Third
Interim Report

Systems Interaction Methodology Applications Program

Prepared for

Office of Standards Development
U. S. Nuclear Regulatory Commission

by

Gary J. Boyd
Wallis R. Cramond
Jack W. Hickman
Alan M. Kolaczkowski
Nuclear Fuel Cycle Safety Research Department
Sandia Laboratories, Albuquerque, NM 87185

Acknowledgements for Work
Supporting the Program

Sidney H. McAhren, University of New Mexico
Desmond W. Stack, Sandia Laboratories, 1758
Kimberly A. Francis, Sandia Laboratories, 1758
Robert B. Klaiber, Evaluation Associates, Inc.
Daniel J. Murphy, Jr., Sandia Laboratories, 4412
David D. Carlson, Sandia Laboratories, 4412

August 31, 1979

Table of Contents

CHAPTER 1

INTRODUCTION

The Systems Interaction Methodology Applications Program is being performed for the Office of Standards Development of the U. S. Nuclear Regulatory Commission. The program is intended to be a contributing element to the resolution of the problem being addressed by Task Action Plan A-17 entitled, "Systems Interaction in Nuclear Power Plants". The lead responsibility for this task action plan is the Division of Project Management, Office of Nuclear Reactor Regulation. The objectives of the Systems Interaction Methodology Applications Program are to develop an independent methodology for identifying and evaluating systems interactions in light water reactor commercial power plants and to assess the Standard Review Plan to determine its comp' ness regarding systems interactions.

This is the third interim report and documents work completed since the last report submitted in March 1979. Work during this period has included: plant logic model (fault tree) development, further development of the systems interaction analysis techniques and application of these techn ques to the logic models, and assessment of the Standard Review Plan for one of the three function logic models.

In review, there are three functions being modeled: achieving or maintaining reactor subcriticality (RS), decay heat removal (DHR), and protection of the reactor coolant

system pressure boundary (RCPB). These functions are being developed for all plant modes except refueling and for the Condition I and II (ANSI N18.2) occurrences which require shutdown or remaining shutdown. This will be discussed further in Chapter 2.

Although the logic models and analysis techniques are applicable to a much broader scope of situations than are being addressed by this program, the extent of what is being covered is limited to allow greater emphasis on development of the methodology. A summary of the scope is given in Table 1-1.

The status of the basic tasks necessary to complete Phase I of the program, as of August 31, 1979, is given in Table 1-2. Tasks 1 through 4 have been previously completed and are not shown. Tasks 5 and 6 have been merged so that the status is best reported relative to the specific models. Similarly Tasks 7, 8, and 9 are closely related tasks which are essentially complete. Task 11 is to assess the Standard Review Plan. Task 12, the Phase I report, will not be started until most of the preceding tasks are complete, thus it is not shown. This report describes all tasks for the reactor coolant pressure boundary (RCPB) function. Chapter 2 covers tasks 5 and 6; Chapter 3, Tasks 7-9; Chapter 4, Task 11; and Chapter 5, Task 10.

Table 1-1. Program Scope.

	Within Scope[1]	Methodology Applicable[2]
Plant Types	Westinghouse Pressurized Water Reactors (PWR)	Other PWR Boiling Water Reactors (BWR
Number of Units Per Site	Single	Multiple
Radioactive Material Source	Reactor Core	Spent Fuel Pool Radwaste System
Plant Functions	Reactor Coolant Pressure Boundary Reactor Subcriticality Decay Heat Remov[illegible]	Other Safety Related Functions Requiring High Performance Reliability
Plant Conditions (ANSI N18.2)	Normal Operations Incidents of Moderate Frequency	Infrequent Incidents Limiting Faults
Environmental Conditions (ANSI N18.2)	Normal	Fire, Earthquake, Hurricane, Tornado, Flood, Sabotage
Interactions	Physical Connections Motive Power Control Power Actuation Cooling Lubrication Hydraulic Spatial Connections (Location) Fluid Thermal Mechanical	Human Errors Design and Construction Procedures Operation Test and Maintenance Physical Connections Water Hammer Spatial Connections Barrier Penetration Drainage Radiation Characteristic Common Manufacturer and Technology Aging and Wear

[1]Within scope indicates those things included in the logic modeling, therefore, being treated explicitly in the study.

[2]Methodology applicable indicates those things which are not included in the logic models, but which could be treated by the analytical techniques if it was desired to expand the logic models at some later date.

Table 1-2. Task Status (X = Completed).

	Tasks 5-6 Fault Tree Models		Task 10 Systems Interaction Analysis		Task 11 Assess Standard Review Plan
	Structure	Computer Plot	Generic	Specific	
RCPB	X	X	X	X	X
DHR	X	X	X		
RS					

CHAPTER 2

FAULT TREE DEVELOPMENT

The fault trees (logic models) form the basis for the system interaction analysis. The three basic function fault trees describing conditions potentially leading to unacceptable core damage which are to be developed for various plant operating modes and initiating occurrences are: failure to achieve or maintain reactor subcriticality, failure to remove decay heat, and failure of the reactor coolant system pressure boundary.

The purpose of the fault trees is to model the combinations of components which if failed would result in loss of any of the above three functions and by assumption result in the potential for unacceptable core damage. These fault trees thus are vehicles for the search and evaluation of system interactions which could influence significantly nuclear power plant safety.

Each fault tree is developed from the function at the top of the tree to specific components at the bottom of the tree that are directly applicable to the success of that function. Only those parts of systems which affect the undesired top event are included. Not all systems are identified explicitly or modeled in their entirety.

The fault tree models identify and delineate the necessary and sufficient functions to respond to an initiating occurrence. The required systems depend on the initiating occurrence and the plant mode at the time of the occurrence. There are five

plant modes and four occurrence categories (from ANSI N18.2) resulting in twenty potentially different sets of circumstances for which the plant safety systems are called upon to prevent unacceptable core damage. These are:

Plant Mode			Occurrence Category	
Power Operation	PO		Loss of Offsite Power	LOP
Startup	SU		Loss of PCS Condenser	PCS
Hot Standby	SB	X	Normal Shutdown	NOR
Hot Shutdown	HS		All Other Occurrences	ACC
Cold Shutdown	CS			

In each case the three basic functions are connected logically as shown in Figure 2-1. Each of the three basic functions are modelled separately and apply to all of the twenty circumstances through the use of notes on the fault tree plots designating specific applicability of branches or events not applicable in all circumstances.

Although the fault trees developed represent the exemplary plant (Watts Bar), generic names were used to reflect that these fault trees can be used as a general guideline for other PWR plants.

There are numerous acronyms used in this chapter in order that the information can be presented concisely, especially on the figures. Thus a glossary is given in Table 2-1.

Simplified logic diagrams for two of the three functions are given in Figures 2-2 and 2-3. The reactor coolant pressure boundary (RCPB) fault tree has already been sent to the NRC.

The decay heat removal fault tree is being sent under separate cover. Figures 2-2 and 2-3 show major branches of those fault trees which in some cases are designated as separate figure (i.e., fault tree plot) numbers. The purpose of dividing the fault trees into more than one plot is due to the size of the plot and convenience in handling. At the top of Figure 2-3 is an exclusive OR gate showing that there are two separate fault trees, one for all plant modes from power operation through hot shutdown (POHS) and one for cold shutdown (CS). The third function, reactor subcriticality (RS) is currently in development.

The definition of plant modes and the RCS pressure/temperature limitations is shown in Figure 2-4. A point of interest is the relationship of cold shutdown and hot shutdown with the residual heat removal system (RHRS) capability. It is assumed that cold shutdown is defined as reactor coolant system temperatures less than 200°F; however, the RHRS can be operated at temperatures up to 350°F and this is sometimes refered to as cold shutdown. Inherent in the fault trees is the concept that RHRS applies only to cold shutdown, and if decay heat removal (DHR) fails while in cold shutdown, the plant can be brought back to hot shutdown if necessary so that other DHR systems are functional. Cold shutdown for the reactor coolant pressure boundary (RCPB) function relates to lower pressure limitations and a lower set point for the pressurizer relief valves, i.e., 1200 psig rather than 2335 psig.

RCPB Fault Tree

The RCPB fault tree is discussed in this report since it is the basis of the analyses presented in Chapters 4 and 5. Event trees are used to explain the fault tree contents. To start with, a functional event tree is given in Figure 2-5. This is not a typical event tree on the left side since it depicts the circumstances leading to the necessity for the RS, DHR, and RCPB functions. On the right side is the functional relationship of these three functions and RCPB mitigation. The right side of the event tree at this level of detail is repeated for all of the other circumstances below.

For this report only the RCPB function will be developed. Failure of the RCPB can occur by component failure under normal RCS pressures and as a result of overpressure. The normal RCS pressure case is straightforward; therefore, only the overpressure event tree is developed in detail. The circumstances affecting the RCPB function have been combined on Figure 2-6 along with some of the events necessary to arrive at overpressure. This is not a traditional event tree since its branches represent choices in the circumstances rather than success or failure of functions or events. The causes are those events, such as an inadvertent pump startup with and without the availability of alternate water sources, which may result in overpressure. The designators ET1 etc. at the right of Figure 2-6 are used only to reference the remainder of the event tree shown in Figures 2-7 and 2-8. After each line is an S for success, i.e., no overpressure, or the overpressure case found in the fault tree.

The event tree method does not show that letdown as an event must be matched to the particular initiating event. This is done in the fault tree. Also under CS cases 1, 3, and 5 neither water solid or alternate source availability were considered to have a significant affect on the outcome. It is further recognized that several cases could be separated allowing for a finer discrimination of the level of overpressure.

The final report will include a set of system and subsystem diagrams. While not as detailed as the plant diagram, they will show the components included in the fault trees. Figure 2-9 is a simplified diagram presented here to demonstrate the multiple use of systems providing input to and letdown from the RCS. Although most of the components are not shown it is worthwhile to note the combinations of sources, pump trains, and paths to the RCS and the normal paths for letdown and relief of the RCS. These systems and subsystems will appear also in the DHR and RS fault trees.

Table 2-1. Glossary of Acronyms and Abbreviations

RS	Reactor Subcriticality Function
DHR	Decay Heat Removal Function
RCPB	Reactor Coolant Pressure Boundary Function
PO	Power Operation Plant Mode
SU	Startup Plant Mode
SB	Hot Standby Plant Mode
HS	Hot Shutdown Plant Mode
CS	Cold Shutdown Plant Mode
POHS	All Plant Modes from Power Operation Through Hot Shutdown
LOP	Loss of Offsite Power
PCS	Loss of the Power Conversion System Condenser
NCR	Occurrences Requiring Normal Plant Shutdown
AOC	All Occurrences Other than LOP, PCS, or NCR
SB	Condition where the Pressurizer has a Steam Bubble
WS	Condition where the Pressurizer is Water Solid
RCS	Reactor Coolant System
ET	Event Tree Transfer Symbol
PRT	Pressurizer Relief Tank
HT	Holdup Tank
VCT	Volume Control Tank
PWST	Primary Water Storage Tank
BAT	Boric Acid Tank
RWST	Refueling Water Storage Tank
PORV	Pressurizer Power Operated Relief Valves
CSV	Pressurizer Code Safety Valves

Table 2-1 (Continued)

P	Pressurizer
UHI ACC	Upper Heat Injection Accumulation
HL	Hot Leg
CL	Cold Leg
RV	Reactor Vessel
SG	Steam Generator
RHR1	Residual Heat Removal Pump Number 1
SI1	Safety Injection Pump Number 1
BIT	Boron Injection Tank
ALT CHG	Alternate Charging
NOR CHG	Normal Charging
FCV	Flow Control Valve
CC1	Centrifugal Charging Pump Number 1
UCD	Unacceptable Core Damage
PDP	Positive Displacement Pump
CCP	Centrifugal Charging Pumps
H	Pressurizer Heaters
SIP	Safety Injection Pumps
UHIS	Upper Head Injection System
RCP	Reactor Coolant Pump
RV-C	Relief Valves Fail Closed
SRV-C	Safety and Relief Valves Fail Closed
LET	Letdown
NS	Normal Spray
AS	Auxiliary Spray
ASV	Auxiliary Spray Output Valves Only
ALT SOURCE	Alternate Source of Water Inadvertently Available

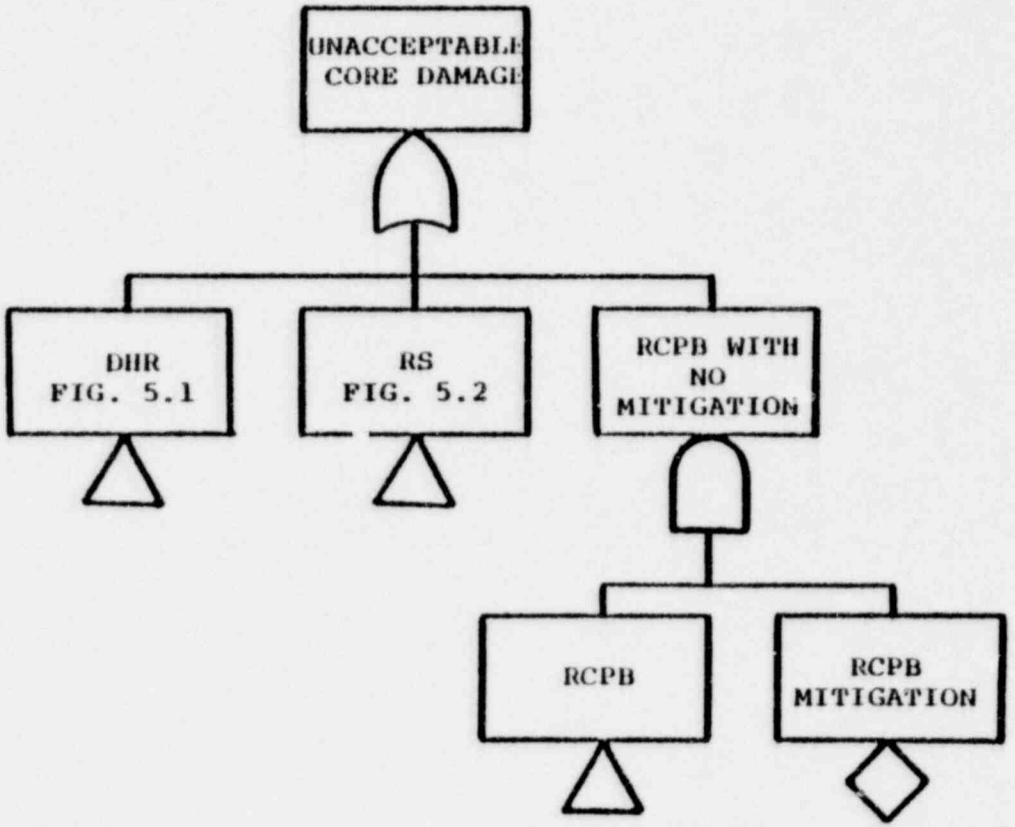

FIGURE 2-1. UNACCEPTABLE CORE DAMAGE FAULT TREE

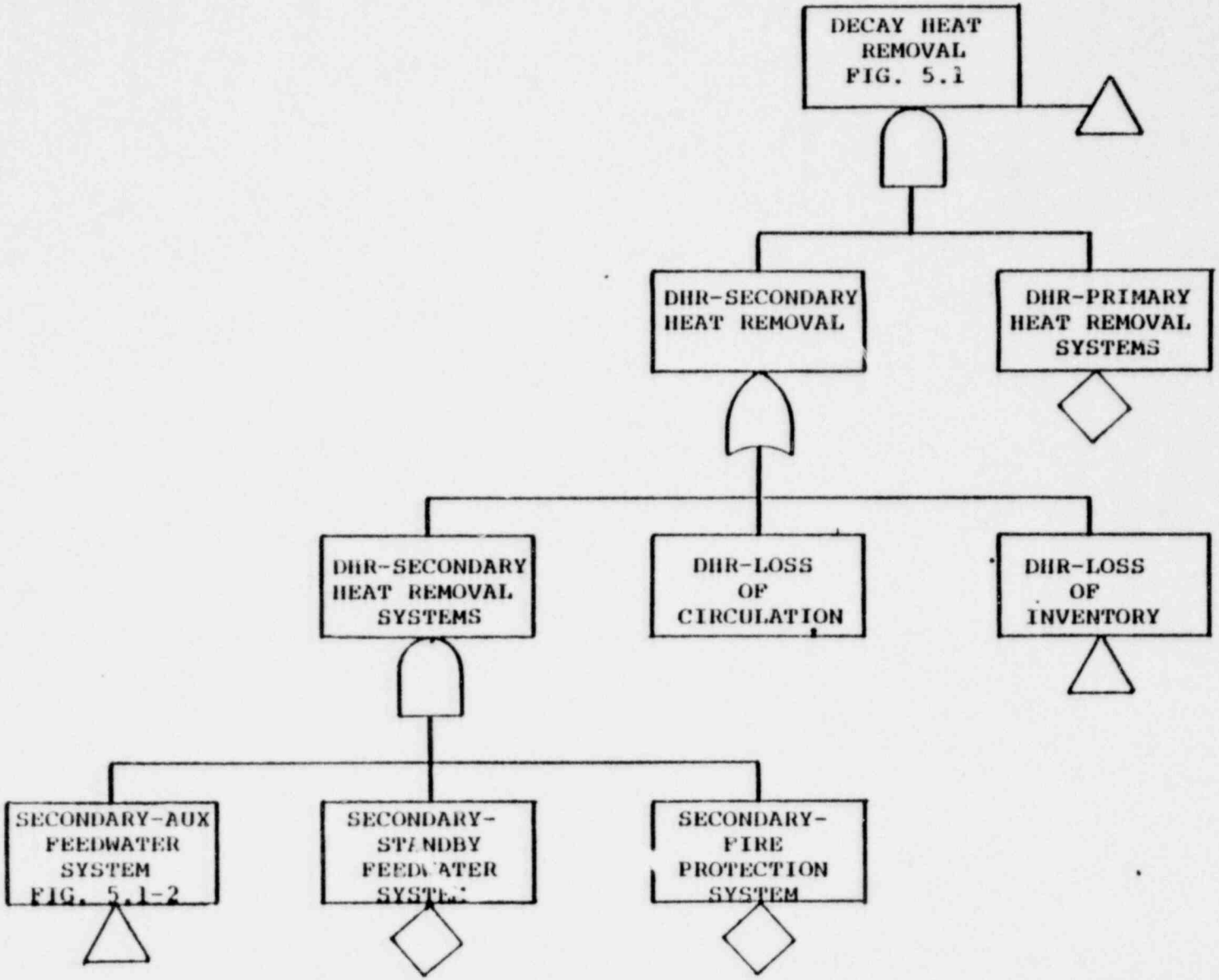

FIGURE 2-2. DECAY HEAT REMOVAL FAULT TREE

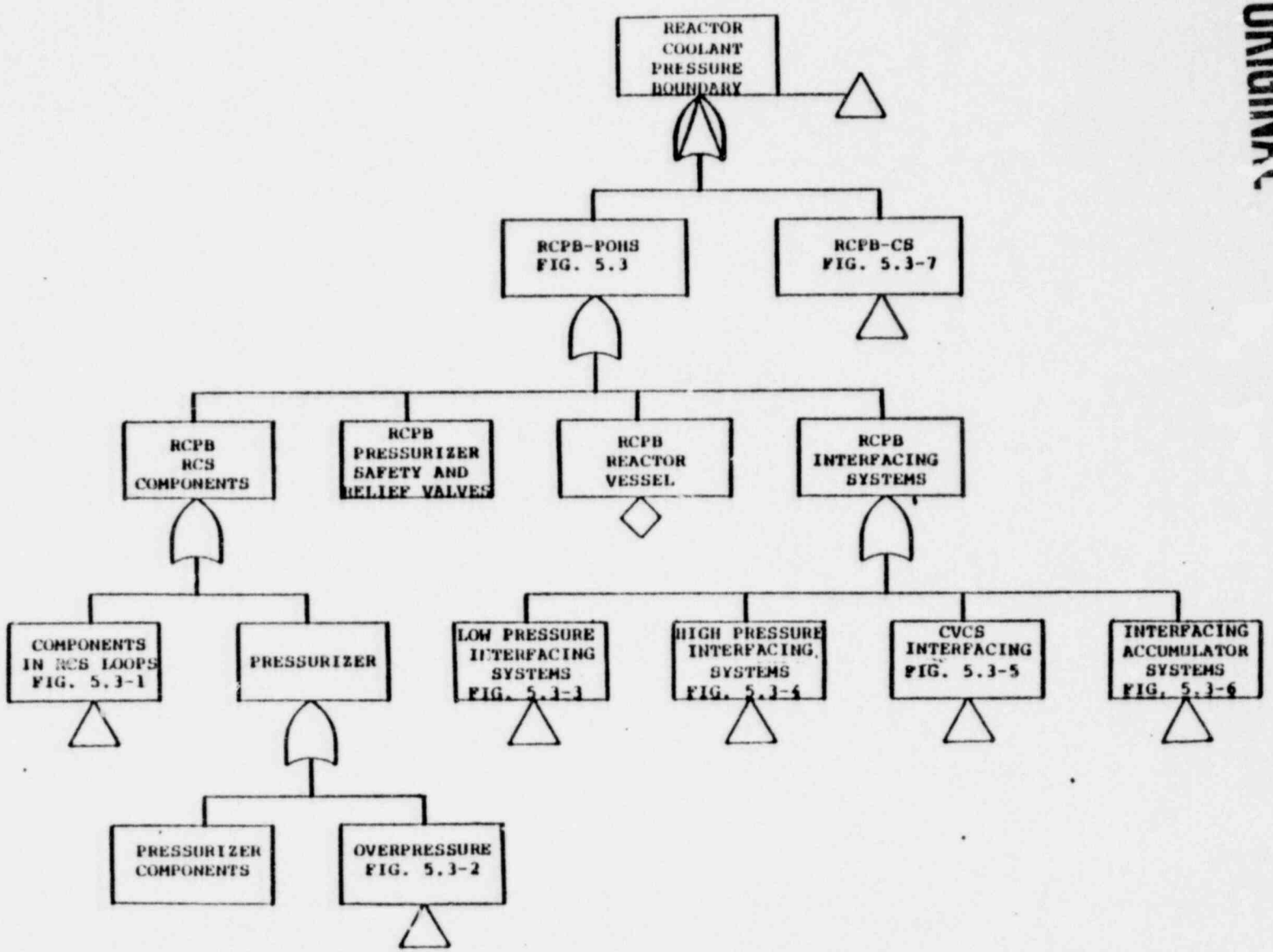

FIGURE 2-3. REACTOR COOLANT PRESSURE BOUNDARY FAULT TREE

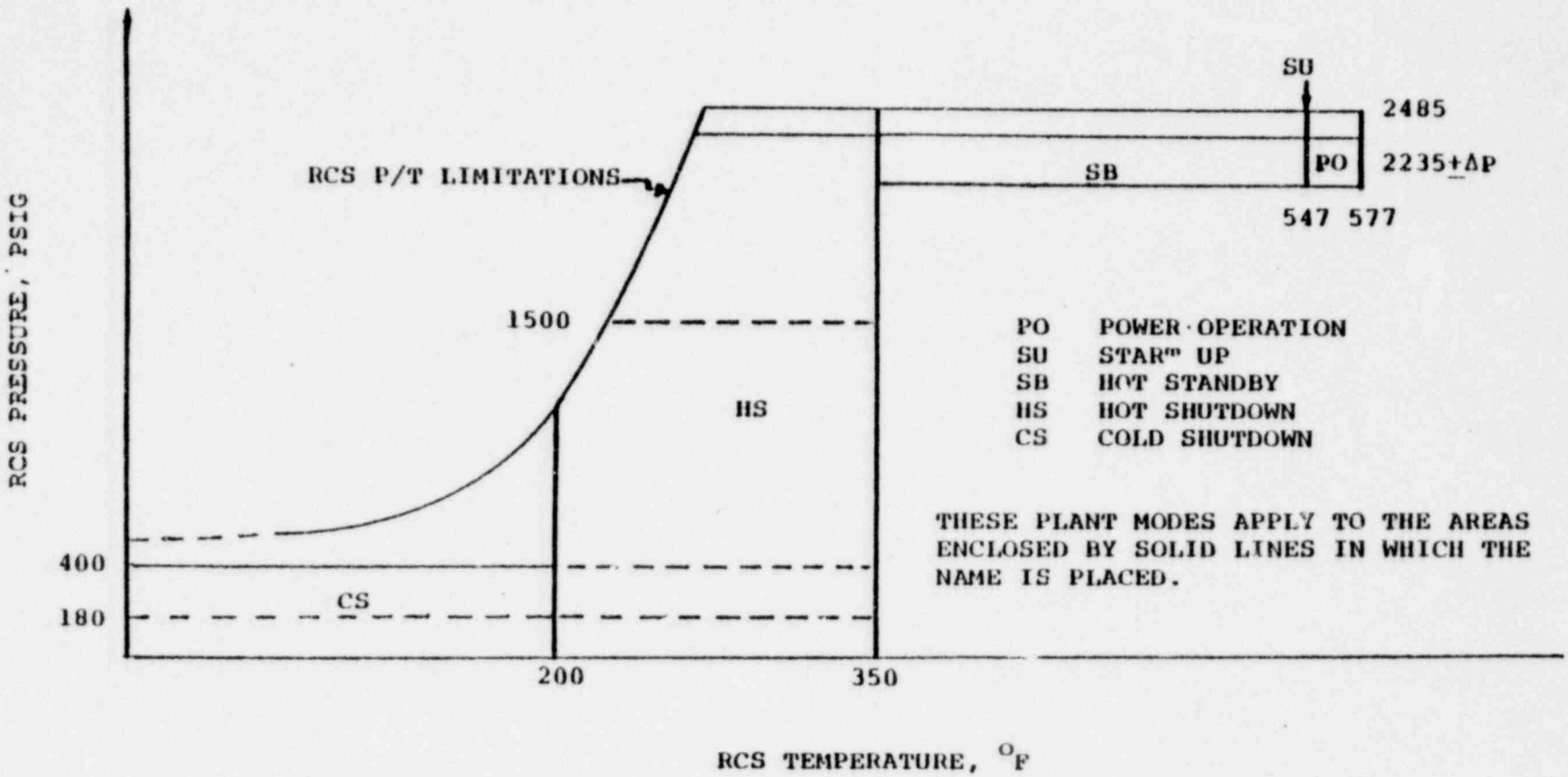

FIGURE 4. RCS PRESSURE TEMPERATURE REGIONS FOR REACTOR OPERATING MODES

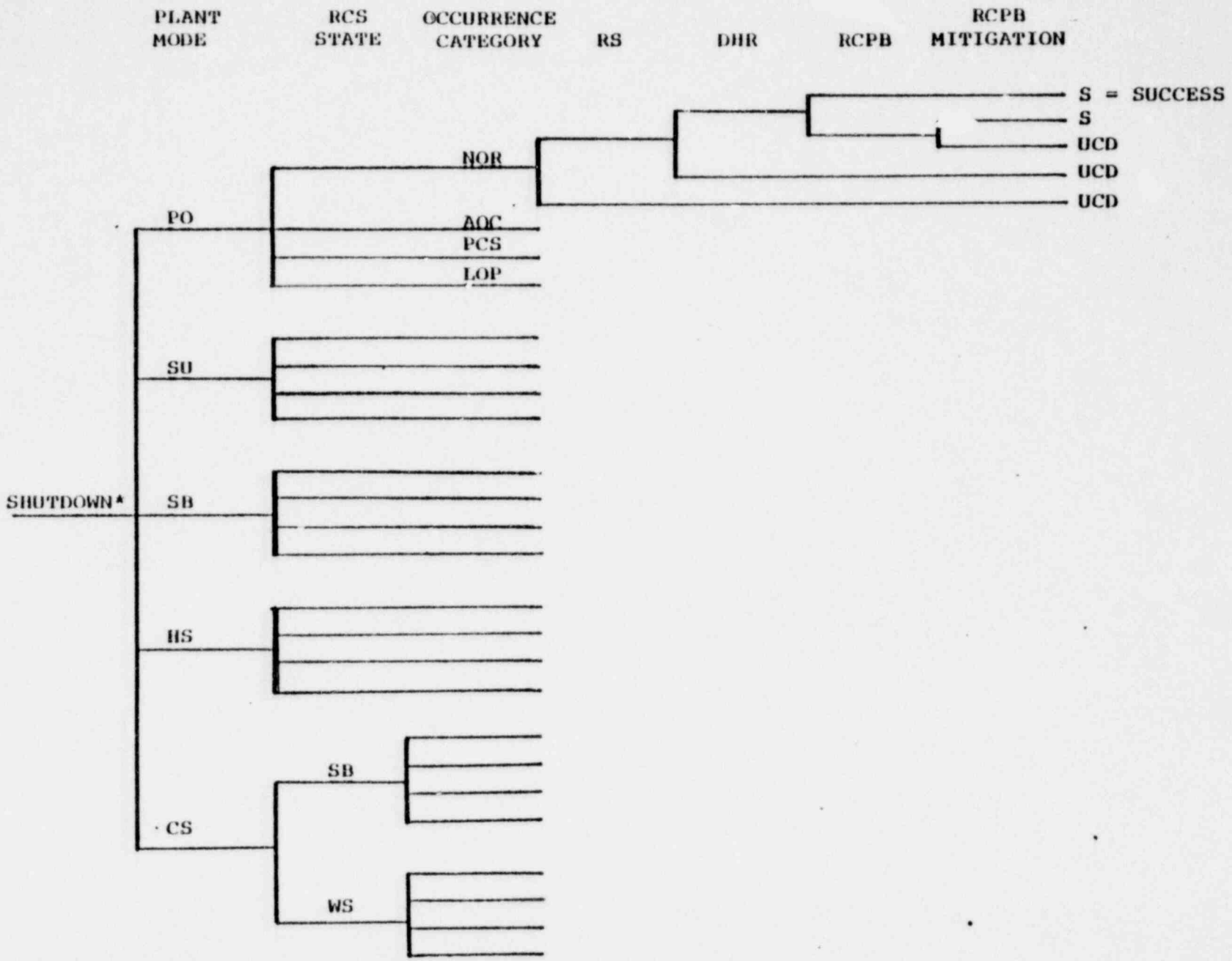

FIGURE 2-5. FUNCTIONAL EVENT TREE

*Cause the reactor to be shutdown or maintain the shutdown state as applicable.

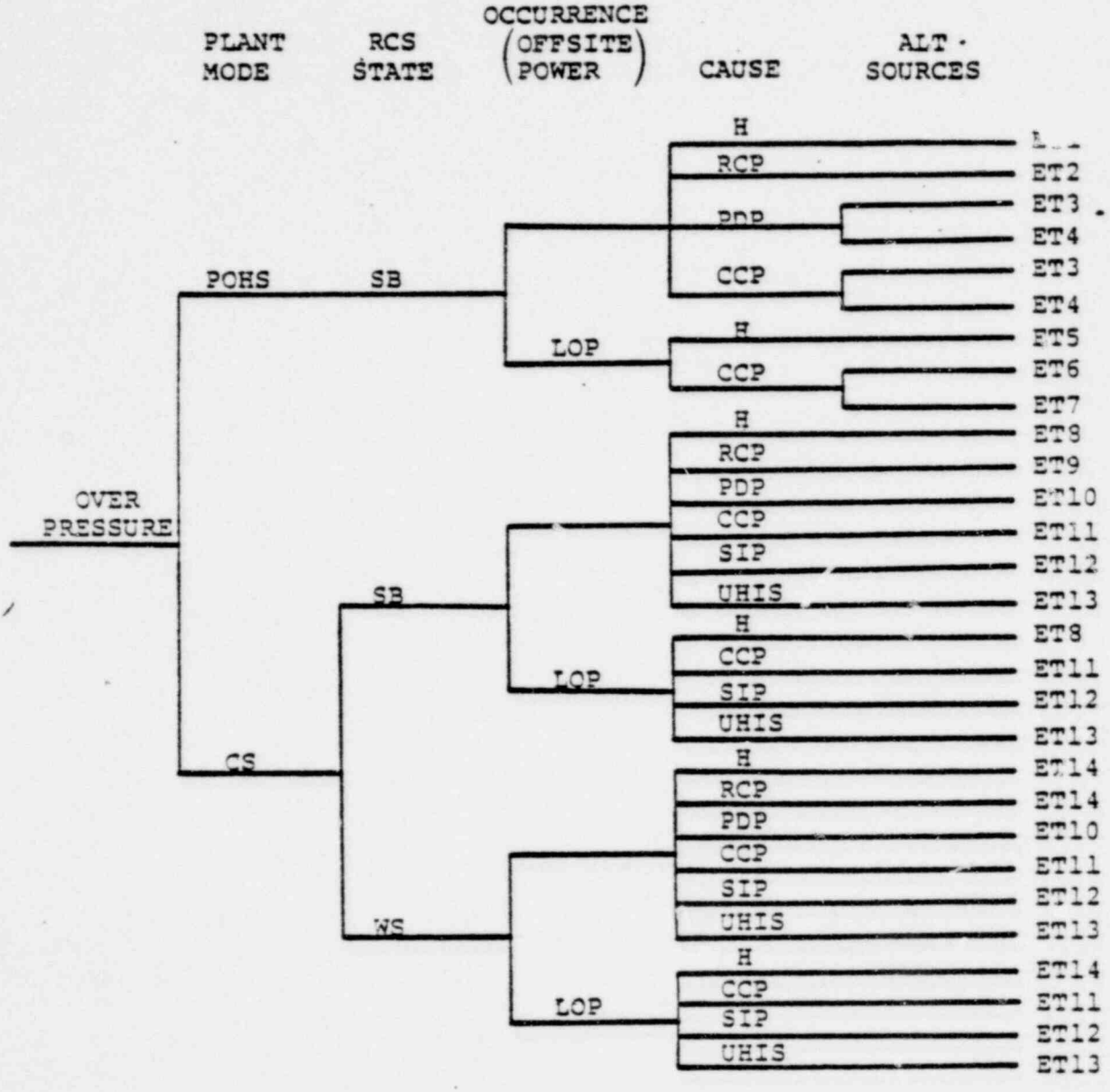

FIGURE 2-6. OVERPRESSURE EVENT TREE - PART I

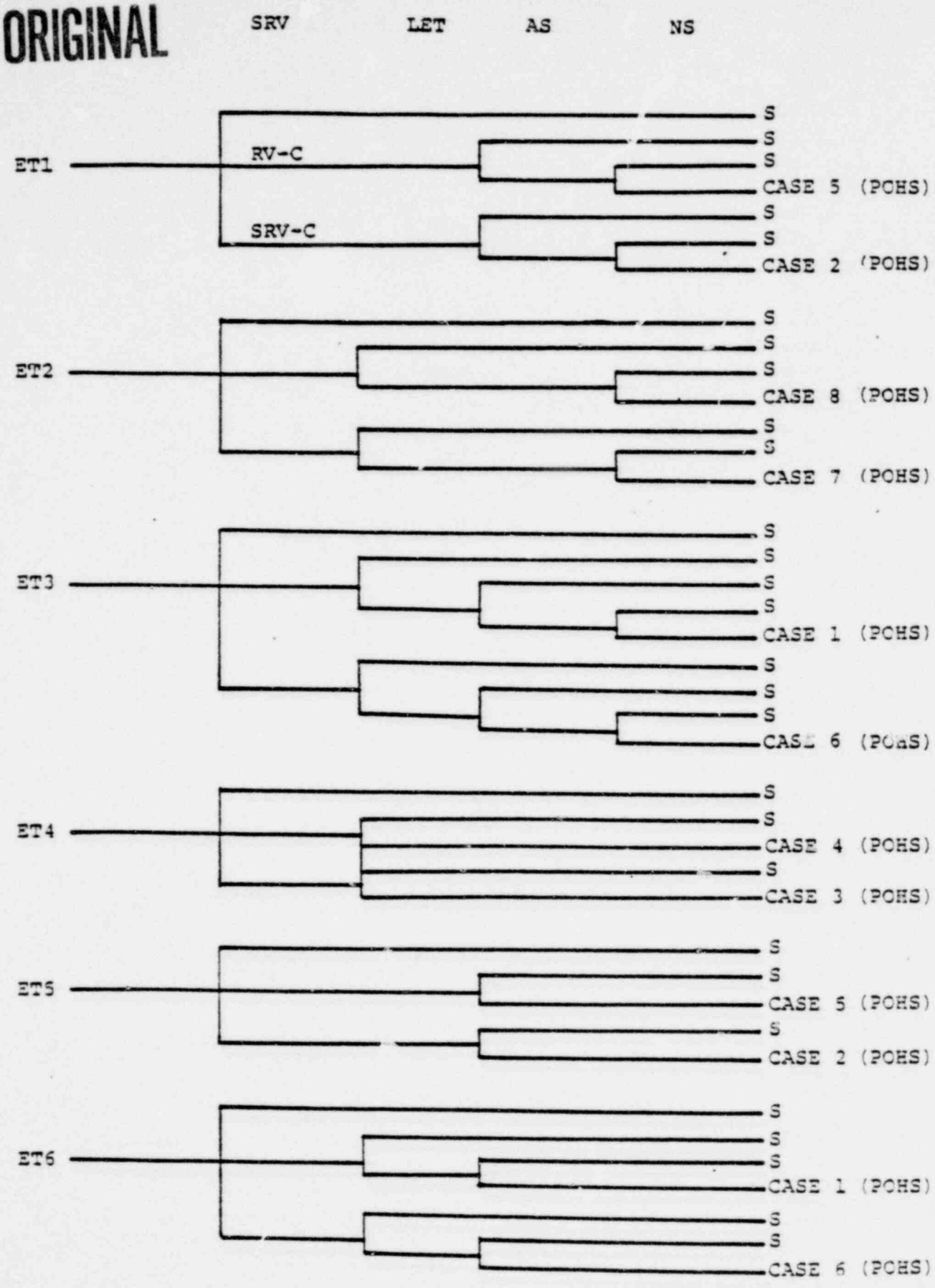

FIGURE 2-7. OVERPRESSURE EVENT TREE - PART II

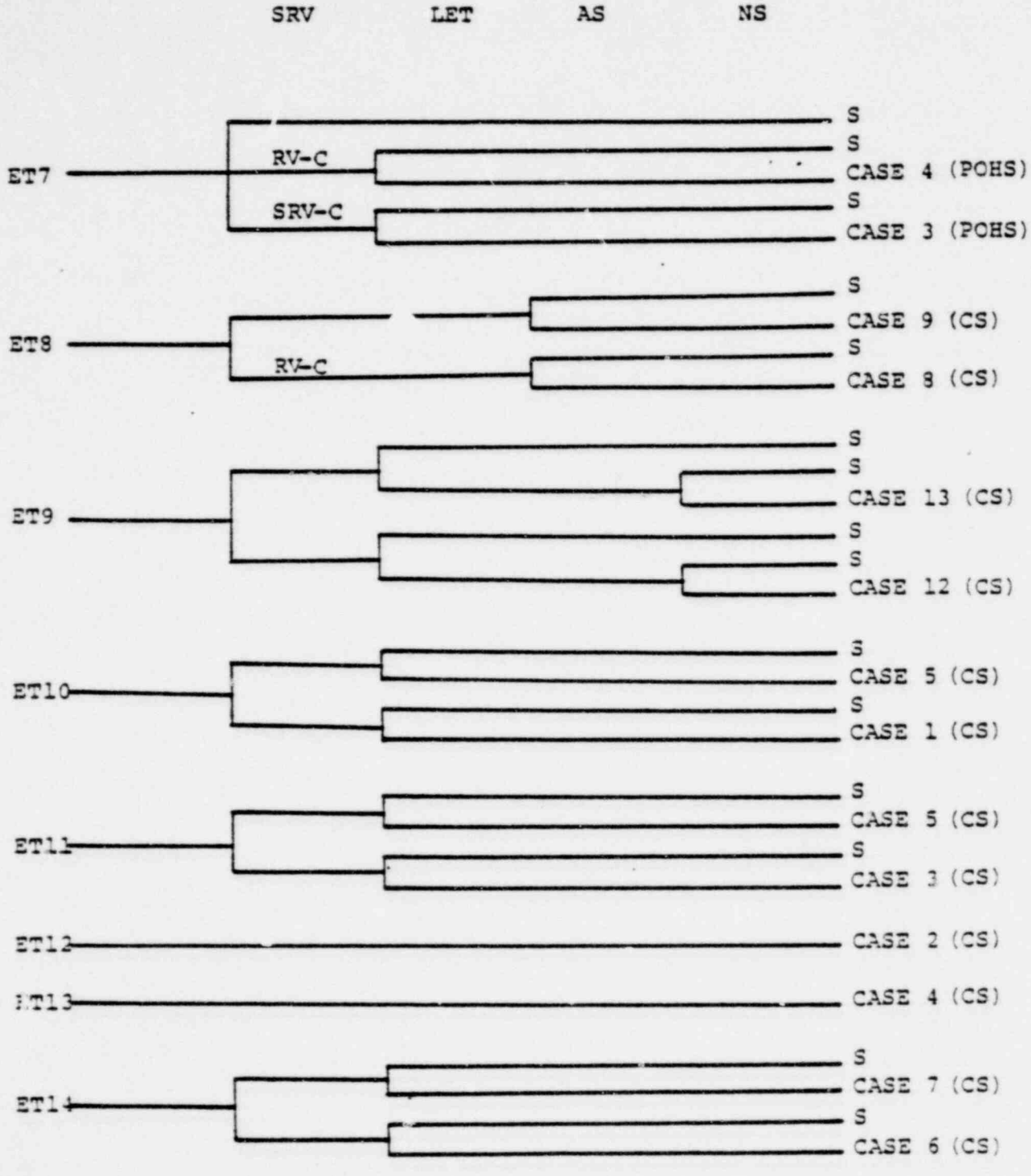

FIGURE 2-8. OVERPRESSURE EVENT TREE - PART III

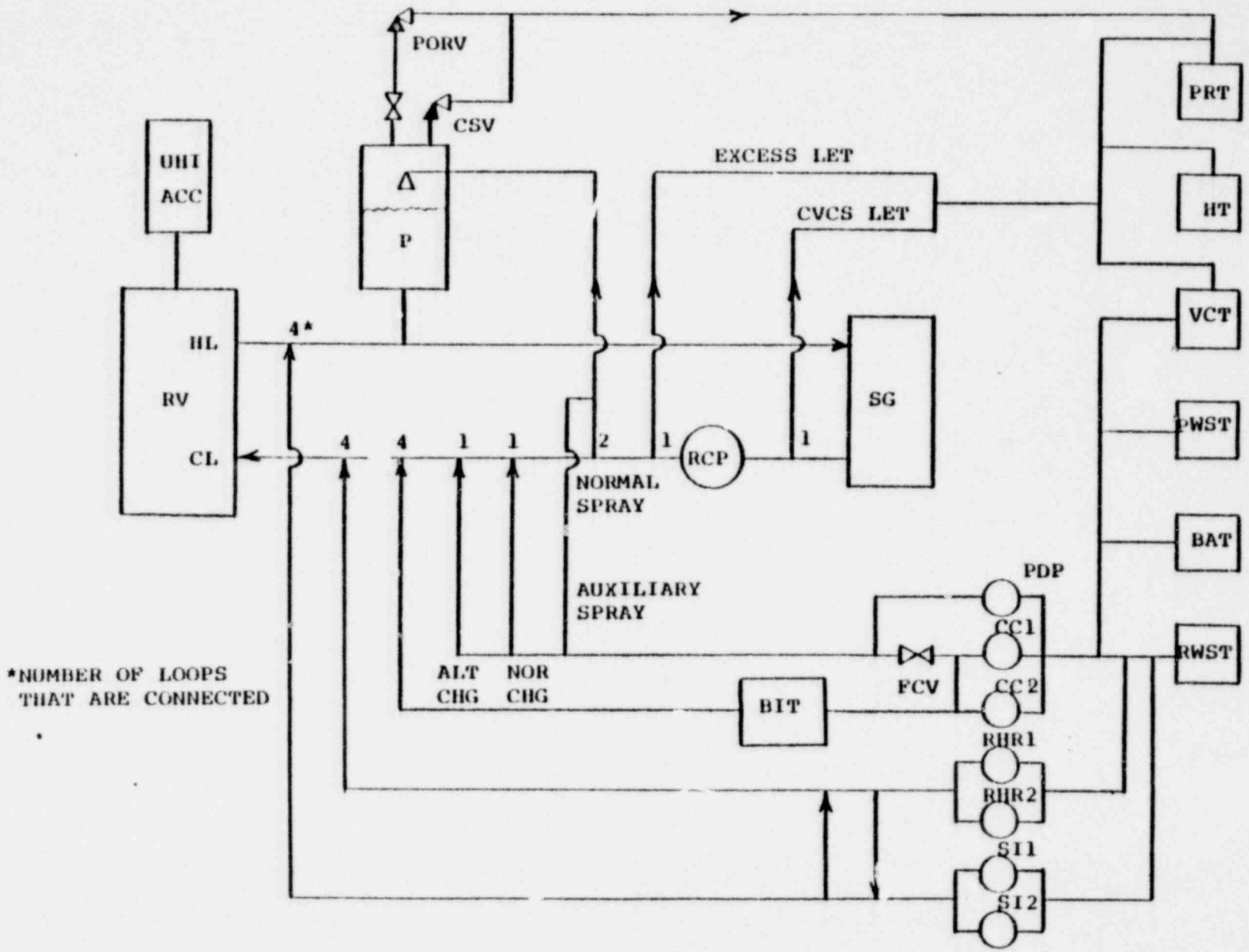

FIGURE 2-9. SIMPLIFIED DIAGRAM OF SUBSYSTEMS INVOLVED IN EXCESS CHARGING, LOSS OF INVENTORY, PRIMARY DHR, AND BORATION

CHAPTER 3

FAULT TREE ANALYSIS TECHNIQUES

The previous chapter has described the development of logic models for important plant functions. When completed, these logic models must be analyzed to determine their susceptibility to potential systems interactions which could prevent or seriously degrade the performance of a particular vital function. The techniques used to identify these potential systems interactions are discussed in this chapter.

Two types of analyses will be undertaken in order to accomplish two principal objectives:

1. To assess the Standard Review Plan and its supporting documents to determine the completeness of the plan regarding the identification and evaluation of potential systems interactions which could impact the performance of important plant functions.
2. To demonstrate how the methodology would be applied to a specific facility in order to determine its susceptibility to the potential interactions defined within the scope of this program.

Section 3.1 describes tasks which are germane to both analyses.

3.1 General Analytical Procedures

3.1.1 Logic Model Evaluation

The fault trees identify systems and components which are necessary to the completion of a particular plant function.

The structure of a tree is determined by relationships between the events (components) which identify the success/failure modes of the function. Hence, the fault trees are graphic representations of Boolean logic relationships between events. The Set Equation Transformation System (SETS),[1] a computer code which performs Boolean algebra manipulation, will be used to derive the minimal cut sets for the fault trees. The minimal cut sets are those distinct combinations of events which will lead to the top event of a tree.* The SETS code determines all of the minimal cut sets, without consideration of probabilities or of the total number of events which must occur. The final output of this task is a list of all the unique combinations of events which will lead to the top event, in this case the failure of a vital plant function. It should be noted that the logic models that have been developed are large and therefore have large numbers of cut sets. If systems interactions were not being considered, one would probably choose not to examine those cut sets which contain many independent events. For this study, <u>all</u> of the cuts sets are being retained and reviewed. This is to ensure that no systems interactions are overlooked which could reduce a cut set with many events to one that contains considerably fewer independent events.

---

*To avoid confusion, all occurrences identified on the fault trees will be termed events rather than failures. Although, most of the events are component failures, some other types of occurrences such as inadvertent or continued operation do exist.

3.1.2 Determination of Linking Characteristics

A system interaction is only possible when there is some connection between the systems. These connections generally exist at the component level. The connection may be physical: a direct and tangible link such as electrical wiring or hydraulic fluid. Spatial connections also exist in which components are linked by environmental conditions, i.e., high temperature or flooding.

The general categories of characteristics which provide possible physical linking between components are:

Motive Power

Control

Actuation

Cooling

Lubrication

Motive power includes AC and DC electrical power, air, steam, and hydraulic power. Control power includes AC and DC electrical power and in some instances air or hydraulic power. Actuation is considered separately from control to account for possible commonalities in sensing and initiation circuitry which could cause an interaction. Cooling consists of indirect and direct cooling, with or without an external cooling medium. An example of direct cooling using an external medium would be the use of component cooling water for pump seals. Other components are cooled by air handling units which may or may not use cooling water. Finally, components

requiring lubrication may derive their lubricant from an internal or external source.

Location will be used to describe possible spatial connections between components. The locations considered are rooms, pipe chases, and general areas that obviously provide an environmental connection. Certain types of interactions may involve location domains that are not as obvious, i.e., a fire may spread between rooms, but these interactions which require special domains are not within the scope of this study. In the first step of the spatial interaction analysis, only the location is considered. The specific environmental conditions which could lead to an interaction need only be investigated after the important locations have been identified. Table 3-1 delineates the linking characteristics which could be associated with the types of components on the fault trees.

Assumptions were made when these linking characteristics where applied to the actual analyses. Manual valves are assumed to stay in their normal position and assumed not to change position due to any systems interactions. These valves are retained as possible independent failures or as causes of an environmental interaction, i.e., a leaking stem resulting in moisture accumulation in a room. Check valves have been excluded because the failure modes of the check valves postulated in the tree (fails open or fails in the reverse direction) do not appear to be subject to any credible external system interaction.

3.2 Generic Analysis

The first goal, the assessment of the Standard Review Plan,* will be accomplished through the generic analysis. This task will identify types of systems interactions which are important and determine whether or not they are addressed in the Standard Review Plan. Although, the logic models were constructed around a specific plant, this analysis should provide information in such a manner that many potential interactions would be identified for any Pressurized Water Reactor. The analysis will not be inclusive; however, as design differences in plants other than a Westinghouse, four loop plant could give rise to additional types of failure modes.

3.2.1 Generic Linking Characteristics

In this part of the analysis it is important to use broad categories of linking characteristics, in order for the Standard Review Plan to be truly tested. Each component will be given support systems which it would need to perform its function. The Standard Review Plan will be studied to determine whether or not it acts to separate these support systems and thus prevent interactions.

Table 3-1 illustrates the categories used for the generic analysis as well as their application to specific components. Each type of component is given linking characteristics which are normally occurring support systems for that type of component.

---

*The Standard Review Plan consists of the plan itself and of all its supporting and referenced documents.

All of the components are given a complete set of characteristics although it is realized that specific components of that type may not exhibit the complete set. For example, motor operated valves are given the characteristics of AC power, DC power, actuation, and location even though not all motor operated valves require DC power. In this analysis, only three locations were used: the containment, the auxiliary building and outside the preceding two. These locations were determined by giving each component the location where it is normally expected to occur.

When a particular column in Table 4.2 is read down, it establishes all the types of components which could be linked by a given characteristic. Hence, every motor operated valve, turbine driven pump, motor driven pump, air operated valve, hydraulic valve, and relief valve in the plant could potentially be linked through the characteristic of DC power. While it is realized that this is not ever the case, this gross categorization provides an excellent method for reviewing the Standard Review Plan. Vital combinations of components are determined through the cut sets, and the Standard Review Plan is relied upon to prevent any potential systems interactions.

It is also realized that certain linking characteristics could be ruled out by factors other than the Standard Review Plan; these include good engineering design and practical equipment layout. These other factors are not considered as we wish only to determine the completeness of the Standard Review Plan in regard to these potential interactions.

3.2.2 Cut Set Sorting

Once the cut sets for a particular fault tree are determined, each component in the tree is renamed giving it each attribute shown in Table 3-1. The computer is then used to search all of the cut sets and provide new cut sets treating each linking characteristic as an independent event. For example, assume that one had the cut set

$$E1 \cdot E2 \cdot E3 \cdot E4 \cdot E5$$

and the table gave linking characteristics as follows:

E1 - Location A, Actuation

E2 - Location A, Actuation, AC Power

E3 - Location A, AC Power, DC Power

E4 - Location A, AC Power, DC Power

E5 - Location A, AC Power, DC Power

After a computer sort, new cut sets would be determined as follows (terms in brackets indicate which events are now replaced by a single system interaction event):

New Cut Sets	Number of Independent Events
Location A[E1, E2, E3, E4, E5]	1
E1 · AC Power[E2, E3, E4, E5]	2
Actuation[E1, E2] · DC Power[E3, E4, E5]	2
E1 · E2 · DC Power[E3, E4, E5]	3

Note: The other combinations of failures which are subsets of the ones given above are also generated, i.e., Location A[E3, E4, E5] · Actuation.

The same cut set that once appeared to consist of five independent failures may now occur in a number of different ways, one of which consists of only one independent event and other which are less than five events.

3.2.3 Interaction Grouping

The Standard Review Plan is for the most part written in general terms, i.e., systems or trains of systems rather than in terms of individual components. For this reason, all of the information attained through the sorting techniques for the generic case needs to be coalesced into broader categories. The reviewing task is also made easier in that many cut set containing potential interactions are reduced to far fewer cut sets containing potential systems interactions. Using our previous example, suppose that events E2, E4 and E5 are components in Train A of system Q, and that E3 is a component in System R, and finally that E1 is a part of train B of system Q.

Event	System
E2	Train A, System Q
E4	Train A, System Q
E5	Train A, System Q
E3	System R
E1	Train B, System Q

One would now review the cut sets listed in section 3.2.2 in terms of systems rather than components. For example, instead of reviewing to see if individual pumps and valves

represented by events E1-E5 are excluded from sharing a common location, one would review the Standard Review Plan to determine if:

Train A of System Q

Train B of System Q

System R

are precluded from all sharing a single location.

3.2.4 Review Procedure

The most significant potential interactions are those that involve all the events of a cut set. This would indicate that there exists a potential for a single failure which would compromise the completion of a given plant function. The prevention of single failures is the philosophy that dominates the Standard Review Plan and its completeness in the evaluation of potential single failures is of principal importance.

Other systems interactions may also be important, as there are undoubtedly cases in which the occurrence of two or more independent events is more likely than a single event. The Standard Review Plan will also be examined to determine if other interactions which are elements of cut sets with other independent events are evaluated. This will be carried out as far as practible to cases where three independent events must occur. Preliminary results, however, indicate that potential interactions which lead to the top event of a tree only if two other independent failures occur are generally not covered

in the Standard Review Plan. This is principally due to the single failure philosophy and the general rather than specific nature of the document.

The output of this task is a list of the important potential interactions and their coverage in the Standard Review Plan and its supporting documents. Specific statements which preclude certain interactions will be documented. If the only reference to a potential interaction is in inference to a general statement, i.e., no single failure shall prevent operation of a system, it will be documented as such. Finally, potential interactions not mentioned in any manner will be pointed out.

3.3 Specific Analysis

3.3.1 Interaction Characteristics

The second goal of the analysis, the application of the technique to a specific plant, is being realized through another analysis. Although similar to the first, this analysis is based on a specific plant and deals with much finer detail. Each component which is an event in a cut set is being analyzed to determine its true supporting systems. The same categories are being used, but their breakdown is considerably more specific as defined below:

1. AC Power - Train A and Train B. The AC power is divided into the two emergency divisions. While it is realized that many potential interactions exist at a more detailed level, a conservative approach is taken by linking all components deriving power from a

particular train. For example, two valves on Train A may share a circuit breaker which could result in a potential interaction. This interaction, however, is a subset of the potential interactions that exist for all components on Train A.

2. DC Power - Train A and Train B.
3. Cooling. For the first analysis, only the broad categorization is being used. In this manner, the importance of cooling certain components will first be identified through the cut sets. The information regarding the specific cooling systems of these components can then be used to search for interactions.
4. Compressed Air. All components needing compressed air will be linked by this attribute.
5. Actuation. The individual electrical schematics are being reviewed when available. External inputs into the control circuits of components are being identified as possible actuation links. For example, many CVCS valves receive automatic actuation based on system conditions (Volume Control Tank Level, etc.). All components which have the same input into their circuits are being linked by that circuit.
6. Hydraulic. Any components needing external hydraulic power are being identified.
7. Lubrication. If a component requires lubrication from an external source, it is being given this characteristic.

8. Location. The specific locations, be they rooms, pipe chases, or general areas are being identified for all the components in the cut sets.

3.3.2 Cut Set Analysis

The computer sorting technique used in the generic analysis will also be used for the specific analysis. For the specific analyses, all new cut sets generated by the potential interaction sorting will be reviewed if the new cut sets now consist of three or less independent failures. For example, the cut sets

New Cut Sets	Number of Independent Failures
Location C100[E6, E7, E8, E9]	1
E6 · Power AC Train A[E7, E8,E9]	2
E6 · E10 · DC Power Train B[E12, E13, E14, E15]	3
E14 · Actuation Circuit A22 [E16, E17] · Location A12[E19, E20]	3
Location P[E18, E20] · Actuation Circuit [E22, E25] · Power AC Train A[E7, E8, E9, E10]	3

would all be retained for further review, while cut sets like:

E15 · E26 · E17 · E28

E15 · E17 · E22 · Actuation Circuit A24[E23, E30]

would not be retained as they involve more than three independent failures.

The cuts sets so retained will then be analyzed to determine whether or not an interaction truly exists. Special attention

will be paid to the potential location interactions, as location by itself does not imply failure. The rooms or areas which are det. mined to be important (through the cut sets) will be reviewed to identify credible events in that room which could bring about an environmental condition that could affect all the members of a cut set. When support systems have been divided into trains, these trains must also be analyzed to ensure that they are truly independent.

3.3.3 Interaction Review and Ranking

Finally, after a list of credible potential interactions has been compiled, an attempt will be made to assess the significance of these potential interactions. It should be emphasized that up to this point the only quantitative reduction in the data occurred after the specific sorting when the list was reduced to cut sets containing three or less independent events. All of the cuts sets were reviewed for potential common modes, no matter how large. After fina. compilation of all important potential systems interactions, a more qualitative review will take place in order to rank these potential interactions and for comparison to non-interactive failure modes of the system. This ranking will be relative and based on a number of factors.

If the interactions are single failures which would cause the top event, the type of interactions purposed will be ranked based upon experience. Those types of interactions which are similar to failure modes which have been seen would be ranked above interactions which do not appear to relate to any known

failure modes. For the other cut sets which involve combinations of independent failures and potential systems interactions, the interactions will first be ranked by the method above. Then this list will be integrated with a ranking of the independent events that must occur with each interaction. These rankings of independent events will be relative and based upon industry experience, i.e., a motor operated valve failure is more likely than a check valve failure.

Finally, these rankings will be reviewed in terms of the non-interactive cut sets. These represent the independent failure modes which could prevent the operation of a function. For example, if the function could fail by means of two independent failures that are failures of the type that have been experienced in other systems, this could be used to put some highly unlikely potential interactions into perspective.

TABLE 3-1

COMPONENT	LINKING CHARACTERISTICS								
	AC POWER	DC POWER	ACTUATION	COOLING	LUBRICATION	AIR	STEAM	HYDRAULIC	LOCATION
MOTOR DRIVEN PUMP	X	X	X	X	X				X
TURBINE DRIVEN PUMP	X	X	X	X	X		X		X
MOTOR OPERATED VALVE	X	X	X						X
AIR OPERATED VALVE		X	X			X			X
HYDRAULIC VALVE	X	X	X					X	X
MANUAL VALVE									X
SAFETY VALVE									X
RELIEF VALVE	X	X	X			X			X
CHECK VALVE									X

CHAPTER 4

STANDARD REVIEW PLAN ANALYSIS

The generic analysis techniques described in Chapter 3 have been applied to the logic models of the Reactor Coolant Pressure boundary function. There were two fundamentally different fault trees for this function, one dealing with the plant operating modes of power operation through hot shutdown, and the other for the cold shutdown mode. In addition, each of these trees has a slightly different structure for the Loss of Offsite Power transient. The cut sets for all four of these logic models were obtained and analyzed for potential interactions. Questions were then formulated which encompassed the types of potential interactions seen in the cut sets. Sections 4.1 through 4.3 discuss the results of the Standard Review Plan (SRP) analysis as to its coverage of the types of interactions seen. Due to the large variance in types of failure modes of this function, the relevance of the questions asked of the SRP reviewer is not immediately obvious. Section 4.4 discusses the reasons for the questions and the significance of the review results.

4.1 Power Operation Through Hot Shutdown

4.1.1 Potential Single Events Leading to Breach of Reactor Coolant Pressure Boundary

Does the SRP and its supporting documents:

1. Prevent a power operated pressurizer relief valve and its associated isolation valve from sharing a common actuation signal?

2. Prevent a power operated pressurizer relief valve and its associated isolation valve from sharing a common location?

3. Prevent the redundant RHR suction valves from sharing a common actuation circuit?

In review of the SRP and supporting documents, the basic approach was to first review the basic system SRP sections which address the pressurizer relief valves and RHR suction valves themselves. From an overall system viewpoint these are sections 5.4.13, 5.4.12, 5.4.10, 5.4.11 and 5.4.7. These further reference other SRP sections, Branch Technical Positions, General Design Criteria, Regulatory Guides, IEEE Standards, and sections of the ASME code. These were scanned to determine what additional requirements were imposed by these documents which would impact the questions above. The results of the review is as follows:

No statements specifically related to the first two questions could be found in the SRP or referenced documents. A number of general statements which might imply answers to the first two questions are summarized below:

- From 5.2.2 (III.1) - The piping and instrumentation diagrams are examined to determine the number, type, and location of safety and relief valves ... (However, it is not clear what the examiner reviewing for.)
- From 5.2.2 (I) - EICSB, as described in SRP 7.6, evaluates the adequacy of controls and instrumentation of the overpressure protection components ...

- From 7.6 (II) - The acceptance criteria discuss in general terms the requirements of redundancy, single failure criteria, and functionability. Related documents such as IEEE 279 and others elaborate on these requirements but no specific mention is made of the design relationship between power operated relief valves and their isolation valves. One statement related to the relative physical location of components (in general) is found in 7.6 (II) which states the ASB reviews the physical arrangement of components and structures related to "other instrumentation systems required for safety" ... and determines that single events will not disable redundant parts of these systems.
- From ASME Code, Section III, Article NB-7000 (referenced in SRP section 5.2.2) ... redundancy and independence of pressure relief devices and their associated ... systems must be employed to preclude loss of overpressure protection ...

As a result, it appears that general statements may apply to the first two questions, but no specific references to such design requirements can be found.

With regard to question #3:

- From BTP-RSB 5-1 (referenced in 5.4.7) - Items B.1 (a) thru B.1 (c) apply <u>specifically</u> to this question to assure that the RHR system can not be inadvertently opened to RCS pressure by discussing the need for

two valves on the suction line which have independent diverse interlocks. Other references to single failure criteria and redundancy are also made.

4.1.2 Potential Interactions Involved in Cut Sets with 2 Independent Events

Does the SRP and its supporting documents:

1. Prevent both power operated pressurizer relief valves and their isolation valves from sharing common AC and/or DC power sources?
2. Prevent both power operated relief valves from sharing a common actuation circuit?
3. Require that power operated relief valves be used?
4. Require that pressurizer relief valves not share actuation circuits with CVCS letdown and charging systems?
5. Require that pressurizer relief valves or their isolation valves not share actuation with CVCS charging pumps?
6. Require that pressurizer relief valves or their isolation valves not share actuation with pressurizer relief valves?
7. Require two trains of high pressure injection system? (In this case, this would be the CVCS pumps.)

Further, does the SRP address the questions below:

8. Can all of the CVCS be on one power source or one control and actuation circuit?

9. Is any mention made of suction sources for the CVCS sharing actuation circuits with the letdown paths?

10. Are all letdown and excess letdown control valves allowed to be on the same actuation circuit?

11. Is any mention made of the Primary Water Makeup System and its relationship to the CVCS?

With regard to the first two questions above, the same references and statements apply as for question #1 and #2 in the previous section.

For question #3, the following statements can be made:

- From ASME Code, Section III, Article NB-7000 (referenced in SRP section 5.2.2) - Any of the following types or combinations of types of pressure relief devices may be used to secure the required relieving capacity:
  a) Safety valves meeting the requirements of NB-7610;
  b) Pilot operated pressure relief valves subject to meeting the requirements of NB-7620;
  c) Power actuated pressure relief valves subject to meeting the requirements of NB-7630;
  d) Safety valves with auxiliary actuating devices meeting the requirements of NB-7640.

Besides the SRP sections and related documents reviewed for potential single events, SRP section 9.3.4 (CVCS) and referenced documents were examined relative to questions #4 and #5 above. The following result was obtained:

- No mention of shared actuation circuits between the CVCS and pressurizer relief valves or isolation can be found.

To the extent that portions of the CVCS may also be the high pressure injection system, SRP sections 6.3, 7.3, and related documents were reviewed in addition to 9.3.4 for questions #6 and #7. With regard to question #6, no direct reference to sharing actuation systems can be found. However:

- From IEEE 279 - section 4.6 (referenced in SRP section 7.3) - requirements for channel independence applies ... between redundant ESFAS components and interfaces between ... ESFAS and nonsafety-grade systems ... This statement implies that safety system independence is reviewed. The specific interaction in question 6 might be reviewed since it involves an ESFAS interface.

For question #7:

- SRP sections 6.3, 7.3, 9.3.4, and related documents all have statements concerning redundancy, single failure criteria, and independence which appear to adequately address this question.

SRP sections 9.3.4, 7.3, and related documents were reviewed for questions #8, 9, and 10. Questions #9 and #10 are too detailed and are not specifically addressed. However, the many references to redundancy, single failure criteria, and independence would seem to generally address these concerns.

With regard to question 8, the safety related portions of the CVCS must meet the single failure and redundancy requirements.

- For question #11, specific reviews of SRP sections 9.3.4 and 9.2.3 were conducted. There appear to be no specific design relationships required between the makeup system and the CVCS other than the assurance that each functions properly and that (from 9.2.3): ... a malfunction or failure of a component will not have an adverse effect on any safety-related system or components.

4.2 Cold Shutdown - Potential Interaction Involved in Cut Sets with 2 Independent Events

Does the SRP and it supporting documents address the following questions:

1. Are the pressurizer heaters and the CVCS charging systems required to be separate in actuation?
2. Are the pressurizer heater control and the pressurizer valves (especially alternate spray) required to be separate in location?
3. Are the pressurizer heaters required to be independent in actuation from both power operated relief valves and their isolation valves?
4. What are the isolation requirements for the upper head injection system? Can one actuation signal be used to initiate the system?
5. Are the letdown and excess letdown paths required to be independent in actuation and motive power?

6. Is the boric acid tank required to have two trains of heating?

For questions #1, 2, and 3, SRP sections 5.4.10, 5.4.13, 9.3.4, 7.7, and related documents were reviewed. No specific references to these possible interactions could be found. The major concern for systems such as the pressurizer heaters is taken from 7.7:

- From 7.7 (II) - The control systems not required for safety are acceptable if failures ... would not significantly affect the ability of plant safety systems to function ... or cause plant conditions more severe than those for which the plant safety systems are designed.

Questions #4 and #6 appear to be adequately addressed by the following:

- From 6.3 (II) - Many statements exist concerning single failure requirements and redundancy of these systems. For example, ... actuation must be initiated by signals of suitable diversity and redundance ...
- From 7.3 - Many more and similar statements as the one above exist in this SRP section. IEEE 279 provides sufficient guidelines in this area.

With regard to question #5, the following result was obtained:

- No specific mention of two letdown paths is made. However, similar general statements as mentioned for other questions appear to apply. More specifically:

- From 9.3.4 (II) - The reviewer ... determines that the system can sustain the loss of any active component and meet the minimum system requirements for site shutdown or accident mitigation.

4.3 General Conclusions Concerning SRP Review

Those questions concerned with the requirements of two trains or two actuation signals for a given system appear to be adequately covered by the SRP and related documents. Other questions, particularly those affecting possible common modes between systems are probably not well addressed. Further, many of the questions are too detailed to be specifically addressed by the review process. "Motherhood" statements concerning redundancy, single failure criteria, and others may implicitly cover the particular concerns; however, this probably depends on the degree of detail covered by the reviewer when examining each system.

4.4 Significance of SRP Results

The two previous sections have outlined the results of the actual SRP review process. These results do not alone provide useful information. The origins of the questions and their relation to failure of the function need to be explained. In section 4.5 these results will also be put into perspective; that is, compared to other failure modes of the function.

Table 4-1 summarizes the results of the SRP review. The first three items in the table are most important, as these represent potential systems interactions which could cause

breach of the pressure boundary in a single event. The Residual Heat Removal (RHR) suction valves provide a direct interface between low and high pressure piping. The cut sets identified these valves as being subject to a potential interaction if they were to share an actuation system. The SRP specifically states that these valves must be redundantly interlocked to prevent their inadvertent opening.

The other potential single events involved the power operated pressurizer relief valves. These valves and their associated isolation valves were identified with possible linking characteristics of actuation and location. Neither of these items were covered specifically in the SRP. Certain general statements could possibly imply that these situations should be reviewed for. The failure modes being considered involve a possible actuation or environmental link between a relief valve and its isolation valve that could result in a small LOCA that could not be isolated.

All of the other questions are derived from cut sets which involve more than a single event. In addition, all of the cut sets that these originate from result in overpressurization. A series of events leads to some level of overpressurization but the failure of the boundary will not occur in every case (its probability is, however, higher). The only overpressurization branches actually reviewed involved overcharging to a water solid state. This was a direct result of the fact that the system modeled had three code safety valves, each of which was considered to be an independent failure (when failing

in a closed state). Therefore, more than three indpendent failures would have to occur before the system pressure could get above 2485 psi in all cases except the water solid case. The information obtained in the analysis of this logic model is general in nature, and much of it applies to reactors which might have less than three safety valves.

In Table 4-1 the potential interactions outlined in questions from section 4.1.2 all involve similar failure modes. All are combinations of overcharging, insufficient letdown, and insufficient pressure relief which lead to an overpressure state. The combinations of ways in which this can take place are numerous as evidenced by large numbers of cut sets. The questions specifically address interactions which could reduce the number of independent failures necessary to bring about this sequence of events. This mode of overpressurization could occur in one event if the CVCS charging and letdown, and the pressure relief devices were linked to a common actuation circuit. This particular type of interaction may not be reviewed for in the SRP. The postulated interaction would probably occur in a pressure sensing circuit. Even if all three of these subsystems did share a common pressure sensing device, one must postulate a failure which would cause the system to overcharge, the letdown to close, and the power operated relief valves to stay closed. In conclusion, a potential interaction has been discovered which may not be specifically reviewed for. This interaction does not, however, appear to be particularly likely to occur.

Other interactions involving this sequence of overpressure were also reviewed. These are basically subsets of the interaction above. Once again, the sequence involves overpressurization through overcharging, insufficient letdown, and insufficient pressure relief. A systems interaction which could reduce the number of events in this sequence would be a tie between CVCS charging and letdown. This does not appear to be covered in the SRP and does appear to be highly plausible. However, even if the overcharging and insufficient letdown occur as a result of a single event, two other failures must occur: pressure relief failure and failure of the boundary due to excessive pressure.

The questions which are listed in section 4.2 all involve overpressurization in the cold shutdown model of operation. Once again, rupture of the system is not assured through overpressurization, which is defined in this case as any pressure over 400 psi. One method of overpressurization involves overcharging. The potential interactions involving overcharging and insufficient letdown have been discussed above.

Another method of overpressure in this case involves excessive heat input. Potentials for interactions were found to exist if the heaters and CVCS system were to share actuation. This interaction was not specifically reviewed in the SRP and appears to be possible. A low pressure sensor failure could be postulated which would cause the heaters to start and the CVCS to charge the system. If the pressurizer is not subsequently sprayed down, the pressure would continue to rise. The normal

charging path must close or the spraying will be inadequate due to the fact that the water would primarily be entering the system through the normal charging path. In conclusion, a potential interaction has been found which does not appear to be covered in the SRP and which could lead to an undesirable pressure rise in the cold shutdown state.

The pressure rise in the previous case would be limited if the power operated relief valves worked. A failure mode that would cause the heaters to come on, the CVCS to malfunction and the pressure relief valves to fail closed, all in a single event, appears unlikely. This is because the heaters and charging would react to low pressure while the relief valves would react to high pressure.

The pressurizer heaters (or at least some their electrical support systems) share a common location with the pressurizer spray valves. This does not appear to be reviewed for in the Standard Review Plan. However, once again it is difficult to postulate a failure mode due to an environmental condition which would cause the heaters to fail in the on position and the spray valves to fail in a closed position.

In the cold shutdown state, the system could be subjected to a pressure surge if the upper head injection system were to inadvertently discharge. The SRP specifically reviews the isolation of these types of systems and requires that they be redundant and free from single failures.

4.5 Conclusions - Generic Analysis of Reactor Coolant Pressure Boundary

A number of potential interactions were discovered which do not appear to be covered specifically in the review process outlined by the Standard Review Plan. The significance of these potential interactions can only be determined when the event sequences are reviewed and compared to non-interactive failure modes of the system.

The potential interactions involving the power operated pressurizer relief valves and their isolation valves appear to be significant; principally because a single event, either in actuation or environmental, could result in a small LOCA. Other non interactive LOCA's are also possible in a single event, i.e., the sticking open of a safety valve.

Some potential interactions which appear in cut sets with other indpednent events were also identified. Many of these, especially those involving the CVCS charging and letdown, could result in overpressurization occurring as the result of two or three independent events. These potential interactions to not appear to be too important when one realistically reviews the sequence of events. The cause of the over-pressurization, be it heat addition or inadvertent pump operation, must be continuous and the operator is assumed either to not try or to not be able to turn off the cause of the overpressurization. This assumption is highly conservative. In addition, these overpressurization incidents result in pressures above technical specification limitations, but would seldom be expected to

rise above the static test pressure. The failure of the boundary at these higher pressures is more likely but not assured.

Table 4-1

SRP Review Results

Section Number	Question Number	System Involved	Potential Interaction	SRP Coverage			Other Events in Cut Set
				Specific Statements	General Statements	Not Covered	
4.1.1	1	Power Operated Relief Valves	Actuation		Yes	Possibly	None
4.1.1	2	"	Location		Yes	Possibly	"
4.1.1	3	RHR Suction Valves	Actuation	Yes			"
4.1.2	1&3	Power Operated Relief Valves	Motive Power		Yes	Possibly	Overcharging
4.1.2	2	"	Actuation		Yes	Possibly	"
4.1.2	4&5	Power Operated Relief Valves and CVCS Letdown and Charging	Actuation		Yes	Possibly	Overpressure Induced Rupture
4.1.2	6	Pressure Relief		Same	Yes		Overcharging
4.1.2	7	High Pressure Injection	Motive Power	Yes			Pressure Relief
4.1.2	8,9,10	CVCS Charging and Letdown	Actuation		Some	Possibly	Pressure Relief

Table 4-1 (Continued)

Section Number	Question Number	System Involved	Potential Interaction	SRP Coverage			Other Events in Cut Set
				Specific Statements	General Statements	Not Covered	
4.2	1	Pressurizer Heaters and Charging	Actuation		Yes	Possibly	Pressure Relief
4.2	2	Pressurizer Heaters and Sprays	Actuation Location		Yes	Possibly	*
4.2	3	Pressurizer Heaters and Pressure Relief	Actuation		Yes	Possibly	Pressurizer Sprays
4.2	4	Upper Head Injection	Actuation	Yes			None
4.2	5	Letdown Paths	Actuation and Motive Power			Yes	Inadvertent Pump Operation
4.2	6	Boric Acid System	Actuation and Power	Yes			Pressure Relief

Table 4-2

Generic Analysis Conclusions

Systems	Interactions
Interactions Not Covered in the SRP and Considered Somewhat Important	
Power Operated Relief Valves - Relief Isolation Valves	Actuation and Location
Interactions Not Covered in the SRP and Not Considered Important	
CVCS Charging - CVCS Letdown	Actuation Motive Power
Pressurizer Heaters - CVCS Charging	Actuation
Pressurizer Heaters - Pressurizer Sprays	Actuation Location
Power Operated Relief Valves - CVCS Charging	Actuation
Interactions Covered in the SRP	
RHR Suction Valves	Actuation
CHIS Isolation	Actuation

CHAPTER 5

EXEMPLARY PLANT ANALYSIS

Information on the exemplary facility was obtained and utilized as described in Chapter 3. The reactor coolant pressure boundary function was divided into two basic logic models; one dealing with the plant operation modes of power operation through hot shutdown, and the other covering the cold shutdown mode. The specific analysis was done separately on these two models. In addition, the loss of offsite power transient was recognized as providing different failure modes than other transients. For this reason, both of the logic models were analyzed twice, with and without the availability of offsite power.

5.1 Logic Model Overview

Before discussing the results in detail, an overview of the reactor coolant pressure boundary is necessary for perspective. The mitigating systems were not modeled.* The exclusion of the LOCA mitigating systems results in two characteristics of this analysis which should be emphasized: 1) the occurrence of the top event of the reactor coolant pressure boundary tree does not necessarily lead to unacceptable core damage, 2) any systems interaction which causes the pressure boundary to fail

*We were not tasked to model mitigating systems due to the amount of attention that these systems have received in other studies.

and also results in the failure of one or more of the available mitigating systems will not be analyzed.

The pressure boundary function is generally divided into three types of occurrences which could result in boundary failure: 1) ruptures and leaks of pipes and components, 2) interfacing systems which, if failed, would allow high pressure fluid to enter low pressure piping, and 3) over-pressurization. The ruptures and leaks are single events which immediately breach the pressure boundary. Although missiles were considered in the location analysis of specific components, not all pipes within the pressure boundary were reviewed for the possibility of missile induced rupture. The justification for not analyzing all potential missiles is that these are reviewed extensively in the safety analysis and that the most likely source for missiles and pipe whip are those high pressure lines within the pressure boundary. If one of these were to fail and produce a missile or other effects, it could cause systems interactions. However, for this analysis the rupture of the pipe would by itself cause the top event. (These missiles and pipe whip generated by primary system rupture could be very important if one were analyzing the mitigating systems.)

The interfacing systems include all subsystems which at some point enter the boundary of the reactor coolant system. As previously discussed, check valve failures are assumed not to be subject to potential interactions other than water hammer phenomena. In addition, the failure of the check valves which separate high and low pressure is generally enough to cause the

top event; hence very few interactions are postulated for the interfacing systems.

5.2 Specific Results - Power Operation Through Hot Shutdown

The only potential interaction involving interfacing systems involves the RHR suction valves. The analysis of the exemplary facility shows that these valves are not subject to any interaction within the scope of this project.

Another type of interface with the pressure boundary involves the pressure relief capability. Given a transient which would cause the safety valves to open, there is some chance that one or more of these valves would fail to reclose. This was found to be an independent event and not subject to potential interactions. The power operated relief valves also interface with the pressure boundary. A potential interaction was found at the exemplary facility involving these valves. The power operated relief valves and their isolation valves share a common location. Sharing location is by itself not a failure - one would have to postulate a failure mode which would affect the components sharing the location. In this case, the failure mode would involve the failure of a power operated relief valve in such a manner that it could not reclose and at the same time it would leak (spray) its isolation valve and prevent its closure. It should be noted that this valve is environmentally qualified for a LOCA in the containment.

Finally, the pressure boundary can fail as a result of overpressurization. Overpressure alone does not necessarily

cause failure of the boundary; it brings about a situation in which the likelihood of failure is increased. Since the failures of each of the code safety valves were considered to be independent events, almost all of the overpressure branches of the logic model involve more than 3 events to achieve a pressure greater than 2485 psi. If water is continuously pumped into a closed system, the system could be driven water solid and the pressure could exceed the 2485 psi pressure limit.

For the power operation mode through the hot shutdown state, no interactions were found which could result in over-pressurization in a single event. The cut sets reviewed involved the following sequence of events:

1. Inadvertent and continued high pressure pump operation.
2. Closure of letdown and excess letdown paths.
3. Failure of pressurizer relief valves.
4. Inadvertent opening of valves to additional water sources for the pump.

In some cases, many of the members of a cut set were found to share a linking characteristic. For example, both power operated relief valves, the letdown isolation valve, and the primary water suction valve all are linked by compressed air. Upon further investigation, however, one will find that no failure mode of the air system could fail all the components in the position needed to bring about the failure mode. All of the valves would fail closed upon loss of air. For the failure mode indicated, the primary water valve needs to fail open

in order to supply an additional source of water for charging. In addition, there are two trains of compressed air. The only interactions found in this part of the analysis were between two components in a sequence of more than three events. These interactions would be expected as they generally occurred within a single train. In conclusion, no potential interactions were found at the exemplary facility which would result in overpressurization.

5.3 Specific Results - Cold Shutdown

The cold shutdown case was slightly different in that only overpressure was considered. Overpressure was defined as any pressure above 400 psi during cold shutdown. Breach of the boundary could then occur as a result of rupture or through an interfacing system. The residual heat removal system is operating during cold shutdown. This system has an operating limit of 400 psi and a design limit of 600 psi. Any pressure transient above these values could result in rupture of the low pressure system.

Once again, no potential interactions were found which could result in overpressurization in a single event. In some cases all the elements of a cut set were linked by a characteristic but no failure mode could cause both events to happen. For example, some cut sets involved heaters failing on and a valve failing to move. Although both may share a power source it is difficult to postulate a failure mode which would cause both events.

The interactions which are elements of cut sets containing two or more events were not found to be significant. For

example, many of the valves in the letdown path share motive power sources, but there are also many single events which could fail a letdown path. The power operated relief valves and many of the charging and letdown valves need compressed air, but there are two trains of this air. If the entire air system were to fail, the pressurizer relief valves would fail closed, the letdown path would fail closed, the charging path would fail open, and the alternate pressurizer spray would fail closed. This, coupled with an inadvertent pump startup or a heater failing in the on position could bring about excessive pressures. The compressed air system is currently being reviewed for its potential for a single failure. The pressurizer relief valve isolation valves also share a common location. One could postulate a local moisture accumulation which would cause these valves to fail closed. The pressure could then raise above the limit for these valves, but this pressure rise would consist of one or more additional failures.

5.4 Conclusions - Specific Results for Reactor Coolant Pressure Boundary

The most significant potential interaction found at the exemplary facility involves the pressurizer power operated relief valves. These valves share a common location with their isolation valves. If a pressurizer relief valve were to fail open and also leak (spray), it could potentially fail its own isolation valve.

No significant interactions were found in the other branches of the tree dealing with the power operation through hot shutdown

modes. The only interactions found were in cut sets with three or more independent events. In addition, all of these interactions except for the location interaction potential of the two relief valve isolation valves involve components within the same emergency division, i.e., two components in train A. These interactions became even less significant when one realizes that for these sequences of overpressurization to occur, no operator intervention is assumed in response to the cause of the overpressurization.

The analysis of the cold shutdown case once again revealed only interactions in cut sets with more than two independent events. These interactions also mostly involved interactions between components on the same emergency train which are known interactions.

Some potential for interaction was discovered between letdown and excess letdown. Even if all the letdown were to fail in a single event other events such as overcharging, heat addition, and failure of pressure relief must occur. These potential interactions are overshadowed by the non-interactive cut sets which could bring about an undesirable pressure rise. These include the single events: safety injection pump inadvertent startup, CVCS pump inadvertent startup, and reactor coolant pump inadvertent startup. There are also a number of double events which include pressurizer heater startup and failures of letdown or spray valves. In conclusion for the cold shutdown case, some potential interactions were discovered between events in cut sets. None were judged to be significant when

number of failures and realism of the sequence of events was considered. However, it is interesting to note that the cuts sets do identify a number of single non-interactive events which would lead to an undesirable pressure rise. The administrative controls on the cold shutdown state should be reviewed in light of these findings.