes inoperable. In this case the operator can align ECWS train A from the control room or locally align ECWS train B if ECWS train A fails.

During normal plant operation the ECWS is not operating.

The ESPS provides cooling water needed for those components that must operate following a loss-of-coolant accident (LOCA) and that are essential to a safe reactor shutdown:

- Standby diesel generator cooling systems
- Essential Cooling Water System (ECWS) Heat Exchangers.

The system consists of two redundant, safety-related ESPS trains. Each ESPS train in conjunction with the associated ECWS train is capable of supporting 100 percent of the cooling functions required for a safe shutdown or required following an accident. Each train includes a 100

percent capacity ESPS pump and a 100 percent heat dissipation capacity spray pond (ultimate heat sink). The water is pumped through the components being cooled, to the spray nozzles and back to the pump.

The ultimate heat sink consists of two Essential Spray Ponds (ESP) that are adjacent to each other. The two ESP are interconnected with redundant valves installed in their common wall in order to permit equalization of the water levels between EPS of the same unit. Discharge from the spray pond system is directed through the spray nozzles during operation of the sprays. During the time that the sprays are operating, the thermal load is dissipated to the air by the sprays and the surface heat exchange of the unsprayed area. During the time when the sprays are not operating, a part of the thermal load is dissipated to the atmosphere by the surface heat exchange of the total pond area, whereas the remainder goes into raising the spray pond temperature. During normal plant operation, the ESPS is not operating.

The motors of one ECWS pump and the related ESPS pump are connected to a Class 1E bus in one division and the motors of the other pumps to the other division. Loss of offsite power results in the shutdown and restarting of the ECWS and ESPS in accordance with the direct generator load sequencing.

Both trains of the ECWS and ESPS are actuated by any single or any combination of the following signals or operations:

- Safety injection actuation signal (SIAS)
- Control room ventilation and isolation actuation signal (CRVIAS)
- Control room essential filtration actuation signal (CREFAS)
- Diesel generator start signal (DGSS)
- Loss of offsite power signal (LOP)
- Manual start by control room

6.15.2 Analysis Assumptions

The following assumptions were made in performing the reliability analysis.

1. System failure is defined as the inability to deliver Essential Cooling Water to the required components. One 100 percent capacity train including a ECWS pump, a ECWS heat exchanger, a ESPS pump and an essential spray pond is assumed to provide sufficient cooling.

2. The only operator action considered is manual backup of the SIAS from the control room.

3. The ECWS and ESPS are not normally operating.

4. The motor valves HV49A and HV50A are FAI (fail as is) and are manually open.

5. It is assumed that components in train A receive SIAS-A and components in train B receive SIAS-B.

6. Since maintenance can only be performed on one ECW pump or on one ESP pump during plant operation, unavailability contributions due to pump maintenance are included only for ECW pump EWA-P01 and ESP pump SPA-P01 respectively.

6.15.3 Results

The results of this evaluation consist of fault tree logic diagrams. Cooling Water Systems interactions can be modelled by utilizing these logic diagrams as support branches to other fault trees.

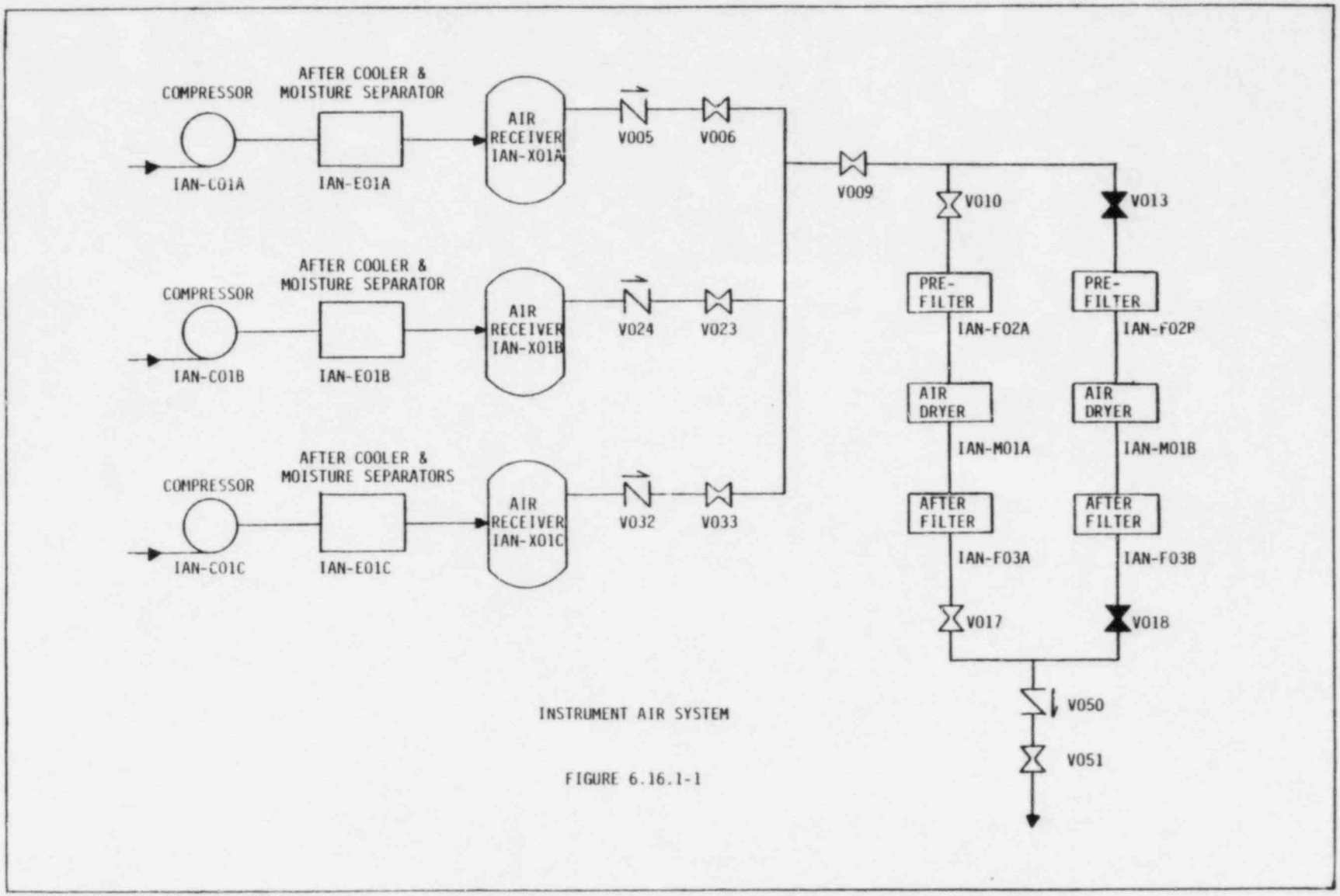
6.16 INSTRUMENT AIR SYSTEM

This analysis includes construction and evaluation of a fault tree logic diagram for Loss of Instrument Air. The results are used as input to the system level fault trees.

6.16.1 System Description

Figure 6.16.1-1 presents a schematic of the PVNGS Instrument Air System. The Instrument air system has three parallel trains, each consisting of an intake air filter, a compressor, an 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 two parallel drying/filter lines. Each line has a prefilter, an instrument air dryer and an afterfilter. Downstream of the afterfilter, the two lines join into a header from which all instrument air requirements are supplied.

The compressors are reciprocating type with water cooled cylinders. Each compressor is capable of delivering 100% of the instrument air requirement or 50% total (i.e., instrument air and service air) requirements. The two drying/filter trains are each of 100% capacity. Each dryer has dual towers loaded with activated alumina, a desiccant. An automatic control system reverses the chambers operation every five minutes to provide continuous drying of the air. 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 and the backup nitrogen system. The instrument air system is not essential for safe shutdown of the plant.



INSTRUMENT AIR SYSTEM

FIGURE 6.16.1-1

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 the air supplied from one compressor train.

2. System boundaries are defined to be from the air intake filters to the instrument air header.

3. Compressing Unit C01A is in service during normal operation. Compressing Units C01B and C01C are in standby.

4. Following a turbine trip, the Instrument Air System Components are transferred to the offsite power source.

5. Operator action to establish a compressed air supply is not included. The Instrument Air dryer M01A is in service. The air dryer M01B is isolated and requires an operator action (open valves V013 and V018) to bring it into service. Since operator actions to establish air supply are not included, air dryer M01B is not modelled. Similarly, nitrogen back-up is also not modelled as it requires an operator action to open valve V052.

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 the three cases. 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 PVNGS INSTRUMENT AIR

Case Number	Description	Failure Probability (Median Value)	Failure Rate (Median Value)
One	Loss of Instrument Air before Turbine Trip	N/A	2.23E-5/hr
	Error Factor		4
Two	Loss of Instrument Air following reactor trip	1.1E-2	1.64E-5/hr
	Error Factor	4	2
Three	Loss of Instrument Air Given offsite power is available	8.1E-3	1.64E-5/hr
	Error Factor	5	2

TABLE 6.16.3-2

DOMINANT CUTSETS FOR PVNGS INSTRUMENT AIR

Case Number	Cutset	Description	% of Total Failure* Probability
One	1. IARC2062	IA Dryer Fails	56%
	2. IFAT2061	Pre/After filters of the dryer fails	19%
	3. ECRP2791	Voltage regulator for 120VDP E-NHN-D11 fails	10%
	4. EXLP2758	480VLC E-NGN-L25 transformer fails	7%
Two	1. IARC2062	IA Dryer fails	33%
	2. ECBV2810	Battery E-NKN-F17 for 125VDC Bus not available	16%
	3. EBGP2682	Grid collapse on turbine trip	16%
	4. EBFA2697	UAT Fast Transfer breaker fails to open	16%
	5. EBFB2699	13.8KV Bus E-NAN-S01 Fast Transfer Breaker fails to close	16%
Three	1. IARC2062	IA Dryer fails	39%
	2. ECBV2810	Battery E-NKN-F17 for 125VDC Bus not available	20%
	3. EBFA2692	UAT Fast Transfer breaker fails to open	20%
	4. EBFB2699	13.8KV Bus E-NAN-S01 Fast Transfer Breaker fails to close.	20%

*Percentage of failure rate for Case 1 and unavailability for Cases 2 and 3.

6.17 RESTORATION OF FEED FLOW ANALYSIS

The restoration of feed flow analysis for PVNGS includes an analysis of the human error probability of the operator manually restoring the Seismic Category I auxiliary feedwater pumps and an unavailability analysis on the non-essential motor-driven auxiliary feedwater pump. (The non-essential AFW pump is manually actuated and aligned from the control room.) The restoration analysis assumes a loss of MFW flow and the failure of the Seismic Category I motor and turbine-driven AFW pumps to automatically deliver flow to at least one steam generator. Operator actions to manually establish flow from the Seismic Category I AFW pumps are analyzed in Section 6.17.1-6.17.3. Operation of the non-essential AFW pump is addressed in Sections 6.17.4 and 6.17.5. The results of the combined restoration of feed flow actions are presented in Section 6.17.6.

6.17.1 Restoration 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 system descriptions, 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 were also considered in the analysis. Recovery, 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 each activity 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. For the purposes of this study, total loss of feedwater flow was the initiating event and restarting any one of the two AFW pumps and associated valve train constituted successful recovery of feed flow. SGTR was not considered. The review of the AFW system design, and previous interviews with operators were used 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 action 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 an operator.

The HEP event tree was generated for the most general case, failure of the AFW actuation signal (AFAS). In this case, both AFW trains are available. For more specific cases, such as having one pump out of service for maintenance or testing 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 AFAS. For other failure modes, specific parts of the total event tree were used. Success was obtained if the operator started any one of the two auxiliary feedwater trains.

6.17.2 Restoration 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 two 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 engineering safeguards panel NP-10 or feedwater panel NP-5 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 locations on the panels and are used constantly during normal operation (NP-5). If the operator misreads these 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 or by noting alarms. He could later recover by noticing primary coolant pressure and temperature are increasing. Approximately 25 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 (60 minutes after reactor trip) to recognize that there is no feedwater flow before core damage conditions cannot be prevented (28, Section 2.8).

The operators are assumed to be at a normal stress level for the initial SG status readings and at a moderately high stress level for subsequent actions. One operator is assigned to the primary side and the second operator is assigned to the secondary side and operates the AFW 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 Gattmann). Contributions by the shift supervisor, the shift technical advisor, and the nuclear auxiliary operator (NAO) are neglected although they would also be present. Dependencies of specific actions on the execution of the previous action are also considered in the analysis. The probability of the operators not recognizing total loss of feedwater in the allotted time is less than 10^{-4}.

Operator action includes three basic activities in restoring the AFW. He first attempts to start AFW by manually activating the AFAS (assuming no signal was generated). If he fails at this activity, he will manually start the pumps and open the AFW valves. Only one recovery activity at each step is considered.

For manual override of the AFAS, the operator has two push buttons he can activate on NP-6. He can omit this step or make a commission error (wrong push buttons). Complete dependency between the two switches is assumed, i.e., if he fails to activate the first switch, he will fail to activate the other switch. If he fails to start the pumps, he may correct himself by noticing the pump status indicators.

If the operator fails to initiate AFW by activating the AFAS (or the AFAS 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 pump was assumed. The operator starts both pumps as a single activity. The HEPs for failure to start one pump and for failure to start both is therefore identical. If he fails to start one of the pumps, only one chance to recover was considered. He can notice there is no pump discharge pressure (with high dependencies on starting the pump). 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 control and isolation valves. For the loss of feedwater cases, he can open anyone of the valve trains to each of the two steam generators. The two pumps feed each of the two steam generators through two motor-operated valves in series. All valve controls on each train are located together on the panel with status lights. Because of the grouping of the valves, omission errors dominate and commission errors were neglected. A single recovery factor was considered and manually activating the valves from the Auxiliary Building was neglected.

When combining major activities, a mild dependency was assumed between tasks. For example, for an AFAS failure, the operator can either activate the AFAS override or manually start the pumps. If he failed to activate the AFAS override, (HEP = 0.008) then the HEP for manual activating the pumps was 0.15. The independent failure probability for starting the pumps was 0.003.

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) for the Western Systems Coordination Council (WSCC) region. Failure probabilities for restoration of offsite AC are 0.23 (60 min.) and 0.30 (25 min.). The failure probability of restoration of the diesel generator was taken from Reference (42) and is 0.77 (60 min.) and 0.92 (25 min., linear interpolation). The combined failure to restore any AC power is 0.2 (60 min.) and 0.27 (25 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 Restoration 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 most probable failure modes, restoration failure probabilities were calculated and are given in Table 6.17.3-2. Results for both the sixty minute period and twenty-five minute period are given. Case 1 represents the best estimate case where the operator has 60 minutes to restore feedwater before fuel damage is unavoidable. Case two represents the case where the operator has 25 minutes to restore feedwater before he must commit to use of feed and bleed operation (28, Section 2.8).

The results are based on a three operator model with high dependency between the three operators. However, other people (shift supervisor, shift technical advisor and NAO) could assist the operators. This would reduce the HEPs since the additional personnel could identify errors. Also additional instrumentation and manual operation from the auxiliary building was neglected. These effects have not been considered in this study and therefore the results are very conservative.

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).

TABLE 6.17.2-1

INITIAL OPERATOR ACTIONS FOR TOTAL LOSS OF FEEDWATER

1) Reactor scrams. Lights and alarms alert operator.

2) Operator scans reactivity control panel to see if rods entered and if power is decreasing.

3) Operator verifies turbine trip.

4) Operator scans power panel to see if transfer from auxiliary to startup transformer has occurred.

5) Operator verifies unit output breakers are open and turbine speed is decreasing.

6) Operator scans ESF panel for power and actuation

7) Operator verifies SG pressure is at 1000 psia.

8) Operator scans feedwater panel for 5% runback (MFW flow)

TABLE 6.17.3-1

HEP FOR COMBINED TASKS*

Actuate AFAS Train	1.0E-3
Manually Turn On Pump	3.0E-3
Change Valve Position from Control Room	4.0E-3
2nd Operator Backup 1st Operator	.5
3rd Operator Backup (50 Minute Only)	.5

* Single Operator at Moderately High Stress with One Recovery Activity

TABLE 6.17.3-2

HEPs FOR RESTORATION OF AUXILIARY FEEDWATER
FOR SPECIFIC EVENTS

Failure Mode	(60 Min.)	(25 Min.)
TDP Fails Start, MDP in Maintenance	8.0E-4	1.5E-3
AFAS Failure	2.5E-4	5.0E-4
TDP in Maintenance, MDP Suction Line Closed	1.0	1.0
MDP in Maintenance, TDP Suction Line Closed	1.0	1.0
TDP in Maintenance, MDP Discharge Line Closed	8.0E-2	1.0
MDP in Maintenance, TDP Discharge Line Closed	8.0E-2	1.0
TDP in Maintenance, MDP Recirc. Bypass Open	8.0E-2	1.0
MDP in Maintenance, TDP Steam Line Closed	1.0E-3	2.0E-3
MDP in Maintenance, TDP Recirc. Bypass Open	8.0E-2	1.0
TDP Fails to Start, MDP in Test	4.0E-4	8.0E-4
TDP Fails to Start, Grid Collapse, DG02 Fails to Start	4.0E-4	8.0E-4
TDP in Test, MDP Suction Line Closed	2.0E-2	4.0E-2
MDP in Test, TDP Suction Line Closed	2.0E-2	4.0E-2
TDP in Test, MDP Discharge Line Closed	1.0E-2	2.0E-2
MDP in Test, TDP Discharge Line Closed	1.0E-2	2.0E-2
TDP in Test, MDP Recirc. Bypass Open	1.0E-2	2.0E-2
MDP in Test, TDP Steam Line Closed	5.0E-4	1.0E-3
MDP in Test, TDP Recirc. Bypass Open	1.0E-2	2.0E-2

TABLE 6.17.3-2
(Continued)
HEPs FOR RESTORATION OF AUXILIARY FEEDWATER
FOR SPECIFIC EVENTS

Failure Mode	(60 Min.)	(25 Min.)
TDP in Maint., Grid Collapse, DG02 Fails to Start	2.0E-1	2.7E-1
TDP Fails to Start, Grid Collapse, DG02 Fails to Operate	4.0E-4	8.0E-4
TDP Discharge Line Closed, Grid Collapse, DG02 Fails to Start	1.0E-2	2.0E-2
TDP Steam Line Closed, Grid Collapse, DG02 Fails to Start	5.0E-4	1.0E-3
TDP Recirc. Bypass Open, Grid Collapse, DG02 Fails to Start	4.0E-2	2.7E-1
TDP Suction Line Closed, Grid Collapse, DG02 Fails to Start	2.0E-1	2.7E-1
TDP Maintenance, MDP Fails to Start	8.0E-4	1.5E-3

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

6.17.4 Non-Essential AFW Pump Operation

A schematic of the non-essential, non-seismic Category I AFW pump is presented in Figure 6.17.4-1. The non-essential pump (AFN-P01) is normally used for startup, hot standby and normal shutdown plant operation. The motor-driven pump can be manually started and its associated valves manually aligned from the control room. The pump takes suction through a separate line from the condensate storage tank. The pump supply lines join the main feedwater supply upstream of the main feedwater control and isolation valves. The pump and associated valves receive power from offsite and onsite power sources.

The support system dependency diagram for the non-essential AFW pump is provided in Figure 6.11.1-2 of Section 6.11, Auxiliary Feedwater System.

6.17.5 Non-Essential AFW Pump Analysis Assumptions

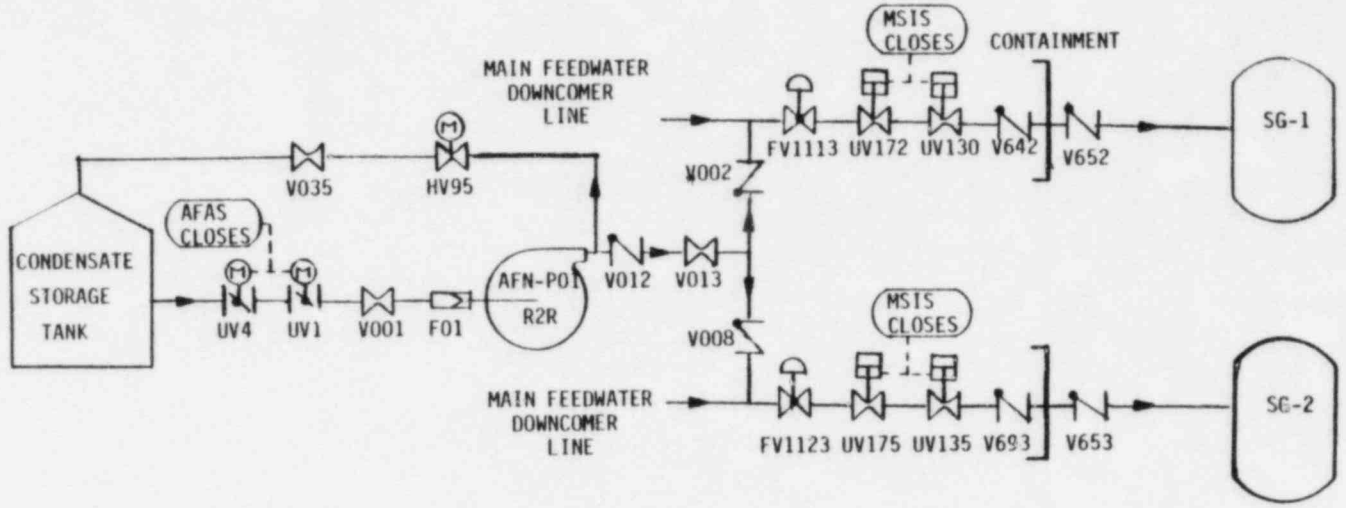
The following assumptions were made in performing the fault tree analysis for the Loss of Secondary Heat Sink Analysis:

1. For the Loss of Secondary Heat Sink analysis, Failure of the non-essential AFW pump is defined as failing to deliver non-essential AFW pump flow to at least one SG.

2. The motor-operated isolation valves from condensate storage tank have closed on AFAS.

6.17.6 Results

A fault tree logic diagram was used to evaluate the probability of failing to deliver non-essential AFW pump flow to at least one SG. A human error probability task analysis was used to evaluate the probability of failing to restore automatic AFW pump flow to at least one SG. Both analysis were



NON-ESSENTIAL AUXILIARY FEEDWATER PUMP

FIGURE 6.17.4-1

performed assuming a 60 and 25 minute time period for operation actions for the current plant design and the plant design assuming feed and bleed operation respectively.

The HEPs developed fo the various failure modes of Table 6.17.3-2 were combined to determine the total failure probability for restoration of the Seismic Category I AFW pumps. 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. The failure modes specifically analyzed comprise approximately 85.7% 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 restoration of secondary feedwater flow analyses was used to determine the following probabilities:

- Probability of failure to deliver non-essential AFW pump flow to at least one SG.

- Probability of failure to deliver non-essential AFW pump flow to at least one SG given a loss of MFW and AFW.

- Probability of failure to restore AFW flow, failure to restore Seismic Category I AFW pumps and failure to deliver non-essential AFW flow.

- Probability of failure to restore AFW flow, failure to restore Seismic Category I AFW pumps and failure to deliver non-essential AFW pump flow given a loss of MFW and AFW.

The quantitative results of the analyses are presented as Cases One through Four respectively for the 60 and 25 minute time periods in Table 6.17.6-1. The confidence distributions of the failure probabilities are

presented in terms of the median values and associated error factors. The error factor is defines as the ratio of the 95 to 50 percentile. For cases two and four, the dependencies that exist between the MFW, AFW and the non-essential AFW pump have been incorporated into the non-essential AFW pump failure probability.

Table 6.17.6-2 contains a list of the qualitative results for Cases 1 and 2 in terms of the dominant cutsets for those cases. Included in the table is a brief description of each cutset as well as the percent contribution of the total failure probability. The percentage is based on a point estimate ratio. The qualitative results of the restoration analysis of the Seismic Category I AFW pumps is presented in Table 6.17.3-2 in terms of the restoration actions considered.

TABLE 6.17.6-1

FAILURE PROBABILITIES FOR PVNGS RESTORATION ANALYSIS

Case Number	Description	Failure Probability Median Value (60 Min)	(25 Min)	Error Factor (60 Min)	(25 Min)
One	Failure to deliver non-essential AFW pump to at least 1 SG - System Unavailability	8.6E-3	1.1E-2	3.5	3.0
Two	Failure to deliver non-essential AFW pump to at least 1 SG given loss of MFW and AFW - System Unavailability	1.5E-2	1.7E-2	3.0	2.8
Three	Failure to restore AFW flow, failure to manually restore Seismic Category I AFW pumps and failure to deliver non-essential AFW pump flow to at least 1 SG	4.0E-3	8.4E-3	3.5	3.4
Four	Failure to restore AFW flow, failure to manually restore Seismic Category I AFW pumps and failure to deliver non-essential AFW pump to at least 1 SG given loss of MFW and AFW	6.9E-3	1.3E-2	3.1	2.9

TABLE 6.17.6-2

DOMINANT CUTSETS FOR PVNGS NON-ESSENTIAL AFW PUMP

Case Number	Cutset	Description	% of Total Failure Probability (60 Min)	(25 Min)
One	1. AVMO2448	Operator Fails to Open Pump Suction Valves	16.8%	26.9%
	2. APMO2447	Operator Fails to Start Pump	16.8%	20.2%
	3. AVMA2452	Pump Suction Valve UV1 Fails to Open	16.8%	13.4%
	4. AVMA2451	Pump Suction Valve UV4 Fails to Open	16.8%	13.4%
Two	1. EBGP2680 EDDJ2816	Spurious Grid Collapse and DG G01 Fails to Start	17.4%	14.6%
	2. EBGP2680 EDDK2818	Spurious Grid Collapse and DG G01 Fails to Operate	14.6%	11.7%
	3. AVMO2448	Operator Fails to Open Pump Suction Valves	11.1%	18.6%
	4. AVMO2447	Operator Fails to Start Pump	8.9%	13.9%

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 capability. 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 was filtered using a cutoff frequency of 10^{-8} 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 the Seismic Category I AFW pumps or operation of the non-essential AFW pump with the condensate system

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	7.27E-06	11
		Total Core Damage Frequency	7.3E-06	11

being employed after restoration actions have failed. The analysis assumed a 60 minute time period following reactor trip on low steam generator level for operator action (28, Section 2.8). (Introduction of feed flow after the 60 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 7.3E-6 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 PVNGS AFWS system unavailability. In addition, the major contributors to system unavailability are restorable by operator action within the 60 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 panel and is supplied with 480 VAC power from a different MCC. Each unit has 2 backup diesel generators available in the event of loss of offsite power.

- Operator Action. The operator has approximately 60 minutes following reactor trip to restore the AFW system or establish flow from the non-essential AFW pump to 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 for the manual and automatic design feed and bleed system are presented in Table 7.1.2-1.[1] Two minimal core damage scenarios were identified for each design. The scenarios were filtered using a cutoff frequency of 10^{-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 for the manual and automatic designs are identical and are discussed below:

Scenario 1. LF-$G_1U_2^Y$ 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, has failed. The analysis assumed that the operator initiated feed and bleed operation at 25 minutes into the transient for both the manual and automatic designs (28,Section 2.8). For the 25 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 operation is not considered. Due to the

[1] For the manual design, plant operates with block valves closed and for the automatic design, plant operates with block valves open. For both designs, feed and bleed is manually initiated.

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
(a) Manual Feed and Bleed Design[1]			
1. LF-G_1U_2Y	• Initiating Event • Fail to Deliver AFW Flow • Failure to Restore Feed Flow • Failure of Feed Bleed Operation	9.87E-06	12
2. LF-G_1U_2R	• Initiating Event • Fail to Deliver AFW Flow • Failure to Restore Feed Flow • Failure to Achieve HP Recirc.	1.60E-09	57
	Total Core Damage Frequency	1.0E-05	12
(b) Automatic Feed and Bleed Design[1]			
1. LF-G_1U_2Y	• Initiating Event • Fail to Deliver AFW Flow • Failure to Restore Feed Flow • Failure of Feed Bleed Operation	4.93E-06	13
2. LF-G_1U_2R	• Initiating Event • Fail to Deliver AFW Flow • Failure to Restore Feed Flow • Failure to Achieve HP Recirc.	1.60E-09	57
	Total Core Damage Frequency	5.0E-06	13

1 For the manual design, plant operates with block valves closed and for the automatic design, plant operates with block valves open. For both designs, feed and bleed is manually initiated.

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 25 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. $LF\text{-}G_1U_2R$ This sequence is defined by Loss of Main Feedwater, Failure to Deliver AFW Flow, Failure to Restore Feed Flow, and Failure to Achieve HP 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.

Only one 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 scenarios are presented in Table 7.2.1-1. Eight minimal core damage scenarios were identified. The total frequency of scenarios eliminated by the cutoff frequency of 10^{-8} per year is approximately 2.9E-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 eight 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	6.08E-7	13
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	2.76E-8	12
3. T1-ONL	• Initiating Event • Fail to Throttle HPSI • Fail to Initiate Auxiliary Spray Flow • ADV on Affected SG Fails to Reclose	3.06E-8	13
4. 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	8
5. T1-DM_1	• Initiating Event • TBV Fails to Reclose • 1 MSSV on Affected SG Fails to Reclose	1.97E-6	7
6. T1-DE_1	• Initiating Event • TBV Fails to Reclose • MSIV on Affected SG Fails to Close	3.66E-7	7
7. T1-C_1M_1	• Initiating Event • TBVs Fail to Quick Open • 1 MSSV on Affected SG Fails to Reclose	2.11E-6	10
8. T1-A	• Initating Event • Fail to Deliver Sufficient HPSI Flow	5.14E-7	15
	Total Core Damage Frequency:	1.1E-5	5

Scenario 1. $T1\text{-}OQ_1L$ 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 ADVs on the affected SG are opened by the operator (to prevent a MSSV from opening) and begin to discharge primary inventory. When one of the two ADVs 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. $T1\text{-}OQ_1KM_1$ 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 ADVs 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-ONL 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 and failing to initiate auxiliary spray flow which results in a large integrated leak flow through the tube rupture. Although the SGBS is available, the SG is assumed to fill with subcooled water. The ADVs on the affected SG are opened by the operator (to prevent a MSSV from opening) and begin to discharge primary inventory. When one of the two ADVs 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 4. T1-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 5. $T1\text{-}DM_1$ 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 6. $T1\text{-}DE_1$ 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. One of the two MSIVs 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 7. $T1\text{-}C_1M_1$ In this scenario, the TBVs fail to quick open following turbine trip. The resulting pressure spike opens 6 MSSVs on each SG. (The steam flow through 12 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 8. 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 1.4E-9 per year. The results are presented in 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-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 6 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

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	6.23E-7	15
2. T2-L	• Initiating Event • ADV on Affected SG Fails to Close	3.23E-8	24
3. T2-KM_1	• Initiating Event • ADV on Affected SG Unavailable • MSSV on Affected SG Fails to Reclose	1.39E-9	25
4. T2-OKM_1	• Initiating Event • Fail to Throttle HPSI • ADV on Affected SG Unavailable • MSSV on Affected SG Fails to Reclose	3.74E-10	33
5. T2-A	• Initiating Event • Fail to Deliver Sufficient HPSI Flow	2.26E-8	23
6. T2-A'	• Initiating Event • Fail to Maintain HPSI Flow	9.52E-9	54
	Total Core Damage Frequency	8.0E-7	14

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, one 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. $T2\text{-}KM_1$ — Following a tube rupture in one SG with coincident LOOP, the operator is required to open the ADVs to initiate cooldown. In this scenario, both ADVs on the affected SG fail to open (e.g., the operator fails to open the ADVs from the control room) 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. $T2\text{-}OKM_1$ — 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 one of the two ADVs on the affected SG 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. Fourteen minimal core damage scenarios were identified. The total frequency of scenarios eliminated by the cutoff frequency of 10^{-8} per year is approximately 5.8E-7 per year. The results are presented in terms

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	6.69E-8	11
2. T3-DE_1	• Initiating Event • TBV Fails to Reclose • MSIV on Most Affected SG Fails to Close	6.93E-8	11
3. T3-C_1M_1	• Initiating Event • TBVs Fail to Quick Open • MSSV on Most Affected SG Fails to Reclose	3.65E-7	15
4. T3-C_1I_1	• Initiating Event • TBVs Fail to Quick Open • MSSV on Least Affected SG Fails to Reclose	3.98E-7	17
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	1.93E-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	1.97E-7	12
7. T3-DM_1	• Initiating Event • TBV Fails to Reclose • MSSV on Most Affected SG Fails to Reclose	3.90E-7	10
8. T3-DI_1	• Initiating Event • TBV Fails to Reclose • MSSV on Least Affected SG Fails to Reclose	4.23E-7	9

TABLE 7.2.3-1
(Continued)
SGTR IN TWO SG CORE DAMAGE SEQUENCES

Path	Description	Frequency (Median Value per Year)	Error Factor
9. T3-$0Q_4$L	• Initiating Event • Fail to Throttle HPSI • Fail to Initiate Blowdown • ADV on Most Affected SG Fails to Reclose	8.83E-8	19
10. T3-$0Q_4$H	• Initiating Event • Fail to Throttle HPSI • Fail to Initiate Blowdown • ADV on Least Affected SG Fails to Reclose	8.36E-8	18
11. T3-$0Q_2$L	• Initiating Event • Fail to Throttle HPSI • No Blowdown from Most Affected SG • ADV on Most Affected SG Fails to Reclose	2.61E-8	16
12. T3-$0Q_3$H	• Initiating Event • Fail to Throttle HPSI • No Blowdown from Least Affected SG • ADV on Least Affected SG Fails to Reclose	2.90E-8	16
13. T3-F_2H	• Initiating Event • Loss of TBV Flow After Iso. of Affected SG • ADV on Least Affected SG Fails to Reclose	1.37E-7	13
14. T3-A	• Initiating Event • Fail to Deliver Sufficient HPSI Flow	1.12E-7	15
	Total Core Damage Frequency	4.2E-6	8

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 fourteen 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. $T3\text{-}DE_2$ 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. One 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 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-F_1M_1 This scenario is similar to T1-F_1M_1 except that the MSSV on the "affected" SG becomes the MSSV on the "most affected" SG.

Scenario 6. T3-F_1I_1 This scenario is similar to T3-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-DM_1 This scenario is similar to T1-DM_1 except that the MSSV on the "affected" SG becomes the MSSV on the "most affected" SG.

Scenario 8. T3-DI_1 This scenario is similar to T3-DM_1 except that the MSSV on the least affected SG fails to reclose.

Scenario 9. T3-OQ_4L This scenario is similar to T1-OQ_1L except that blowdown flow is not initiated from either SG and the ADV on the "affected" SG becomes the ADV on the "most affected" SG.

Scenario 10. T3-OQ_4H This scenario is similar to T3-OQ_4L except that one ADV on the least affected SG fails to reclose following SG overfill.

Scenario 11. T3-OQ_2L This scenario is similar to T1-OQ_1L except that the ADV on the "affected" SG becomes the ADV on the "most affected" SG.

Scenario 12. T3-OQ_3H This scenario is similar to T1-OQ_1L except that blowdown flow is not initiated from the least affected SG and one ADV on the least affected SG fails to reclose following SG overfill.

Scenario 13. T3-F_2H Following tube ruptures in both SGs, the most affected SG is isolated and RCS cooldown is initiated using the TBS in conjunction with the least affected SG. In this scenario, turbine bypass flow is lost after isolation of the most affected SG. The operator is assumed to continue cooling using the ADVs on the least affected SG. One of the two ADVs fails to close (outside containment LOCA) and a pressure differential is assumed to develop between the RCS and the least affected 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 14. 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. Eight minimal core damage scenarios were identified. The total frequency of scenarios eliminated by the cutoff frequency of 10^{-10} per year is approximately 1.4E-9 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 eight 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.

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	1.12E-7	18
2. T4-I_2	• Initiating Event • MSSV on Least Affected SG Fails to Close Following TT	1.13E-7	17
3. T4-L	• Initiating Event • ADV on Most Affected SG Fails to Close	7.00E-9	21
4. T4-H	• Initiating Event • ADV on Least Affected SG Fails to Close	5.99E-9	26
5. T4-KM_1	• Initiating Event • ADV on Most Affected SG Unavailable • MSSV on Most Affected SG Fails to Close	3.14E-10	24
6. T4-JI_1	• Initiating Event • ADV on Least Affected SG Unavailable • MSSV on Least Affected SG Fails to Close	3.13E-10	21
7. T4-A	• Initiating Event • Fail to Deliver Sufficient HPSI Flow	3.77E-9	28
8. T4-A'	• Initiating Event • Fail to Maintain HPSI Flow	1.71E-9	50
	Total Core Damage Frequency	3.1E-7	13

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.
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-A	This scenario is similar to T2-A. Only the initiating events differ.
Scenario 8.	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 including those that fell below the cut-off frequency for each event tree and the one scenario that appeared above the cut-off frequency (T1-ONL). 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

TABLE 7.2.5-1

MINIMAL CORE DAMAGE SEQUENCES INCLUDING AUXILIARY SPRAY SYSTEM FAILURE

Sequence	Core Damage Frequency (Per Year)
T1-ONL	3.1E-8
T1-ONKM$_1$	1.5E-9
T1-NQ$_1$L	9.0E-9
T1-NQ$_1$KM$_1$	4.2E-10
T2-NL	3.6E-10
T2-NKM$_1$	1.7E-11
T3-ONL	6.1E-9
T3-ONKM$_1$	2.9E-10
T3-ONH	6.1E-9
T3-ONJI$_1$	2.9E-10
T3-NQ$_2$L	4.2E-10
T3-NQ$_2$KM$_1$	2.0E-11
T3-NQ$_3$H	4.2E-10
T3-NQ$_3$JI$_1$	2.0E-11
T3-NQ$_4$L	1.2E-9
T3-NQ$_4$KM$_1$	5.9E-11
T3-NQ$_4$H	1.2E-9
T3-NQ$_4$JI$_1$	5.9E-11
T4-NL	7.1E-11
T4-NKM$_1$	3.3E-12
T4-NH	7.1E-11
T4-NJI$_1$	3.3E-12

TABLE 7.2.5-2[1]

CHANGE IN CORE DAMAGE FREQUENCY (λCD) DUE TO ADDED DEPRESSURIZATION CAPABILITY OF PORVs

Event Tree Description	λCD (per yr.) Aux. Spray Accident Scenarios	λCD (per yr.) with PORVs	$\Delta\lambda$CD (per yr.)	λCD (per yr.) From All Other Scenarios
SGTR in One SG	4.2E-8	4.6E-11	4.2E-8	1.1E-5
SGTR in One SG with Coincident LOOP	3.8E-10	1.3E-12	3.8E-10	8.0E-7
SGTR in Two SG	1.6E-8	1.8E-11	1.6E-8	4.2E-6
SGTR in Two SG with Coincident LOOP	1.5E-10	5.3E-13	1.5E-10	3.1E-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 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.

- 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	2.6E-6	16
T1-ON	9.5E-6	9
T1-OQ_1	1.8E-4	6
T1-NQ_1	2.7E-6	8
T2-P_1	2.6E-9	48
T2-O	2.9E-6	13
T2-N	1.1E-7	16
T3-P_1	5.4E-7	24
T3-P_3	5.7E-7	25
T3-ON	1.9E-6	9
T3-OQ_2	8.0E-6	9
T3-OQ_3	8.1E-6	8
T3-OQ_4	2.4E-5	8
T3-NQ_2	1.2E-7	12
T3-NQ_3	1.3E-7	10
T3-NQ_4	3.6E-7	13
T4-P_1	4.9E-10	49
T4-P_2	5.3E-10	41
T4-Q	4.6E-7	18
T4-N	2.1E-8	15

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	2.0E-4	5
SGTR in One SG with Coincident LOOP	2.8E-6	16
SGTR in Two SG	4.8E-5	8
SGTR in Two SG with Coincident LOOP	5.3E-7	16

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 following loss 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 the

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	1.22E-9	70
2. P1-A	• Initiating Event • Failure to Deliver Sufficient HPSI Flow	1.06E-9	29
Total Core Damage Frequency:		3.7E-9	46

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 followingloss 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. Two scenarios were eliminated by the cutoff frequency of 1.0E-15 per year. The total frequency of scenarios eliminated by the cutoff frequency is 9.9E-16 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	8.98E-9	51
2. P2-Z_1G_2	• Initiating Event • Failure to Deliver 5% MFW to One Steam Generator • Failure to Deliver AFW to One Steam Generator	5.43E-9	20
3. P2-A	• Initiating Event • Failure to Deliver Sufficient HPSI Flow	7.85E-9	17
	Total Core Damage Frequency	3.9E-8	15

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 or Transient Induced PORV LOCA Core Damage Scenarios

Three minimal core damage scenarios for Spurious or Transient Induced 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 for both PORV designs that were considered. 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 core damage scenarios are described as follows:

Scenario 1. P3-R or P4-R

This scenario refers to a Spurious or Transient Induced 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 or P4-Z_2G_1

This scenario refers to a Spurious or Transient Induced 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 cause the RCS temperature and

TABLE 7.3.3-1

SPURIOUS OR TRANSIENT INDUCED PORV LOCA CORE DAMAGE SEQUENCES

Path	Description	Frequency (Median Value per Year)	Error Factor
(a) Manual PORV Design			
1. P3-R	• Initiating Event • Failure to Achieve High Pressure Recirculation	2.14E-9	78
2. P3-Z_2G_1	• Initiating Event • Failure to Deliver 5% MFW • Failure to Deliver AFW	9.17E-10	49
3. P3-A	• Initiating Event • Failure to Deliver Sufficient HPSI Flow	2.03E-9	30
	Total Core Damage Frequency	9.7E-9	21
(b) Automatic PORV Design			
1. P4-R	• Initiating Event • Failure to Achieve High Pressure Recirculation	3.91E-7	51
2. P4-Z_2G_1	• Initiating Event • Failure to Deliver 5% MFW • Failure to Deliver AFW	6.57E-7	24
3. P4-A	• Initiating Event • Failure to Deliver Sufficient HPSI Flow	1.14E-6	20
	Total Core Damage Frequency	3.1E-6	21

pressure to increase thus inhibiting makeup. Eventually, the core will become uncovered and subsequently core damage will occur.

Scenario 3.	P3-A or P4-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

SUMMARY OF DOMINANT SEQUENCES (No Feed and Bleed)[1]

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 PVNGS.

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 8 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

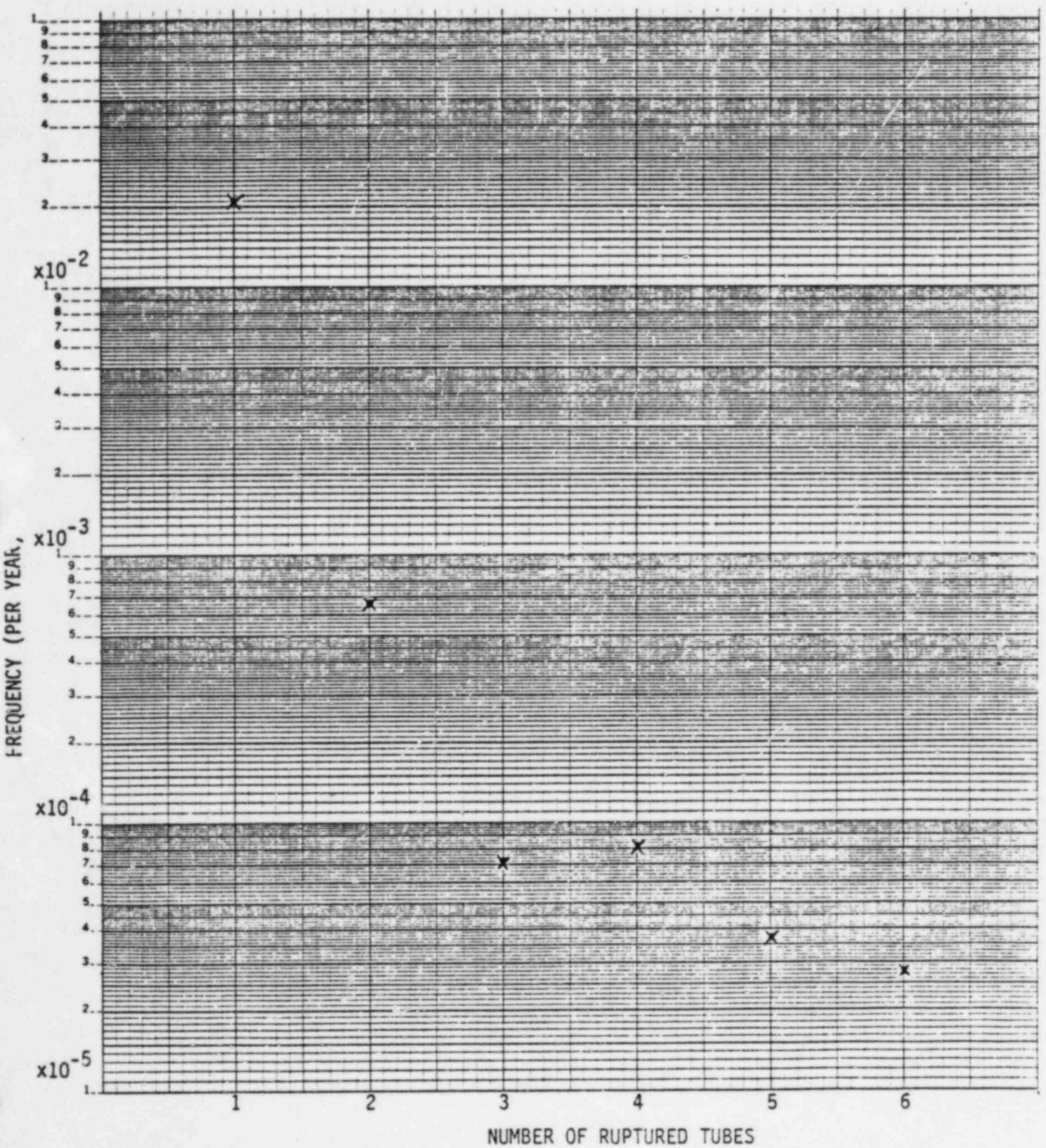
EVENTS CONSIDERED IN TUBE STRENGTH MODEL

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
CEA 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 8.2-1

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	7.3E-6	1.7E-5	1.5E-6	N/A
Error Factor	11	5	10	
Case Two: Median λ_{CD} (per year) with manually actuated PORVs, without ASHR* capability	1.0E-5	1.7E-5	1.5E-6	8.4E-8
Error Factor	12	5	10	11
Case Three: Median λ_{CD} (per year) with automatically actuated PORVs, without ASHR* capability	5.0E-6	1.7E-5	1.5E-6	3.9E-6
Error Factor	13	5	10	17
Case Four: Median λ_{CD} (per year) with no PORVs or ASHR* capability	1.1E-5	1.7E-5	1.5E-6	N/A
Error Factor	13	5	10	

*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 Tank (RWT) is 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 APS 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 5.0E-6 per year (median value) with an associated error factor of 16.

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

$$(LF\text{-}G_1U_1V) - [(LF\text{-}G_1U_2Y) + (LF\text{-}G_1U_2R) + (P1\text{-}R) + (P1\text{-}A) + (P2\text{-}R) + (P2\text{-}Z_1G_2) + (P2\text{-}A) + (P3\text{-}R) + (P3\text{-}Z_2G_1) + (P3\text{-}A)]$$

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 5% upper and 5% lower limits. The negative median value indicates a net increase in core damage frequency due to PORVs of 1.2E-6 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 2.6E-6 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 (λCD per year)	Automatically Actuated PORVs (λCD per year)
Median	-1.2E-6	-2.6E-6
5% Upper Limit[2]	2.7E-5	4.4E-5
5% Lower Limit[3]	-6.7E-5	-1.0E-4

[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 5% Upper Limit, with 95% probability.

[3] Based on data uncertainty the increase in core damage risk due to PORVs is less than the 5% Lower Limit, with 95% probability.

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. Palo Verde Nuclear Generating Station (PVNGS) Units 1, 2 and 3 Final Safety Analysis Report.

8. Palo Verde Nuclear Generating Station Units 1, 2 and 3 System Descriptions (various systems).

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. Palo Verde Nuclear Generating Station Units 1, 2 and 3 Operating Instructions (various systems).

12. Palo Verde Nuclear Generating Station Units 1, 2 and 3 Single-Line Diagrams (various electrical buses).

13. Palo Verde Nuclear Generating Station Units 1, 2 and 3 Main Control Board Layout Drawings and Equipment 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. Combustion Engineering Standard System Analysis Report.

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.

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:

$$F(X;N,\sigma,\mu) = 1 - \left[\text{EXP} -\left(\frac{X-\mu}{\sigma}\right)^N\right]$$

$$\text{for } X > \mu$$

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:

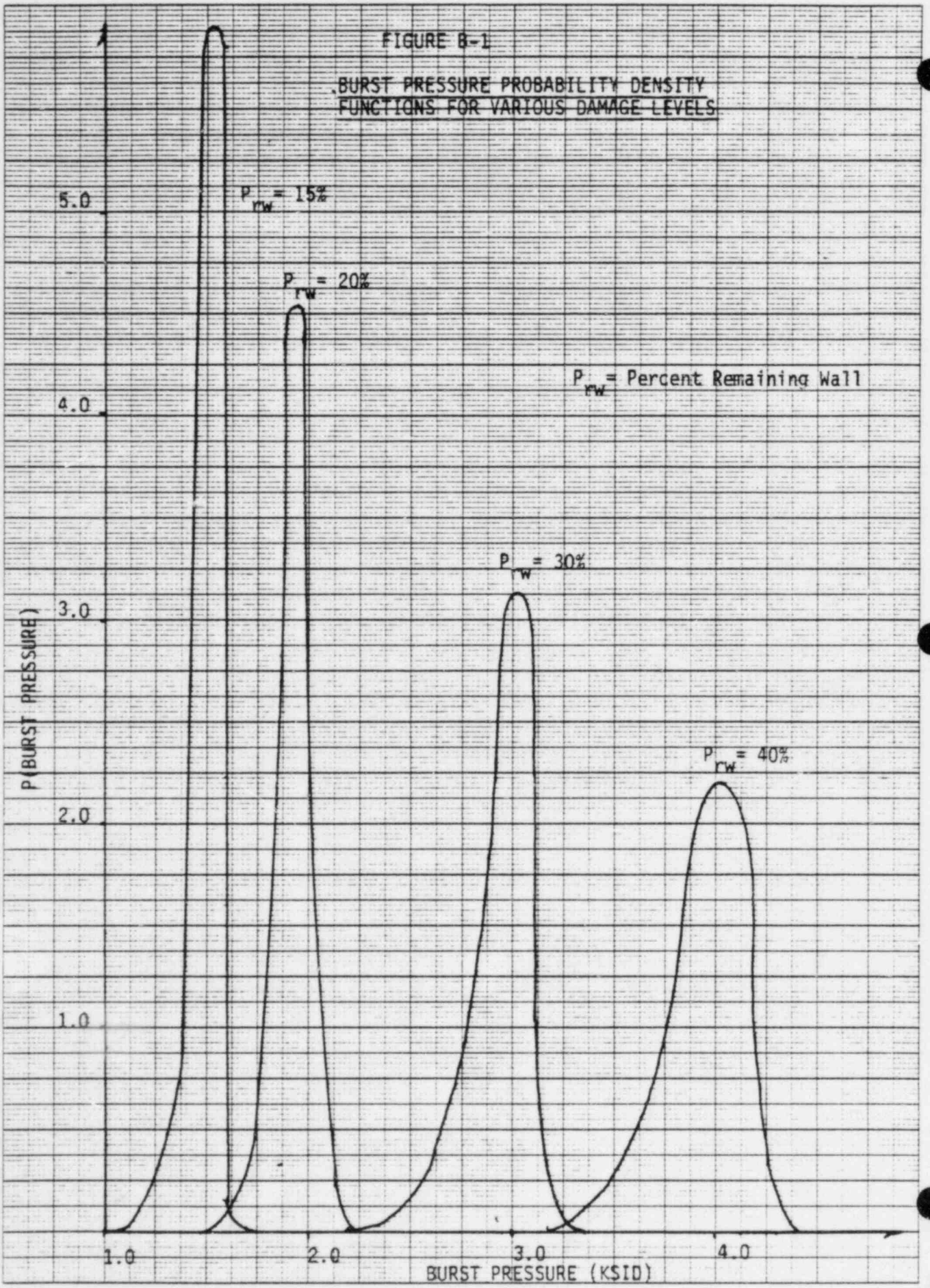
$$BP_d = BP_u \times P_{RW}/100$$

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

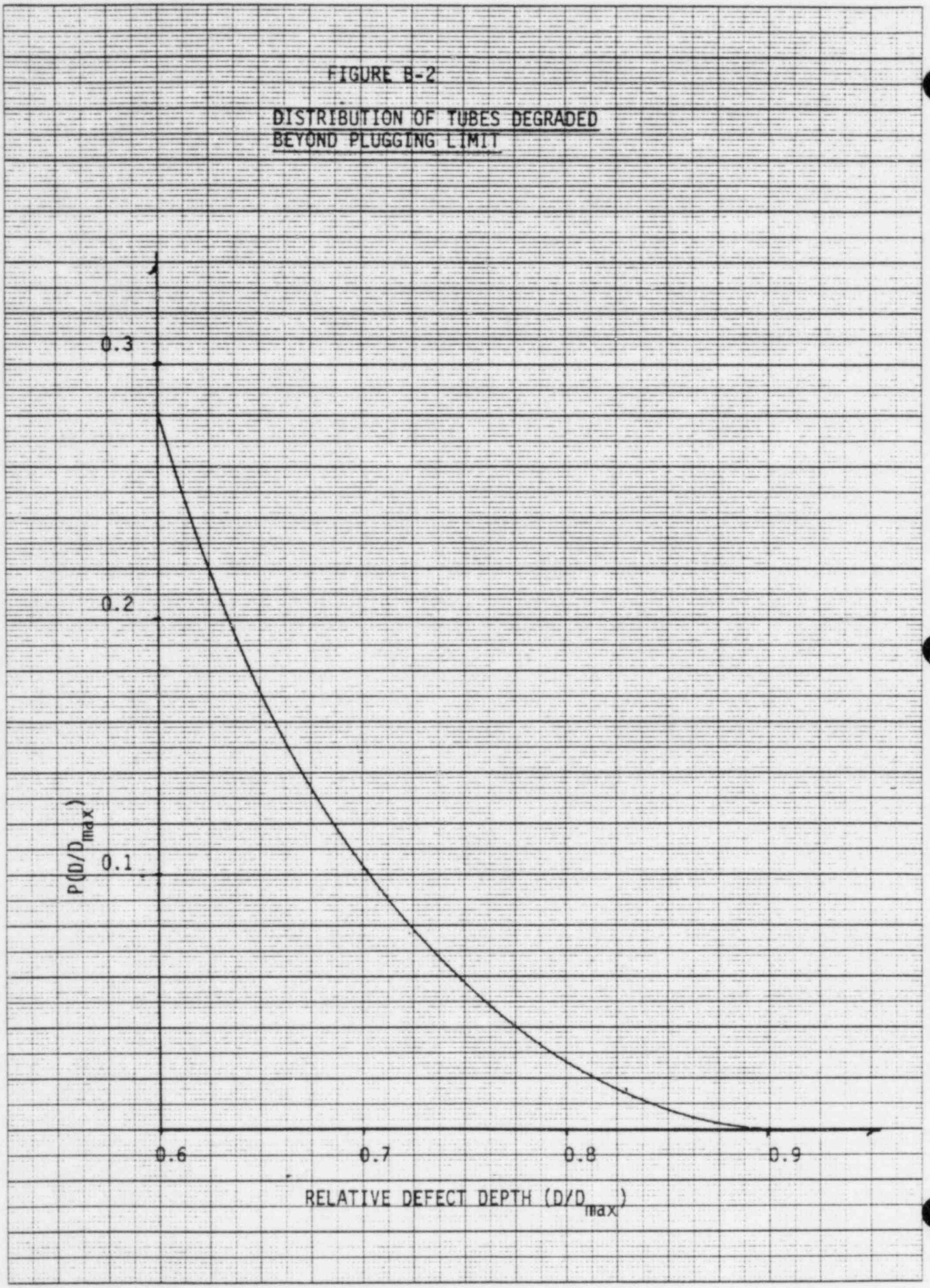
A second important element in the probabilistic tube strength model is the defect inventory, that is, the distribution of damage level among the more than 11000 tubes in a steam generator. Preliminary computations showed that only tubes degraded more than the assumed plugging limit of 60% contributed 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.

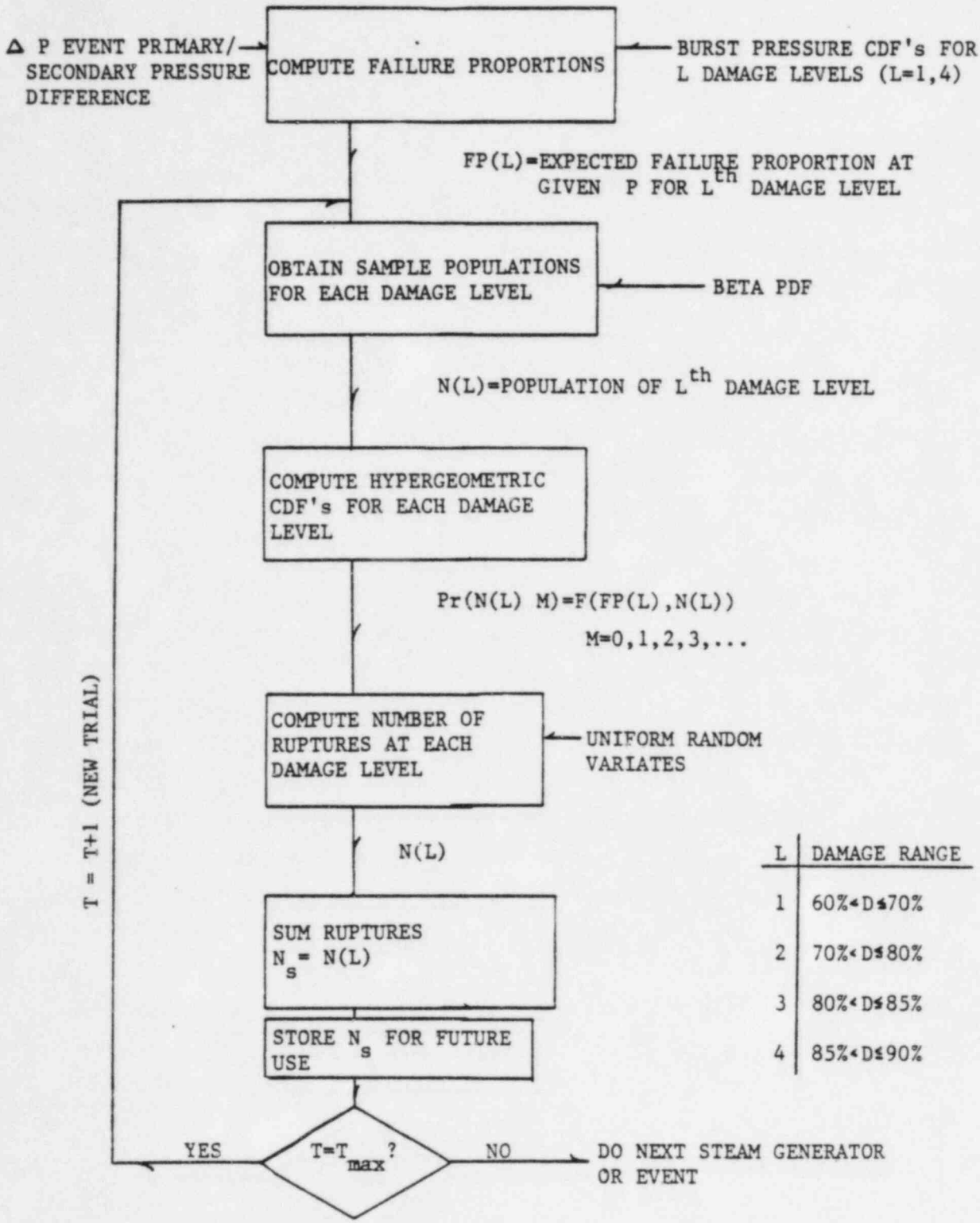
The second step in the computation is to obtain sample values for the number of tubes in each of four damage intervals. This is accomplished by randomly sampling from the distribution shown in Figure B-2. The expected failure proportions computed in the first step are then combined with their respective 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



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.