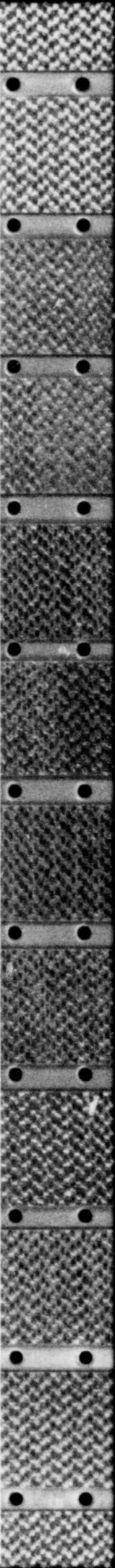
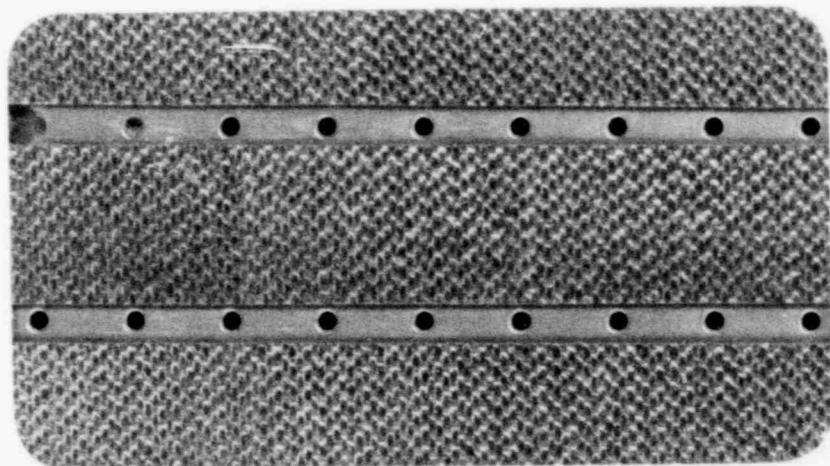
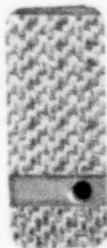


111 112 113 114 115 116 117 118 119 120 121 122 123 124 125 126 127 128 129 130 131 132 133 134 135 136 137 138 139 140 141 142 143 144 145 146 147 148 149 150 151 152 153 154 155 156 157 158 159 160 161 162 163 164 165 166 167 168 169 170 171 172 173 174 175 176 177 178 179 180 181 182 183 184 185 186 187 188 189 190 191 192 193 194 195 196 197 198 199 200



Woolmark 100% Pure New Zealand Wool



8004020432

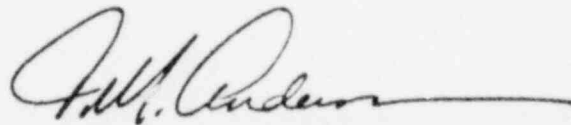
4473

WCAP-9691

NUREG-0578 2.1.9.c  
TRANSIENT AND ACCIDENT ANALYSIS

M. J. Hitchler  
D. R. Sharp  
H. V. Julian  
S. Kellman  
W. E. Shopsy  
D. C. Richardson

March, 1980



APPROVED:

T. M. Anderson, Manager  
Nuclear Safety Department

Westinghouse Electric Corporation  
P. O. Box 355  
Pittsburgh, PA 15230

8004020132

## ABSTRACT

NUREG-0578, Section 2.1.9.c outlines the scope and requirements for analysis of transient and accident scenarios, utilizing the design basis events as specified in Chapter 15 of the FSAR. The information derived from these analyses, which included the use of event trees, was used in reviewing and evaluating emergency and abnormal operating instructions and in providing input into operator training programs.

The results of the evaluation indicate that the Emergency Operating Instructions (EOIs) and the Abnormal Operating Instructions (AOIs) fully cover the current design basis events. Moreover, the EOIs address a number of events beyond the design basis. A review of the event trees and the accidents reported in the Safety Analysis Report show that when followed, the EOIs assure events that are much less severe than those reported in the SAR. As a result of this review specific recommendations concerning EOIs and their incorporation (together with event trees) into operator training programs have been made which provide added assurance that appropriate operator actions occur even during events beyond the design basis of nuclear plants.

# TABLE OF CONTENTS

	<u>Page No.</u>
1.0 INTRODUCTION AND SUMMARY	1-1
2.0 METHODOLOGY	
2.1 DEFINITION AND USE OF EVENT TREES	2-1
2.2 REVIEW STAGES	2-5
3.0 CONCLUSIONS AND RECOMMENDATIONS	
3.1 PROCEDURES	3-1
3.2 TRAINING	3-8
APPENDIX A - ANALYSIS OF LOSS OF PRIMARY AND SECONDARY COOLANT ACCIDENTS	
A.1 TRANSIENT DESCRIPTION	A-1
A.2 SYSTEM DESCRIPTION	A-8
A.3 EVENT TREE DESCRIPTION	A-26
A.4 INSTRUMENTATION DESCRIPTION	A-28
A.5 PROCEDURES REVIEW	A-34
APPENDIX B ANALYSIS OF NON-LOCA PRE-TRIP ACCIDENTS (CONTROL EVENT TREES)	
B.1 CONTROL EVENT TREE DEFINITIONS	B-1
B.2 CONTROL EVENT TREE DESCRIPTIONS	B-7
B.3 INSTRUMENTATION	B-87
APPENDIX C ANALYSIS OF NON-LOCA POST-TRIP ACCIDENTS	
C.1 TRANSIENT DESCRIPTION AND METHODOLOGY	C-1
C.2 SYSTEM DESCRIPTIONS	C-2
C.3 INSTRUMENTATION	C-10

FIGURE TITLES

<u>Figure</u>	<u>Title</u>	<u>Page</u>
2.1	Sample Event Tree	2-3
2.2	Methodology	2-7
A.1	Large LOCA Event Tree	A-39
A.2	Small LOCA Event Tree	A-45
A.3	Feedline Break Event Tree	A-57
A.4	Steamline Break Event Tree	A-67
A.5	Steam Generator Tube Rupture Event Tree - No. 1	A-79
A.6	Steam Generator Tube Rupture Event Tree - No. 2	A-93
B.2.1-1	Excessive Feedwater Event	B-13
B.2.2-1	Spectrum of Steamline Breaks	B-19
B.2.3-1	Loss of External Electrical Load/Turbine Trip	B-27
B.2.4-1	Loss of Normal Feedwater	B-35
B.2.5-1	Feedwater System Pipe Break	B-43
B.2.6-1	Loss of Forced Reactor Coolant Flow (Complete and Partial)/Locked Rotor	B-53
B.2.7-1	RCCA Bank Withdrawal at Power	B-59

FIGURE TITLES (Continued)

<u>Figure</u>	<u>Title</u>	<u>Page</u>
B.2.8-1	Startup of an Inactive Reactor Coolant Loop (SUIL)	B-67
B.2.10.1	Spectrum of Rod Cluster Control Assembly Ejection Accidents	B-75
B.2.11-1	Inadvertent Operation of ECCS	B-83
B.2.12-1	Inadvertent RCS Depressurization	B-89
C.1	Non-LOCA Post-Trip Event Tree	C-31
C.2	Secondary Feedwater System	C-33
C.3	Secondary Steam Relief	C-35
C.4	Primary Inventory and Boron Control	C-37
C.5	Pressurizer Pressure Control Systems	C-39

TABLE TITLES

<u>Table</u>	<u>Title</u>	<u>Page</u>
3.1	TMI Related Considerations	3-3
A.1	Glossary of Safety Functions	A-37
A.2	Large LOCA Systems Status	A-41
A.3	Procedures Review: Large LOCA Event Tree	A-43
A.4	Small LOCA Systems Status	A-47
A.5	Procedures Review: Small LOCA Event Tree	A-53
A.6	Feedline Break Systems Status	A-59
A.7	Procedures Review: Feedline Break Event Tree	A-63
A.8	Steamline Break Systems Status	A-69
A.9	Procedures Review: Steamline Break Event Tree	A-75
A.10	Steam Generator Tube Rupture Event Tree No. 1 - Systems Status	A-81
A.11	Procedures Review: Steam Generator Tube Rupture Event Tree - No. 1	A-89
A.12	Steam Generator Tube Rupture Event Tree No. 2 - Systems Status	A-95
A.13	Procedures Review: Steam Generator Tube Rupture Event Tree - No. 2	A-99
B.1	Control Event Tree Functions	B-3

## TABLE TITLES (Continued)

<u>Table</u>	<u>Title</u>	<u>Page</u>
B.2	Control Event Tree Transients	B-9
B.2.1-1	Decision Points for Excessive Feedwater	B-15
B.2.1-2	Functions Not Used for Excessive Feedwater Event Tree	B-15
B.2.2-1	Decision Points for a Spectrum of Main Steamline Breaks	B-21
B.2.2-2	Functions Not Used for a Spectrum of Main Steamline Breaks	B-23
B.2.3-1	Decision Points for a Loss of External Load/ Turbine Trip	B-29
B.2.4-1	Decision Points for Loss of Normal Feedwater	B-37
B.2.4-2	Functions Not Used for a Loss of Normal Feedwater	B-39
B.2.5-1	Feedwater System Pipe Break	B-45
B.2.5-2	Functions Not Used for a Feedwater System Pipe Break	B-49
B.2.6-1	Decision Points for Loss of Flow/LR	B-55
B.2.6-2	Functions Not Used in Loss of Flow/LR	B-55
B.2.7-1	Decision Points for RCCA Withdrawal at Power	B-61



TABLE TITLES (Continued)

<u>Table</u>	<u>Title</u>	<u>Page</u>
B.2.7-2	Functions Not Used for RCCA Withdrawal At Power	B-63
B.2.8-1	Decision Points for Startup of an Inactive Reactor Coolant Loop	B-69
B.2.8-2	Functions Not Used in Startup of an Inactive Reactor Coolant Loop	B-69
B.2.10-1	Decision Points for RCCA Ejection Event Tree	B-77
B.2.10-2	Functions Not Used for RCCA Ejection Event Tree	B-79
B.2.11-1	Decision Points for Inadvertent Operation of ECCS	B-85
B.2.11-2	Functions Not Used for Inadvertent Operation of ECCS	B-85
B.2.12-1	Decision Points for Inadvertent RCS Depressurization	B-91
B.2.12-2	Functions Not Used for Inadvertent RCS Depressurization	B-93
C.1	Glossary of Functions	C-11
C.2	Instrumentation Available and Qualification	C-13
C.3	Instrument Functions	C-23
C.4	Non-LOCA Failure Mechanisms	C-41

## 1.0 INTRODUCTION AND SUMMARY

NUREG-0578, Section 2.1.9.c outlines the scope and requirements for analysis of transient and accident scenarios, utilizing the design basis events as specified in Chapter 15 of the FSAR. These analyses are to be performed for the purpose of identifying appropriate and inappropriate operator actions relating to important safety considerations such as prevention of core uncover and prevention of more serious accidents. The information derived from these analyses, which may include the use of event trees, is to be used in reviewing and evaluating emergency and abnormal operating instructions and to provide input into operator training programs.

To provide a systematic, efficient way in which to respond to these requirements the event trees provided in this report have been generated. These trees identify sequences of functions called upon to operate during the transients and, consequently, the need for further analyses of sequences may be defined. They also serve as a useful vehicle to examine operator actions and to evaluate abnormal and emergency operating instructions.

The results of the evaluation indicate that the Emergency Operating Instructions (EOIs) and the Abnormal Operating Instructions (AOIs) fully cover the current design basis events. Moreover, the EOIs and AOIs address a number of events beyond the design basis. (See Appendix A and C). A review of the event trees and the accidents reported in the Safety Analysis Report show that, when followed, the EOIs and AOIs assure events that are much less severe than those reported in the SAR. As a result of this review specific recommendations concerning EOIs and AOIs and their incorporation (together with event trees) into operator training programs have been made which provide added assurance that appropriate operator actions occur even during events beyond the design basis of nuclear plants. These results, then, meet the intent of NUREG-0578, Section 2.1.9.c.

## 2.0 METHODOLOGY

### 2.1 DEFINITION AND USE OF EVENT TREES

The application of risk methodology requires the development of a large number of accident scenarios for a variety of initiating events, followed by the identification of the scenarios which are high contributors to risk. In nuclear power plant safety analyses, a typical initiating event is a significant occurrence that may take place during power plant operation which requires that the reactor be shut down. The initiating event may be a mechanical failure such as a large pipe break in the reactor coolant system or a transient event, such as a complete loss-of-load to the plant. Either type of occurrence places heavy demands on a plant operator and on operating and/or emergency safety systems. If enough safety systems were to fail and/or a plant operator were to fail to respond properly, the potential for reactor core damage, and large radioactive releases could exist. Thus, there is a need for a systematic approach to organizing the large number of potential accident scenarios and for evaluating their likelihood of occurrence. Event tree analysis provides such an approach. Event trees, once prepared, may also be used as an aid to identify critical accident sequences in reviewing plant operational procedures and can serve as a tool in designing operator training programs.

A prime example of the application of event tree methodology is presented in Appendix I of WASH-1400 (Reactor Safety Study). Some basic concepts are summarized in the paragraphs that follow.

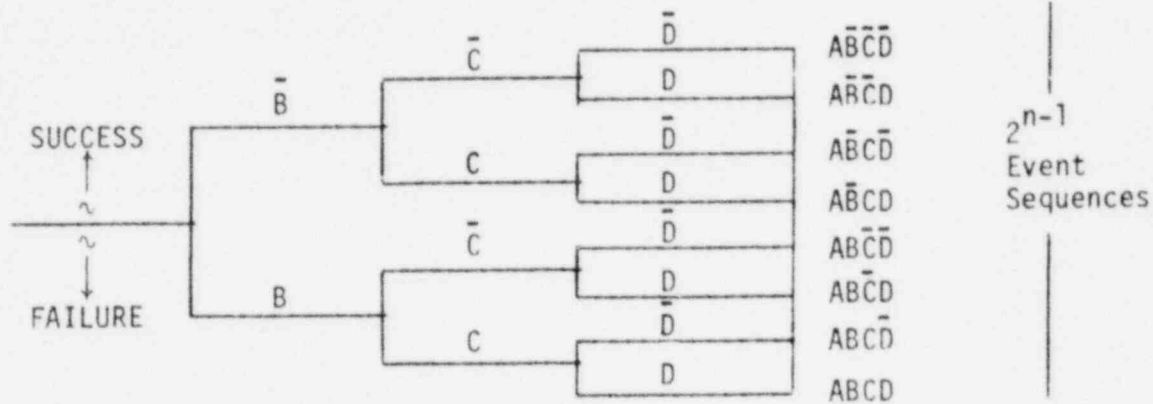
An event tree is a forward-looking (or inductive) logic diagram whose form is similar to that of decision trees used in business administration and in economics; the tree consists of an initiating event and a number of branches which connect that event to other subsequent events to produce defined sequences.

The development of an event tree for safety analysis is started by defining the various system design functions which could have an impact on meeting pre-defined safety limits. In WASH-1400 and in this study this includes such functions as electric power, reactor trip, auxiliary feedwater, and emergency core cooling. These functions are used as event headings in the tree and are initially considered in chronological order as required in the system response to the initiating event. The tree proceeds from left to right (initiating event first) by addition of branches under each heading corresponding to success or failure of the safety function in meeting its design functional requirements. Successful performance of a function is indicated by an upward drawn branch and failure by a downward drawn branch. Diagram (a) of Figure 2.1 illustrates the initial construction of an event tree. It should be noted that the tree presented is for illustrative purposes only and thus does not show all safety system functions required for a small loss-of-coolant accident (LOCA) event. After the tree is drawn, paths across it can be traced by choosing a branch under each successive heading. For example, event sequence ABCD of the basic event tree shown, indicates an accident scenario whereby a small LOCA is experienced; electrical power is provided successfully to all safety systems; there is successful trip of the reactor; and the secondary auxiliary feedwater system fails to function. Note that each sequence may really denote one or more possible sequences depending on the timing of the various failures indicated in the tree.

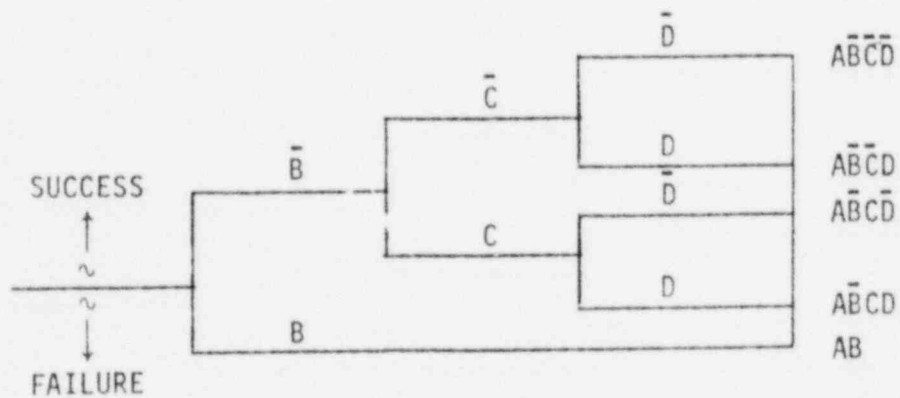
When more headings are used because of additional safety functional requirements, the number of accident sequences can become quite large (i.e.,  $2^{n-1}$  paths, where "n" is the number of individual headings). Fortunately, when functional and operational relationships between systems are considered many sequences that are illogical or meaningless are eliminated from the event tree.

n EVENTS

A	B	C	D	ACCIDENT EVENT SEQUENCE
INITIATING EVENT	SAFETY SYSTEM #1	SAFETY SYSTEM #2	SAFETY SYSTEM #3	
SMALL LOCA	ELECTRIC POWER	REACTOR TRIP	AUXILIARY FEEDWATER	



(a) Basic Event Tree



(b) Reduced Event Tree

FIGURE 2.1 Sample Event Tree

The development of an event tree is a two-step process that requires the analyst to: (1) define an initiating event and construct an initial event tree as described above, and (2) reduce the initial event tree to a final form. To perform the latter step it is necessary to

- identify the conditional dependencies in the tree and thus eliminate illogical or impossible event sequences, and
- identify timing and sequential dependencies and incorporate them in the tree; if necessary, construct additional event trees for the same initiating event with differently ordered subsequent events.

Diagram (b) of Figure 2.1 is an example of an initial basic event tree reduced by considering the above items. For example, Safety Systems #2 and #3 depend on the availability of Safety System #1, Electric Power. Since failure of electric power will lead to eventual core uncover for the sample event (a small break LOCA) regardless of the operability of reactor trip and auxiliary feedwater, branch choices for these functions need not be shown. Thus, the last four sequences may be eliminated from the basic tree, to be replaced by a single sequence AB as shown.

The event tree presented in this section was introduced to illustrate the thought processes involved in developing event trees. The actual trees presented in the appendices were drawn with many iterations, and with many interactions examined to assure completeness and adequacy. Thus, although only one tree is shown for an initiating event, a large number of trees were drawn before a final structured choice was made.

## 2.2 REVIEW STAGES

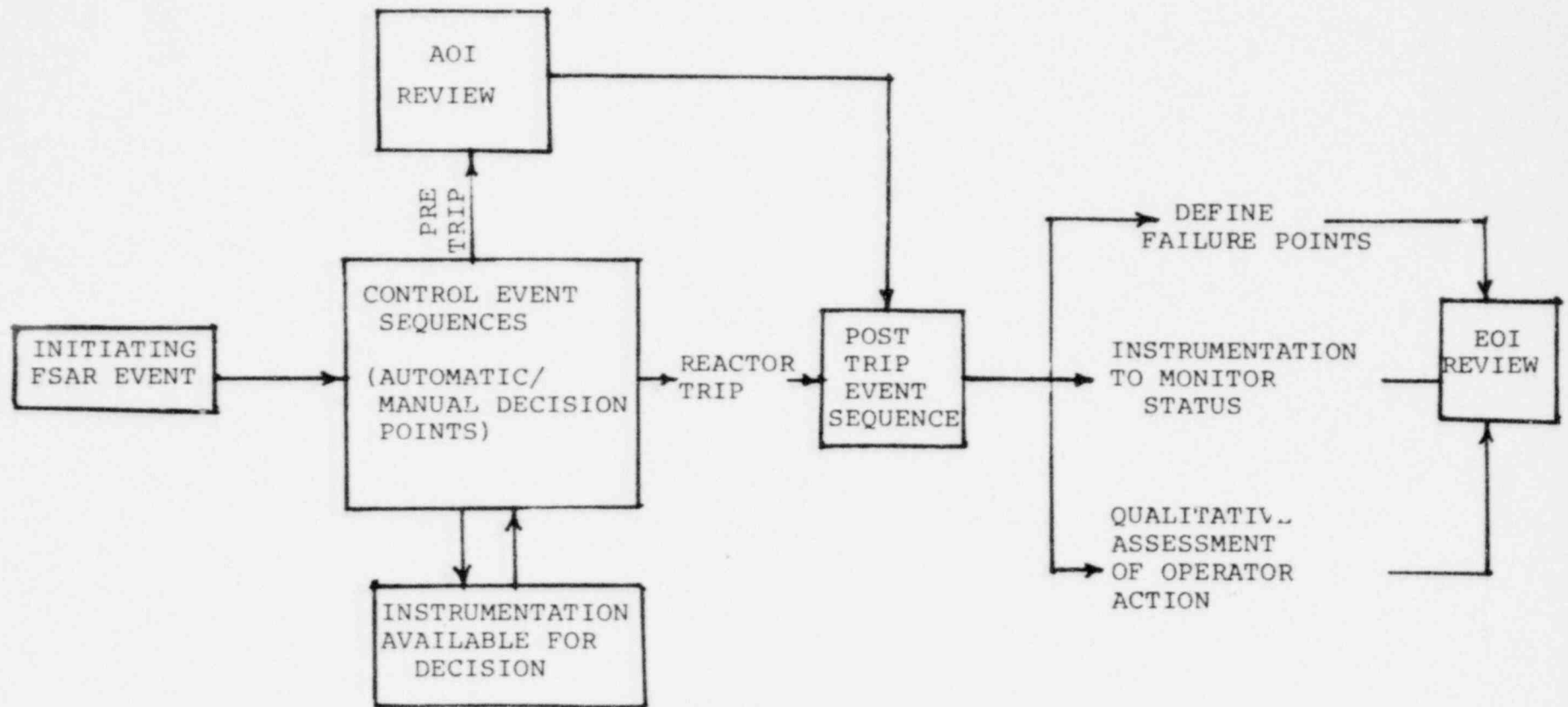
The review of transient events is divided into three segments. The first is pre-reactor trip. The pre-reactor trip segment is significant, since the operator or system response during this interval can impact

post-reactor trip conditions and how the operator would proceed to stabilize the plant; in addition, a significant aspect of the Abnormal Operating Instructions should be to assure that abnormal conditions do not evolve into emergency conditions. The second segment is post-reactor trip which is designed to study the longer term decisions the operator must make in bringing the plant to a stabilized shutdown condition; this section focuses on post-trip conditions which initially do not involve a loss of primary or secondary system coolant; it emphasizes diagnosis of current plant status (trends) and what types of failures could occur if these trends continued without operator corrective action. The third segment of the review is for loss of primary or secondary coolant accidents.

Figure 2.2 shows a block diagram of the process used in assessing operator actions. The FSAR accidents were used to define the types of events studied. Control event sequences were developed for FSAR accidents which show alternate paths the accidents may follow using FSAR and non-FSAR assumptions for severity of failures and equipment responses. Most of these event sequences were developed for the time frames normally studied in the FSAR (i.e., up to and immediately following time of reactor trip or safety injection). The intent is to show the control system interactions which could significantly affect the accident (i.e., increase the severity or transform the accident into an alternate unexpected event). The Control Event Trees were then used for a general review of the plant Abnormal Operating Instructions (AOIs). The review was made to assess the operator's ability to diagnose the transient and the appropriateness of corrective actions.

Reactor trip event trees were developed for non-LOCA and Loss of Primary Secondary Coolant Accident sequences. The non-LOCA emphasis was placed on paths which could ultimately lead to a LOCA, loss of secondary coolant or core uncover if correct operator action were not performed. Instrumentation available to the operator to assess plant status and safety equipment operation has been identified for each safety function. The event trees and instrumentation were then reviewed with respect to the abnormal and emergency operating instructions to assure that adequate guidance was provided.

Figure 2.2  
METHODOLOGY



2-7



### 3.0 CONCLUSIONS AND RECOMMENDATIONS

As a result of the evaluation of the event trees, transient events, and various analyses with respect to emergency and abnormal operating instructions (EOIs and AOIs), the following conclusions and recommendations are provided with respect to current EOIs, AOIs and operator training.

#### 3.1 PROCEDURES

The results of the evaluation indicate that the EOIs and AOIs fully cover the current design basis events. A review of the event trees and of the accidents which lead to safety injection results in the conclusion that the EOIs and AOIs provide complete coverage and, in fact, when followed will result in much less severe events than those reported in the SAR. In addition, the event trees presented in Appendices A and C incorporate accident scenarios which are beyond the current design bases. It should be noted that many of these sequences incorporate multiple failures within a system which result in more than one total loss of function. Despite this, the EOIs and AOIs in most instances provide guidance to restore or to augment critical functions in order to mitigate these events or to bring them back within the design basis.

The EOIs incorporate many lessons learned from TMI. Examples of these considerations and how they relate to the amount of coverage identified in Appendix A are given in Table 3.1. As discussed, Tables A.3, A.5, A.7, A.9, A.11, and A.13 summarize how event tree sequences are covered in the instruction guidelines.

In addition other plant operating experiences have been incorporated into the EOIs and AOIs. Westinghouse has evaluated recent events, including the North Anna transient (stuck open steam dump valve), and the Prairie Island steam generator tube rupture and has made additional changes to the instruction guidelines. An example of a change made to the guidelines based on operating experience is the modification of E-3 Step 9 to include an instruction to close the supply valve in the steamline to the auxiliary feedwater pump associated with the faulted steam generator.

TABLE 3.1

TMI RELATED CONSIDERATIONS

<u>Consideration</u>	<u>Where Consideration Incorporated</u>	
	<u>Instruction</u>	<u>Step</u>
1. Improved diagnostics	E-0	D
2. Possibility of misdiagnosing events	E-0	D.5
	E-1	C.1, C.3.G Caution, C.3.J Caution
	E-2	C.3, C.4, C.6
	E-3	C.11
3. Criteria for Emergency Coolant Injection (ECI) termination/continuation	E-0	D.7, C.2, C.3, D.7
	E-1	C.1, C.3, C.4, C.7, C.9, C.10 C.11, C.12, Tables
	E-2	C.1, C.5, C.6, C.10, Table E-2.1
	E-3	C.7, C.13, C.14
4. RCP trip criteria	E-0	D.2
	E-1	C.5
	E-2	C.2
	E-3	C.2, C.11, C.17
5. Instructions on instrumentation	E-0	Notes
	E-1	Notes
	E-2	Notes
	E-3	Notes
6. Auxiliary feedwater flow verification	E-0	C.2, C.3
	E-1	C.1, C.2
	E-2	C.4
	E-3	C.6
7. Containment Isolation verification/maintenance	E-0	C.2, C.5
	E-1	C.3
	E-2	C.1
	E-3	C.4

TABLE 3.1 (Continued)

TMI RELATED CONSIDERATIONS

<u>Consideration</u>	<u>Where Consideration Incorporated</u>	
	<u>Instruction</u>	<u>Step</u>
8. PORV status verification	E-0 E-1 E-3	D.1 C.2 C.1, C.13
9. Pressurizer Relief Tank (PRT) integrity maintenance	E-3	C.12
10. Multiple Events/Hierarchy of Procedures	E-0 E-1 E-2 E-3	D.3 thru D.7 C.1, C.3 C.3, C.4, C.6 C.11, C.13
11. Resetting SI	E-0 E-1 E-2 E-3	D.7 C.3, C.4 C.1, C.6 C.7
12. Subcooling criteria	E-0 E-1 E-2 E-3	D.7 C.3 C.6 C.10, C.13, C.15
13. Pressurizer steam space breaks	E-0 E-1 E-3	D.1, D.7 C.2, C.3 C.1, C.13, C.20
14. Use of pressurizer heaters	E-0 E-1 E-2 E-3	D.7 C.3 C.6 C.16
15. Restarting of RCP	E-2 E-3	C.9 C.17
16. Use of multiple parameters	E-0 E-1 E-2 E-3	Throughout the instructions Throughout the instructions Throughout the instructions Throughout the instructions

Some events which are not addressed in the instruction guidelines do not require coverage because their likelihood of occurrence is extremely small. Two examples are the loss of all secondary steam relief capability via the failure to open of any steam dump, relief or safety valves, and the loss of primary relief capability via failure to open of any pressurizer relief or safety valves.

Some specific revisions or improvements to the guidelines are recommended as a result of the review.

- A number of the non-design basis event tree paths may lead to Inadequate Core Cooling (ICC) scenarios due to complete loss of safety function (e.g., total loss of total auxiliary feedwater). Activities in this area are continuing under separate review; therefore no specific recommendations have been made as part of this study. However, the paths identified in this study should be utilized as an input to this activity.
- In the case of multiple events, the structure of the guidelines should permit the operator to detect the multiple events and to direct him to the procedure for the most critical event. For example, a secondary high energy line break at power (Procedure E-2) can potentially result in water relief from the pressurizer PORVs. The guidelines should caution the operator that relief can occur in this situation due to the resultant system heatup, and if it does, to verify PORV reclosure after the pressure falls below the set-point. If the valves do not reclose, the guidelines should direct the operator to go immediately to E-1.
- In the steam generator tube rupture event (Procedure E-3), two cautions should be added to the guidelines. If isolation of the faulted steam generator is not achieved, the operator should be cautioned that he will be unable to meet the subcooling criteria for the non-faulted loops for safety injection termination; in this instance the operator should be instructed to base his decision for

safety injection termination on pressurizer level and RCS pressure, paying close attention to containment parameters and PORV status; he should subsequently obtain the required subcooling when the steam generator can be isolated. If the steam line isolation valve to the faulted steam generator cannot be closed, the operator should be cautioned to close the steamline isolation valves to the other steam generators in order to isolate the affected steam generator. Steam relief can then proceed from the intact steam generators using the atmospheric steam dump valves without resulting in release of radioactive steam.

In conclusion, the EOIs and AOIs have been reviewed with respect to the event tree sequences developed for the various transients and the degree of coverage for these sequences delineated. Specific recommendations for additions to the EOIs and AOIs have been identified. Therefore, the intent of NUREG-0578 Section 2.1.9.c has been met.

### 3.2 TRAINING

The EOIs have been used as the basis for extensive training of operating plant personnel. At week-long seminars, the EOIs were discussed on a step-by-step basis, along with background information which provided the basis for the EOIs and included the systems design and better estimate analyses. This permitted a more effective adaptation of the EOIs into plant specific procedures. Additional plant specific training on the plant procedures was provided to plant operators. Current design basis events are fully covered by the training programs utilizing the EOIs, plant procedures and simulators.

In addition, these event trees can be beneficial in augmenting operator training for events beyond the current design basis. Specific training can be aimed at significant event paths. Certain of the branches of several event trees lend themselves to evaluation and training on simulators. The event trees can be applied to the training which will be conducted in connection with Inadequate Core Cooling activities.

## APPENDIX A

### ANALYSIS OF LOSS OF PRIMARY AND SECONDARY COOLANT ACCIDENTS

#### A.1 TRANSIENT DESCRIPTION

This section presents the event trees relating to loss of primary and secondary coolant accidents for a 4-loop, RESAR-3 type pressurized water reactor. The analysis, in terms of potential safety function failure, is applicable to all plants; differences from RESAR 3 will exist in the definition of plant systems and system failure, and perhaps in some individual statements made in table footnotes about event trends and possible operator actions; these differences, however, will not alter the recommendations and conclusions resulting from this review.

A loss of primary coolant accident (LOCA) is defined as a rupture of a pipe in the reactor coolant system (RCS) of a size whereby the normally operating charging system flow is not sufficient to maintain pressurizer water level and pressure within desired operating limits. In general, emergency core cooling systems (ECCS) are designed to cover two main categories of breaks in the RCS, large and small. The large break covers sizes that range from the equivalent of a ten-inch diameter hole size to the double-ended guillotine rupture of the largest pipe in the RCS. A small break covers sizes of one-half inch to ten inches equivalent diameter holes in the RCS. Treated separately is steam generator tube rupture (SGTR) accident, a small break discharging to the secondary system rather than to the containment.

A loss of secondary coolant accident can be separated into two types of events, feedline and steamline breaks. A feedline break is defined as a rupture of a pipe in the feedwater system of a size whereby the normal feedwater system flow is not sufficient to maintain steam generator

water level. A steamline break is defined as a rupture of a pipe in the steam system or the failure to reclose of steam dump, steam generator safety or relief valves.

#### A.1.1 LARGE BREAK LOCA TRANSIENT

Before the large break occurs, the unit is assumed to be in an equilibrium condition, i.e., the heat generated in the core is being removed via the secondary system. At the beginning of the blowdown phase, the entire RCS contains subcooled liquid which transfers heat from the core by forced convection with some fully developed nucleate boiling. Thereafter, the core heat transfer is based on local conditions with transition boiling and forced convection to steam as the major heat transfer mechanisms.

The heat transfer between the RCS and the secondary system may be in either direction, depending on the relative temperatures. In the case of heat removal from the primary side, secondary system pressure increases, and the main steam safety valves may actuate to limit the pressure. Makeup water to the secondary side is automatically provided by the auxiliary feedwater system. The safety injection signal actuates a feedwater isolation signal which isolates normal feedwater flow by closing the main feedwater isolation valves and also initiates emergency feedwater flow by starting the auxiliary feedwater pumps. The secondary flow aids in the reduction in RCS pressure. When the RCS depressurizes to 600 psia, the accumulators begin to inject borated water into the reactor coolant cold legs. If loss of offsite power is assumed, the reactor coolant pumps are tripped at the inception of the accident. The effects of pump coastdown are included in the blowdown analysis.

The large break LOCA has four characteristic stages: blowdown, refill, reflood and long-term recirculation. The blowdown phase of the transient ends when the RCS pressure (initially assumed at 2250 psia) falls to a value approaching that of the containment atmosphere. At the time

that bypass of emergency core cooling water ends, refill of the reactor vessel lower plenum begins. Refill is complete when emergency core cooling water has filled the lower plenum of the reactor vessel.

The reflood phase of the transient is defined as the time period lasting from the end-of-refill until the reactor vessel has been filled with water to the extent that the core temperature rise has been terminated. From the later stage of blowdown through the beginning of reflood, the accumulator tanks rapidly discharge borated cooling water into the RCS, contributing to the filling of the reactor vessel downcomer. The downcomer water elevation head provides the driving force required for the reflooding of the reactor core. The low head and high head safety injection pumps aid in the filling of the downcomer and, subsequently, supply water to maintain a full downcomer and complete the reflooding process.

Continued operation of the ECCS pumps supplies water during long-term cooling. Core temperatures have been reduced to long-term steady state levels associated with the dissipation of residual heat generation. After the water level of the refueling water storage tank reaches a minimum allowable value, coolant for long-term cooling of the core is obtained by switching to the cold leg recirculation phase of operation in which spilled borated water is drawn from the containment sump by the low head safety injection (residual heat removal) pumps and returned to the RCS cold legs. Approximately 24 hours after initiation of the LOCA, the ECCS is realigned to supply water to the RCS hot legs in order to control the boric acid concentration in the reactor vessel.

#### A.1.2 SMALL BREAK LOCA TRANSIENT

As contrasted with the large break, the blowdown phase of the small break occurs over a longer time period. Thus, for a small-break LOCA there are only three characteristic stages, i.e., a gradual blowdown in which the decrease in water level is checked, core recovery, and long-term recirculation.



Unlike the large break in which all decay heat may be removed by the break, small breaks depend on the steam generator for heat removal early in the transient for break sizes in the range 1/2 to 2 inches equivalent diameter. Therefore, small breaks may be subdivided into two groups, i.e., 1/2 to 2 and 2 to 10 inch equivalent diameter hole size. The grouping reflects the differences in demand imposed by break size on the equipment that has to operate to provide core cooling. An event tree for small breaks in the range of 2 to 10 inch equivalent diameter hole size would be similar to that shown in Figure A.1 for the large break; that is, since decay heat is removed by the break, the secondary system is not relied upon for long term heat removal. (See WCAP-9600, Section 3.2 for a discussion of limiting breaks.) However, the large LOCA tree does not incorporate a branch point for reactor trip (RPS function), which is required to mitigate the accident for smaller breaks in the 2 to 10 inch range. The RPS branch point is included in the event tree for the 1/2 to 2 inch range; but that tree considers (conservatively) equipment requirements that are unnecessary for the 2 to 10 inch range. Therefore, for the purposes of this study, since the 2 to 10 inch range of break sizes is covered by sequences in both event trees, only two LOCA event trees will be discussed, one for large LOCA and one for small LOCA in the 1/2 to 2 inch equivalent diameter range.

### A.1.3 FEEDLINE BREAK TRANSIENT

For this section feedline rupture is defined as a break in a feedwater pipe large enough to prevent the addition of sufficient feedwater to the steam generators to maintain shell-side fluid inventory in the steam generators. For pipe breaks smaller than this size see Appendix B Section B.2.5.

Due to the continued reverse blowdown of the ruptured steam generator, the heat removal capability of the steam generators exceeds the heat generation by decay of fission products in the core. The secondary and primary temperatures continue to decrease from the time of reactor trip until the low steamline pressure setpoint is reached, at which time all

main steamline isolation valves close and safety injection flow to the primary system is initiated. At that time the reverse steam blowdown through the ruptured steam generator ceases and the pressure in the intact steam generators increases until the steam generator safety valves open. Due to the loss of heat sink and a smaller delta temperature from primary to secondary, less heat transfer from primary to secondary exists and the primary temperatures again begin to increase.

The transient is turned around when the auxiliary feedwater supply is adequate to remove the decay heat generated in the core.

#### A.1.4 STEAMLINE BREAK TRANSIENT

Excessive steam releases from the secondary system cause an increase in the heat extraction rate from the reactor coolant system, resulting in a reduction of primary system temperature and pressure and reduction in RCS volume. Through control systems or through the inherent load following nature of an undermoderated PWR, core power will increase in an effort to equalize the thermal load caused by the steam leak. See Appendix B Section B.3.2 for a discussion of control functions.

Breaks of various sizes at different locations may be postulated to occur in the main steam system which cause an increase in steam load. The incremental steam load would cause a rapid primary and secondary depressurization and cooldown. If the plant is at full power, a power increase could result due to the cooldown in the presence of a large negative temperature coefficient of reactivity (end of life); the reactor is tripped on overpower signals or on low steamline pressure. If the plant is at hot shutdown, sufficient cooldown could occur to allow a return to criticality.

A second type of steamline break would be a failed open steam dump, steam generator safety or relief valve. Because this "break" is small,

plant control systems may be capable of maintaining pressurizer pressure, pressurizer level, steam generator level and reactor power below protection system setpoints, establishing a new steady state condition. This case is considered as an initiating event in this study and also as a consequential (additional) failure.

#### A.1.5 STEAM GENERATOR TUBE RUPTURE TRANSIENT

The accident examined is the rupture of a steam generator tube(s), creating a maximum break area equal to that of the complete severance of a single tube. The transient is assumed to take place at power, at which time the reactor coolant is contaminated with fission products corresponding to continuous operation with a limited amount of defective fuel rods. The accident leads to an increase in the contamination of the secondary system due to the leakage of radioactive coolant from the RCS. In the event of a coincident loss of offsite power or failure of the steam dump system, discharge of activity to the atmosphere takes place via the steam generator safety and/or power-operated relief valves.

If normal operation of the various plant control systems is assumed, the following sequence of events is initiated by a tube rupture:

- a. Pressurizer low pressure and low level alarms are actuated and charging pump flow increases in an attempt to maintain pressurizer level. On the secondary side, there is a steam flow/feedwater flow mismatch before trip as feedwater flow to the affected steam generator is reduced due to the additional break flow to that unit.
- b. Continued loss of reactor coolant inventory leads to a reactor trip signal generated by low pressurizer pressure, followed by a safety injection signal. Plant cooldown following reactor trip leads to a rapid change in pressurizer level. The safety injection signal automatically terminates normal feedwater supply and initiates auxiliary feedwater addition.

- c. The steam generator blowdown radiation monitor and/or the condenser air ejector radiation monitor will alarm, indicating a sharp increase in radioactivity in the secondary system, and will automatically isolate steam generator blowdown.
- d. The reactor trip automatically trips the turbine; if offsite power is available the steam dump valves open, permitting steam dump to the condenser. In the event of a coincident station blackout, the steam dump valves would automatically close to protect the condenser; steam generator pressure would rapidly increase, resulting in steam discharge to the atmosphere through the steam generator safety and/or power-operated relief valves.

Without operator intervention, the RCS would eventually stabilize at a pressure at which safety injection flow would match break flow through the rupture. However, the operator is expected to determine that a steam generator tube rupture (SGTR) has occurred, and to identify and isolate the faulted steam generator before starting the cooldown by use of the non-faulted steam generators. The cooldown to 50°F below no-load temperature begins by dumping steam from the non-faulted steam generators to the condenser if offsite power is available, or by opening the steam generator atmospheric relief valves if offsite power is not available. Once the primary temperature is reduced to 50°F below no-load, the primary pressure can be reduced by use of the normal pressurizer spray system, or by pressure relief through one pressurizer PORV if normal spray is not available. When the reactor coolant pressure falls to that of the faulted steam generator, the depressurization process via spray is terminated or the PORV is closed. The primary pressure is then allowed to increase 200 psi, and when the pressurizer water level is greater than 20 percent of span, the SIS is manually turned off.

The normal charging and letdown systems are established to maintain a water level at 20 percent of span. Normal pressurizer spray (if an RCP

is in service) is used to decrease the reactor coolant pressure below that of the faulted steam generator thus terminating the leak flow; otherwise use is made of auxiliary spray or brief intermittent opening of one PORV. The faulted steam generator is slowly depressurized by opening an atmospheric relief valve or the bypass valve to the condenser (if the condenser is available). Continuation of the cooldown and depressurization of the RCS and the faulted steam generator is accomplished by minimizing leak flow until the residual heat removal system (RHRS) can be put into operation (350°F, 400 psia). Once the RHRS is in operation and RCS hot leg temperature is reduced below 200°F, the pressure is reduced with the auxiliary spray until the RCS and the faulted steam generator pressures have equilibrated.

## A.2 SYSTEMS DESCRIPTION

The systems required to mitigate the consequences of a break in the RCS or secondary system pressure boundary, defined as core uncover for the purposes of this study, are shown in the event trees of Figures A.1-A.6. For the purpose of tree construction, the assumption has been made that containment heat removal systems do not have significant impact on emergency coolant availability and on progress/trends of the transient; therefore, these systems do not appear in the event trees. A brief description of each system pertinent to the event trees is presented in the paragraphs that follow.

### A.2.1 ELECTRIC POWER (EP)

The Electrical Power system provides a reliable source of power to all plant auxiliaries required during any normal or emergency mode of plant operation. The design of the system is such that sufficient independence or isolation between the various sources of electrical power is provided to guard against concurrent loss of all auxiliary power. Independence and isolation of supply to the various redundant engineered

safeguards features is maintained so a single bus fault will not result in the loss of all the plant engineered safeguards features systems (ESFs).

The Electrical Power system is designed to provide a simple arrangement of buses, requiring a minimum of switching to restore power to a bus in the event that the normal power supply to it is lost. The off-site AC network and on-site AC diesel generators, together with DC system for vital instrumentation and control, comprise the principal components of the Electric Power system.

Because operability of the ESFs and associated instrumentation depend on the availability of electric power, the event trees are structured to show EP, availability of AC power to the buses that furnish power to the ESFs, as the first event of interest after the initiating event. The structure of the event tree for subsequent events reflects the dependence of other ESFs on electric power. Thus, when electric power fails, further choices are omitted so as to imply failure.

#### A.2.2 REACTOR PROTECTION SYSTEM (RPS)

The solid state Reactor Protection System is designed to protect the integrity of the primary system and its components, to the following criteria:

- high functional reliability
- capability to undergo in-service testing and calibration
- sufficient redundancy to assure that no single failure will disable its protective features

- failure into a safe condition
- additional passive failure must be assumed if an unsafe condition can be caused by an active channel (control) failure, when channels are used for both control and protection

The system automatically trips the plant, by gravity insertion of control rods into the core, whenever plant conditions monitored by nuclear and/or process instrumentation reach specified limits. The system also provides alarms that alert the plant operator when manual action is required to prevent a plant trip. The Reactor Protection System includes the following trip functions:

- overtemperature  $\Delta T$
- overpower  $\Delta T$
- high/low pressurizer pressure
- high pressurizer level
- reactor coolant system low flow
- nuclear instrumentation high flux
- turbine trip
- manual trip
- safety injection trip
- low-low steam generator level

Note that, except for the undervoltage and fault trips associated with the reactor coolant pump breakers, all circuits are redundant.

Safety injection actuation provides the output signal and logic used to initiate emergency diesel startup, feedwater isolation, startup of auxiliary feedwater pumps, startup of emergency containment fan coolers, startup of essential service water pumps and service water isolation, and other selected safeguards functions. ESF actuation signals provided by the protection system include:

- low pressurizer pressure
- low steamline pressure
- high containment pressure
- manual signal

For the event trees, failure of the RPS is conservatively defined to be the failure of more than two full length control rod assemblies to insert into the core. The failure of the required control rod assemblies to insert may be caused by electrical faults in the signals or equipment required to release the rods into the core, or by mechanical faults that cause a hangup of more than two full-length control rod assemblies.

### A.2.3 AUXILIARY FEEDWATER SYSTEM (AFWS)

The Auxiliary Feedwater System serves as a backup system for supplying adequate cooling water to the steam generators at times when main feedwater is not available in the event of a plant trip coupled with a loss of offsite power. The AFWS consists of two motor-driven pumps and a single turbine-driven pump. One of the two motor-driven auxiliary feedwater pumps supplying two of the four steam generators will provide enough feedwater to safely cool the unit down to 350 °F/400 psig at which time the Residual Heat Removal System can be utilized. The single turbine-driven auxiliary feedwater pump has twice the capacity of either motor-driven pump and can supply all four steam generators.

The pumps normally deliver water from the condensate storage tank (CST). The capacity of the CST allows the plant to remain at hot standby for 4 hours and then cool down the primary system at an average rate of 50 °F/hour to a temperature of 350 °F. Two redundant safety-related back-up sources of water from the essential service water system are provided for the pumps.

Sufficient redundancy is provided throughout the auxiliary feed and supporting systems to ensure the required flow to the minimum number of loops while subjected to a single active failure in the short term, or a



single active or passive failure in the long term. Diversity and physical separation of parallel power supplies, water sources, feedwater routes, and controls are provided to cover the many conditions which can cause a loss of normal feedwater or partial loss of auxiliary feedwater. Sufficient remote and local controls, and remote indication of the system state, are provided to allow supervision and manual control from both the control room and local to the auxiliary feed pumps.

For the development of the event trees, auxiliary feedwater delivery failure is considered to be less than full delivery from one of the two electric-driven feedwater pumps or the equivalent flow from the steam-driven auxiliary feedwater pump. The period of demand and operation for the SSR and AFWS are about 1 day for the small LOCA event.

#### A.2.4 MAIN STEAM ISOLATION (MSI)

One main steam isolation valve (MSIV) and associated bypass isolation valve (BIV) is installed in each of the four main steam lines outside the containment and downstream of the safety valves. The MSIVs are installed to prevent uncontrolled blowdown from more than one steam generator. The valves isolate the nonsafety-related portions from the safety-related portions of the system. For emergency closure of either of the two solenoids, provided for the two separate pneumatic/hydraulic power trains and energized from separate Class IE sources, will result in valve closure. The valves are designed to close in 1.5 to 5 seconds against the flows associated with line breaks on either side of the valve, assuming the most limiting normal operating conditions prior to occurrence of the break.

The main steam BIV is used when the MSIVs are closed to permit warming of the main steam lines prior to startup. The bypass valves are air-operated globe valves. For emergency closure, either of two separate solenoids, when de-energized, will result in valve closure; the solenoids are energized from a separate Class IE source.

For the event trees, failure of the MSI function is defined as failure of the MSIV and/or BIV to isolate the main steam line to the faulted generator, or failure to terminate auxiliary feedwater to that steam generator.

#### A.2.5 SECONDARY STEAM RELIEF (SSR)

The SSR system bypasses steam from the turbine-generator to the main condenser or releases steam to the atmosphere (if condenser is not available) in order to minimize transient effects on the RCS during startup, hot shutdown, cooldown, and accident conditions of the plant. SSR consists of three subsystems or functions: steam dump to the condenser, power-operated relief valves, and safety valves located on each main steam line.

##### A. Steam Dump to the Condenser (SDC)

The steam dump system has the capacity to bypass 40% of the main steam to the condenser at full load steam pressure. It will permit a 50% electrical step-load reduction from full power without reactor trip or lifting of the main steam relief and safety valves. Conditions permitting heat to be removed via this system require that the MSIVs be open and that the condenser vacuum be maintained within acceptable limits by (1) operability of the condenser air ejector system; and (2) operability of the circulating water system for condenser cooling. The system is composed of a manifold connected to the main steam lines upstream of the turbine stop valves and lines from the manifold with regulating (dump) valves to each condenser shell. There are 12 dump valves that are air-actuated, pilot-operated, spring-opposed, and fail closed upon loss of air or loss of power to their control system. Hand switches in the main control room are provided for selection of either system operating mode, automatic or manual. Pressure controllers and valve position lights associated with the steam dump system are also located in the main control room.

## B. Main Steam Safety and Relief Valves (S/R)

There are four power-operated atmospheric relief valves in the main steam system, one installed in the outlet piping of each steam generator. The valves are provided for controlled removal of reactor decay heat when the main steam isolation valves are closed or when the steam dump system is not available. The valves will pass sufficient flow at all pressures to achieve a 500°F per hour plant cooldown rate to at least 350°F. The total capacity of the four valves is 15% of rated main steam flow at steam generator no load pressure. The maximum actual capacity of each relief valve at design pressure is limited to reduce the magnitude of a reactor transient if one valve would inadvertently open and remain open. The relief valves, ANS Safety Class 2 type components, are air-operated, supplied by a safety-grade air supply and controlled from Class IE sources. A non-safety grade air supply is available during normal operating conditions. The capability for remote manual valve operation is provided in the main control room and at the plant auxiliary shutdown panel.

There are five safety valves installed in each main steam line. The spring-loaded safety valves provide over-pressure protection in accordance with the ASME Section III code requirements for the secondary side of the steam generators and the main steam piping. The valves discharge directly to the atmosphere via vent stacks. The set pressure of each valve within a steam loop varies (values of 1185, 1197, 1210, 1222, and 1234 psig) along with its discharge capacity. The maximum actual capacity of the safety valves at their design pressure is limited to reduce the magnitude of a reactor transient if one of the valves would open and remain open. The valves are designed and constructed to meet seismic Category I requirements and are ANS Safety Class 2 type components.

In the event trees, SSR column heading SDC represents operation of the valves dumping steam to the condenser. After completion of the first three trees, it was noted that the valves could fail to open or fail to reclose as discussed next for relief and safety valves. Thereafter, the dump valve function was included in the safety/relief valve function in order to simplify the event trees. SSR column heading S/R-V0 represents the opening of the steam generator safety and/or relief valves during significant heat up of the secondary system. Failure of this function corresponds to failure to operate of all safety and power-operated relief valves. Note that operation of one or more safety or relief valves constitutes success. Column heading S/R-VR represents the re-closing of all these valves which is necessary to prevent excessive cooldown of the primary system.

#### A.2.6 PRIMARY PRESSURE CONTROL (PPC)

The pressurizer functions as the Primary Pressure Control system to maintain RCS pressure at desired limits during steady-state reactor operation and limits pressure changes during transients. Electric immersion heaters, and a spray nozzle are located in the pressurizer. Safety/relief valves discharge to a pressurizer relief tank.

##### A. Pressurizer Normal Spray, Heaters and Auxiliary Spray

During an outsurge of water from the pressurizer, flashing of water to steam and generation of steam by automatic actuation of the heaters keeps the pressure above a minimum allowable limit. During an insurge from the RCS, the spray system, which is fed from two cold legs, condenses steam to prevent the pressurizer pressure from reaching the setpoint of the power-operated relief valves during normal design transients. Heaters are energized on high water level during insurge to heat the subcooled water that enters the pressurizer from the reactor coolant loop.

Two separate, automatically controlled spray valves with remote manual overrides are used to initiate pressurizer spray. In parallel with each spray valve is a manual throttle valve which permits a small continuous flow through both spray lines to reduce thermal stresses and helps to maintain uniform water chemistry and temperature in the pressurizer. Temperature sensors with alarms are provided in each spray line to alert the operator to insufficient bypass flow. The spray rate is selected to prevent the pressurizer pressure from reaching the relief valve setpoint during a step reduction in power level of 10 percent of full load.

The pressurizer spray lines and valves are large enough to provide the required spray flow rate under the driving force of the differential pressure between the surge line connection in the hot leg and the spray line connection in the cold leg. The spray line inlet connections extend into the cold leg piping in the form of a scoop in order to utilize the velocity head of the reactor coolant loop flow to add to the spray driving force. The spray valves and line connections are arranged so that the spray will operate when only one reactor coolant pump is operating in one of the two cold legs connected to the spray system.

A flow path from the CVCS to the pressurizer spray line is also provided. This path provides auxiliary spray to the vapor space of the pressurizer during cooldown when the reactor coolant pumps are not operating. The thermal sleeves on the pressurizer spray connection and the spray piping are designed to withstand the thermal stresses resulting from the introduction of cold spray water.

#### B. Pressurizer Safety/Relief Valves

Three spring-loaded safety valves and two power-operated relief valves provide for overpressure protection and control. The ASME-code safety valves, 2.5 in. diameter, are set for the system design pressure of 2485 psig. The combined capacity of the valves is equal

to, or greater than, the maximum surge rate resulting from complete loss of load without reactor trip or any other control except that the secondary plant safety valves are assumed to operate when steam pressure reaches their setpoint. A resistance temperature detector is installed in the discharge piping of each safety valve in order to provide indication and a high temperature alarm in the control room to warn the operator of an actuated or leaky safety valve.

The two power-operated relief valves are set to open at 2335 psig. Their opening, 1.3 in. diameter, is actuated on signals generated by the pressurizer pressure transmitters. A resistance temperature detector, installed in the discharge line common to both valves, serves the same purpose as those for the safety valves. The power-operated relief valves are provided to limit any pressure excursion and thus limit the operation of the spring loaded pressurizer safety valves. Motor-operated stop valves, located ahead of the power-operated relief valves, are provided in order to remove those valves from service should they leak excessively. This is allowable since the safety valves are sized to protect the reactor coolant system without the aid of the power-operated relief valves.

In the event trees, the PPC column heading SPRAY represents the functioning of the normal and auxiliary spray systems within the pressurizer during RCS depressurization and cooldown to cold shutdown conditions. Failure of this function is defined as failure to deliver spray flow from reactor coolant loop cold legs or from the CVCS.

PPC column heading S/R-VO represents the opening of the pressurizer safety and/or relief valves during significant heatup of the primary system. Failure of this function corresponds to failure to operate of all safety and relief valves. Note that operation of one or more safety or relief valves constitutes success. Column heading S/R-VR represents the closing of all these valves which is necessary to prevent excessive discharge of coolant from the primary system.

### A.2.7 CHEMICAL AND VOLUME CONTROL SYSTEM (CVCS)

The basic functions of the Chemical and Volume Control System (CVCS) are to:

- a. Maintain programmed water level in the pressurizer.
- b. Maintain seal-water injection flow to the reactor coolant pumps.
- c. Control reactor coolant water chemistry conditions, activity level, soluble chemical absorber concentration and makeup.
- d. Provide means of filling, draining, and pressure testing of the RCS.
- e. Provide injection flow to the RCS following actuation of the Safety Injection System.

The charging and letdown functions of the CVCS are employed to maintain a programmed water level in the pressurizer, thus maintaining a proper reactor coolant inventory during all phases of plant operation. This is achieved by means of a continuous feed-and-bleed process during which the feed rate is automatically controlled, based on the pressurizer water level.

Reactor coolant is let down to the CVCS from a reactor coolant loop cross-over leg. It then flows through the shell side of the regenerative heat exchanger where its temperature is reduced by heat transfer to the charging flow passing through the tubes. The coolant then experiences a large pressure reduction as it passes through a letdown orifice and flows through the tube side of the letdown heat exchanger where its temperature is further reduced. Downstream of the letdown heat exchanger, a second pressure reduction is performed by the low pressure letdown valve, which maintains upstream pressure and thus prevents flashing downstream of the letdown orifices. The coolant then flows

through one of the mixed bed demineralizers and may pass through the cation bed demineralizer for further purification, through the reactor coolant filter and into the volume control tank (VCT) through a spray nozzle in the top of the tank.

An alternate letdown path is provided which allows part or all of the letdown flow to pass through the Boron Thermal Regeneration System (BTRS) when boron concentration changes are desired to follow plant load. The alternate letdown flow path is directed to the BTRS downstream of the mixed bed demineralizers. After processing by the BTRS, the flow is returned to the CVCS at a point upstream of the reactor coolant filter.

Three charging pumps (one positive displacement pump and two centrifugal charging pumps) are provided to take suction from the VCT and return the purified reactor coolant to the RCS. Normal charging flow is handled by a single pump. The bulk of the charging flow is pumped back to the RCS via the tube side of the regenerative heat exchanger where the outlet temperature approaches the reactor coolant temperature. The flow is then injected into a cold leg of the RCS. Two redundant injection paths are provided for rapid boration of the system. A flow path is also provided from the regenerative heat exchanger outlet to the pressurizer spray line. An air operated valve in the line is employed to provide auxiliary spray to the vapor space of the pressurizer.

A portion of the charging flow is directed to the reactor coolant pumps (nominally 8 gpm per pump) through a seal water injection filter. From the pumps, the leakage water goes to the seal water heat exchanger and then returns to the VCT for another circuit. If the normal letdown and charging path through the regenerative heat exchanger is not operable, water injection into the RCS through the reactor coolant pump seals is returned to the VCT through the excess letdown heat exchanger.

Surges from the RCS accumulate in the VCT unless a high water level in the tank causes flow to be diverted to the Boron Recycle System. Low



level in the VCT initiates makeup from the reactor makeup control system (RMCS). If the RMCS does not supply sufficient makeup, the suction of the charging pumps is transferred from the VCT to the refueling water storage tank.

For the event trees, failure of the CVCS letdown and charging function is defined as operator errors and/or equipment malfunctions that prevent cooldown of the RCS to a cold shutdown state via the CVCS.

#### A.2.8 EMERGENCY COOLANT INJECTION (ECI) AND RECIRCULATION (ECR)

The Safety Injection System (SIS) provides emergency core cooling in the event of a break in either the Reactor Coolant or Steam System. Borated water is introduced into the Reactor Coolant System (RCS) in order to cool the core and to prevent the possibility of an uncontrolled return to criticality. The emergency core cooling following a LOCA is divided into three phases:

##### A. Emergency Cooling-Cold Leg Injection (ECI)

The cold leg injection phase is defined as that period during which borated water is delivered from the Refueling Water Storage Tank (RWST) and accumulators, if actuated, to the RCS cold legs. The primary emphasis during this phase is directed towards minimizing or preventing damage to the core, by rapidly refilling the reactor vessel and reflooding the core.

##### B. Emergency Cooling-Cold Leg Recirculation (ECR<sub>C</sub>)

The cold leg recirculation phase is that period during which borated water is recirculated from the containment sump to the RCS cold legs. The primary function of the SI system during this phase is to remove the decay heat from the reactor core.

### C. Emergency Cooling-Hot Leg Recirculation (ECR<sub>H</sub>)

The hot leg recirculation phase is that period during which borated water is recirculated from the containment sump to both the hot and cold legs of the RCS. The primary function of the SI system during this phase is to terminate any boiling in the core, prevent possible boron precipitation buildup and to maintain the core in a subcooled condition as long as cooling is required.

The overall safety injection system consists of three systems, two active (high-head and low-head) and one passive:

#### 1. High-Head System

The high head system utilizes two subsystems. The first subsystem, which provides extremely rapid response to the safety injection actuation signal, utilizes a boron injection tank (BIT) located upstream of the cold leg injection header, and two parallel centrifugal charging pumps (shut-off head of 2700 psia) of the Chemical Volume Control System. Following an actuation signal, the suction of the charging pumps is diverted from the Volume Control Tank to the RWST. The parallel valves isolating the boron injection tank from the pumps and the parallel valves isolating the tank from the injection header are then automatically opened. Initially, the refueling water flow forces the highly concentrated boric acid solution from the tank, and into the cold legs of each loop.

The second subsystem employs two parallel high head safety injection (HHSI) pumps, valved to take suction from the RWST to deliver borated water to the core through injection nozzles on the RCS cold legs. The shut-off head of these pumps is 1500 psia. After the injection and cold leg recirculation phases, the HHSI subsystem is realigned by operator action for hot leg injection and pump suction from the discharge of the RHR heat exchangers for long term cooling of the reactor.

## 2. Low Head System

The low head system utilizes the two parallel residual heat removal pumps, both of which take suction from the RWST. During the injection phase, borated water is pumped through the residual heat exchangers, to the same injection nozzles used for the accumulators on the RCS cold legs, once RCS pressure drops below that of the pump shutoff head, 200 psia.

The changeover from the injection mode to the recirculation mode (cold leg) is initiated automatically and completed manually by operator action from the main control room. Protection logic is provided to automatically open two parallel SI system recirculation sump isolation valves when two-out-of-four RWST level channels indicate a RWST level less than a low-low water level setpoint in conjunction with the initiation of the SI actuation signal. When the containment sump recirculation valves are fully open, RHR pump suction from the RWST is automatically isolated, and the two RHR pumps are aligned to take suction from the sump and to deliver water directly to the RCS. The low-low RWST level signal is alarmed to inform the operator to initiate manual action to align RHR pump discharge to the suction of the centrifugal charging and high head safety injection pumps in order to assure injection of sufficient coolant into the RCS when the RCS pressure remains above the RHR pumps shutoff head.

The cold leg to hot leg recirculation switch-over procedure requires manual action by the operator to align isolation valves to terminate RHR flow to one RCS cold leg and establish flow to a hot leg of the RCS. The operator must also stop the HHSI pumps one-at-a-time and realign valves within the HHSI subsystem to terminate flow to the cold legs and establish flow to all RCS hot legs.

### 3. Accumulators

The passive accumulative subsystem utilizes the stored energy of compressed nitrogen to inject borated water (2000 ppm boron concentration) into the cold legs of the RCS when system pressure drops below 600 psia, the cover gas pressure. One accumulator tank per loop is provided and is sized so that only the contents of three of the four tanks are necessary to provide sufficient liquid to initiate refill of the reactor vessel following a large break.

Each discharge line contains two swing check valves (in the event that one leaks) and one normally open motor-operated valve for the purpose of isolating the tank.

The SIS is designed to tolerate a single failure without loss of its core protective functions. This failure is limited either to an active failure during the short term (injection) phase following a LOCA or to an active or passive failure during the long-term (recirculation) phase.

In order to meet the single failure criterion, it is necessary that redundancy in system design be employed. For example, valves which need to be opened for proper SIS functioning are duplicated in parallel; valves which must be closed are duplicated in series.

#### A.2.8.1 ECI Termination

For the SGTR accident, once the RCS pressure has been decreased to that of the faulted steam generator and break flow through the rupture has been stopped, the depressurization process via pressurizer spray or relief valve is terminated. To permit continued depressurization and cooldown, the high head safety injection pumps must be tripped. At this point, normal Chemical and Volume Control System (CVCS) charging and letdown flow is established to maintain the pressurizer water level within allowable span limits and to aid in subsequent RCS cooldown. If,

during subsequent recovery actions, pressurizer water level cannot be maintained above 20 percent indicated level, re-initiation of safety injection will be required.

For the large break event tree then, ECI failure is (1) delivery of less borated water than would result from the discharge of three accumulators into the RCS cold legs immediately following a large pipe break, or (2) delivery of borated water at a flow rate less than the design output of one low head safety injection pump to the RCS cold legs (starting at about thirty seconds following a large pipe break). Failure of ECR is defined as failure to inject into the RCS from at least one low-head pump. Failure to realign to hot leg delivery (or failure to achieve coolant delivery, in part, through the hot legs with the continuance of delivery into cold legs) is also considered ECR failure.

For the remainder of the event trees, ECI failure is less than the equivalent in delivery of one train of the high head system. Failure of ECR is defined as failure to deliver water from the containment sump to the reactor cold legs by at least one high head pump taking suction from the discharge from one low head pump. ECR failure is also considered to be failure to switch to hot leg injection at about 1 day after the initiating event occurs.

For the SGTR event tree, ECI TERMINATION failure is defined as improper operator actions and/or equipment failures whereby ECCS flow from the HHSI pumps (both trains) is not terminated, accumulator injection is not isolated, or valve alignment for normal charging and letdown via the CVCS is not accomplished.

#### A.2.9 RHRS RECIRCULATION

The residual heat removal system (RHRS) functions to remove heat from the RCS when RCS pressure and temperature are below approximately 425 psig and 350 °F, respectively. Heat is transferred from the RHRS to the component cooling water system.

The RHRS consists of two residual heat exchangers, two residual heat removal pumps, and the associated piping, valves, and instrumentation necessary for operational control. The inlet and return lines of the RHRS are connected to the hot and cold legs, respectively, of two reactor coolant loops. These return lines are also the ECCS low head injection lines as reported previously in Section A.2.8.

The RHRS is isolated from the RCS on the suction side by two motor-operated valves in series on each suction line. Each motor-operated valve is interlocked to prevent its opening if RCS pressure is greater than 425 psig and to automatically close if RCS pressure exceeds 750 psig. The RHRS is isolated from the RCS on the discharge side by two check valves in each return line. Also provided on the discharge side is a normally open, motor-operated valve downstream of each RHRS heat exchanger.

During RHRS operation reactor coolant flows from the RCS to the residual heat removal pumps, through the tube side of the residual heat exchangers, and back to the RCS. The heat is transferred to the component cooling water circulating through the shell side of the residual heat exchangers. Each inlet line to the RHRS is equipped with a pressure relief valve designed to relieve the combined flow of all the charging pumps at the relief valve set pressure. These relief valves also protect the system from inadvertent overpressurization during plant cooldown or startup. Each discharge line from the RHRS to the RCS is equipped with a pressure relief valve designed to relieve the maximum possible backleakage through the valves isolating the RHRS from the RCS.

The RHRS is designed to be fully operable from the control room for normal operation and accident transients. Manual operations required of the operator are: opening the suction isolation valves, positioning the flow control valves downstream of the RHRS heat exchangers, and restarting the residual heat removal pumps if previously tripped by operator action. By nature of its redundant two-train design, the RHRS is

designed to accept all major component single failures with the only effect being an extension in the required cooldown time. For two low probability electrical system single failures, i.e., failure in the suction isolation valve interlock circuitry or diesel generator failure in conjunction with loss of offsite power, limited operator action outside the control room is required to open the suction isolation valves.

The RCS cooldown rate is manually controlled by regulating the reactor coolant flow through the tube side of the residual heat exchangers. The flow control valve in the bypass line around each residual heat exchanger automatically maintains a constant return flow to the RCS. Instrumentation is provided to monitor system pressure, temperature, and total flow. Coincident with operation of the RHRS, a portion of the reactor coolant flow may be diverted from downstream of the residual heat exchangers to the (CVCS) low pressure letdown line for cleanup and/or pressure control.

In the event tree, failure of the RHRS recirculation function corresponds to failure to deliver water to RCS cold leg by at least one train of RHRS.

### A.3 EVENT TREE DESCRIPTION

Table A.1 is a glossary of safety system functions examined in the event trees that follow, including definition of function failure. In this study, system operability success is defined as the degree of performance required by the NRC, estimated with conservative assumptions. It should be noted that if the system is degraded to the extent that performance is somewhat less than that normally required for success, the system may still be capable of performing the required function depending upon the margin incorporated in the design.

### A.3.1 LARGE LOCA (FIGURE A.1)

The initiating event is a random rupture in the RCS boundary during normal full-power operation that creates a break area ranging from about 10 inches in diameter up to the double-ended rupture of the largest primary pipe (limiting cold leg). Through the break, coolant is discharged to the containment, and results in depressurization of the RCS. Note, that as discussed in Section A.1.2, small breaks in the range of 2 to 10 in. equivalent diameter may be treated as "large" breaks for the purpose of this study. Table A.2 presents the system status for this event tree.

### A.3.2 SMALL LOCA (FIGURE A.2)

The initiating event ( $S_2$ ) is a random rupture in the RCS boundary during normal full-power operation that creates a break area ranging from 1/2 to 2 inches in diameter through which loss of coolant occurs. The event tree is applicable to any break location in the RCS that discharges to the containment, but discussions in Table A.4 Footnotes deal with the limiting cold leg break behavior. Table A.4 presents the systems status for this event tree.

### A.3.3 FEEDLINE BREAK (Figure A.3)

The initiating event ( $S_3$ ) is a random rupture in the feedwater piping system during nominal full-power operation. Operating at intermediate powers at shutdown conditions will result in less limiting results, however the trends identified will be unchanged. Table A.6 presents the systems status for this event tree.

### A.3.4 STEAMLINER BREAK (Figure A.4)

The initiating event ( $S_4$ ) is a random rupture in the steam piping system or the inadvertent opening with failure to reclose of a steam dump, steam generator relief or safety valve during normal full power operation. Table A.8 presents the systems status for this event tree.



### A.3.5 STEAM GENERATOR TUBE RUPTURE (Figures A.5 and A.6)

The initiating event (SGTR) is a random rupture of a steam generator tube during normal full-power operation, creating a maximum break area equal to that of complete severance of a single tube. Through the break, coolant is discharged to the shell side of a steam generator, and results in the depressurization of the RCS and release of fission products to the atmosphere via the condenser air ejector system and/or steam generator safety/relief valves. Two trees are developed for SGTR; the first (Figure A.5) starts with the initiating event and ends with equilibration of primary and faulted secondary pressures, i.e. termination of break flow; the second continues on to RCS depressurization to atmospheric pressure, cooldown to a temperature below 200°F, and zero break flow. Tables A.10 and A.12 present the systems status for the SGTR event trees developed.

## A.4 INSTRUMENTATION DESCRIPTION

The following discussion characterizes the symptoms of Loss of Coolant Accident, Secondary High Energy Line Break (SHEL B) and Steam Generator Tube Rupture primarily in terms of several important instrument indications. It is assumed that reactor trip and safety injection initiation have occurred. Section C.3 provides a discussion of instrumentation available to the operator to perform safety functions following ANS Condition I, II, III or IV events.

### A.4.1 CONTAINMENT PRESSURE, CONTAINMENT SUMP WATER LEVEL, CONTAINMENT RADIATION

Since a LOCA involves loss of primary system inventory, there will always be an increase in containment pressure, sump water level and containment radiation. However, for very small breaks, observable containment pressure and sump water level changes may be very slow. The

rate of increase will depend on break size and location. While the symptoms as shown on these 3 sensors are typical of a LOCA, they are not unique to LOCA. The sensors will give similar indications with a SHELB in containment if prior to the break there existed an observable primary to secondary leakage. Thus, it is necessary to have additional data to determine if the break is a LOCA or SHELB.

For a small SHELB, particularly with continued operation of containment fan coolers, the pressure increase could be undetectable. Containment sump level could significantly increase, but after isolation of auxiliary feedwater to the faulted steam generator, no increase should take place, unless containment spray has been activated.

One distinguishing feature of the SGTR transient is that the containment instrumentation will show no change over pre-accident conditions. The absence of the containment instrument indications is one feature which allows the operator to distinguish between SGTR and LOCA or SHELB inside containment. The absence of containment instrumentation indications will not allow the operator to distinguish between SGTR and spurious SI initiation or secondary side line breaks outside containment.

#### A.4.2 RCS WIDE RANGE PRESSURE

Since a LOCA involves the loss of primary system inventory, there will be a reduction in RCS pressure at a rate and of a magnitude dependent on break size. This indication, however, is not unique to LOCA and additional information is needed to define the type of break.

A SHELB does not involve a loss of primary coolant. The Reactor Coolant System (RCS) pressure will follow the trends of primary temperatures, as heatup or cooldown will expand or shrink the RCS water inventory. This instrumentation is used in the termination procedures for reactor coolant pump operation and Safety Injection. It is also used in verifying that the RCS pressure is sufficient to maintain subcooled conditions.

Since a SGTR does involve a loss of primary system inventory, there will be a reduction of RCS pressure and temperature. These reductions in conjunction with the absence of containment instrument indications provide additional confirmation of a SGTR rather than a small LOCA. When the SI flow matches the leak flow rate, the RCS pressure and temperature will equilibrate at values below nominal setpoint values, and they may be decreasing slowly in a fairly stable manner.

#### A.4.3 PRESSURIZER WATER LEVEL

Following a LOCA, pressurizer water level will decrease (or even drop below the lower tap) initially. This is caused, in part, by the pipe leak mass outflow, the volume shrink following reactor trip and the volume shrink caused by injecting cold SI water. In the case of a small LOCA, once the RCS pressure equilibrates, continued operation of the HHSI can lead to re-establishing level in the pressurizer. This refill process should be relatively slow. It should not exhibit rapid fluctuations or occur very early in the transient. These symptoms may also occur for certain small LOCAs or secondary side breaks, but the presence of containment instrument indications allows the larger LOCA events to be distinguished. In the case of a LOCA from the pressurizer vapor space or a stuck open relief valve, indicated pressurizer level will rise.

For a SHELVB, pressurizer level will respond to RCS volume variations induced by primary temperature changes. With due credit for charging, letdown and Safety Injection (SI) flow, it will be apparent that no loss of RCS inventory occurred, as opposed to loss of reactor coolant or steam generator tube rupture accidents. This is unique to loss of secondary coolant events and can be verified during the long term recovery phase of the accident. This instrumentation is used to verify sufficient pressurizer water volume to cover the heaters. It is also used as an input to the level controller once the plant is stabilized. Caution should be exercised when using this instrumentation due to the possibility of large errors in the indicated level.

Following a SGTR, it is expected that the pressurizer level will initially drop. This is caused in part, by the tube leak mass outflow, the volume shrink following reactor trip and the volume shrink caused by injecting cold SI water. Once the RCS pressure equilibrates, continued operation of the HHSI will lead to re-establishing level in the pressurizer. This refill process should be relatively slow.

#### A.4.4 RCS WIDE RANGE $T_{Hot}$ AND $T_{Cold}$

In general, these indicators will show time variation after LOCA, SGTR and SHEL B. The magnitude of the changes will depend both on break size and location. For that reason, these parameters are not particularly useful in type-of-accident diagnostics.

$T_{Hot}$  is used in determining which Safety Injection termination procedure to use. It is also used in verifying that the RCS temperature is sufficiently low to maintain subcooled conditions.  $T_{Hot}$  is used in conjunction with  $T_{Cold}$  in verifying that core cooling is taking place through either forced flow or natural circulation.

#### A.4.5 STEAM GENERATOR LEVEL (NARROW AND WIDE RANGE LEVELS)

This instrumentation is used in the Safety Injection termination procedure and to verify adequate secondary side heat sink capability for plant cooldown.

For a LOCA, SG level instruments should display readings in their normal range.

With due credit for auxiliary feedwater operation, low steam generator level will occur in at least one steam generator for a loss of secondary coolant. For certain break locations the accident will appear similar to a loss of normal feedwater. Hence, this parameter alone is not sufficient to diagnose a loss of secondary coolant.

Following AFW actuation for an SGTR, the SG level may initially fall then rise due to AFWS operation. If a large SGTR has occurred, it may become difficult for the operator to maintain water level in the affected SG without throttling back the AFW to that SG. If the AFW flow to all SGs are balanced, then the affected SG water level should rise at a higher rate due to the mass flow from the break. For very small SGTRs, it may be very difficult to notice any difference in SG levels or level rise rates among the SGs. SG level indication does not provide any key information to aid in short term diagnosis for an SGTR. However, it should be verified that level has been established so that the steam generators can be used as heat sinks.

#### A.4.6 STEAMLINER PRESSURE

For a LOCA, this instrument should display a reading in its normal range. However, very low steam generator pressure, e.g. lower than the steamline isolation setpoint, in one or more steam generators is indicative of a loss of secondary coolant. But certain break locations can produce no change or actually lead to an increase in steam generator pressure; hence, this parameter alone is not sufficient for diagnosis of a loss of secondary coolant.

Following a SGTR, steam pressure in the affected SG may continue to stay at a pressure above that found in an intact SG. This symptom is of limited diagnostic utility for very small SGTR leak rates.

#### A.4.7 STEAM FLOW, FEEDWATER FLOW

For a loss of secondary coolant, these parameters can exhibit widely differing behavior, depending upon break size and location. High steam flow after safety injection actuation is indicative of a loss of secondary coolant. The accident is certainly a loss of secondary coolant event if high steam flow persists after successful steamline

isolation, with the due credit for potential steamline relief/safety valve operation. This is also the case for feedwater flow since feedwater isolation occurs on a safety injection signal.

#### A.4.8 CONDENSER AIR EJECTOR RADIATION AND SG BLOWDOWN RADIATION

These symptoms are the ones most characteristic of a SGTR event. Assuming that no leakage existed prior to the event, high-radiation alarms will result rapidly following SGTR. If some leakage (within tech specs) exists prior to the event, the signal will rapidly increase corresponding to the increased leak rate into the SG. If the normal operating range for these instruments is low, the presence of high radiation levels due to the SGTR may drive the response off-scale so rapidly that no useful information can be obtained regarding rate phenomena.

These instrument indications can also be useful in helping to distinguish between certain small LOCAs and SGTR. If the LOCA is small enough that immediate indications from containment sump levels and containment radiation do not occur, the absence of SG blowdown radiation and condenser air ejector radiation in conjunction with continued operation of the HHSI should guide the operator to look for alternative indications of a LOCA.

#### A.4.9 AUXILIARY FEEDWATER FLOW

Following an "S" signal during an SGTR event, the AFWS will deliver to all SGs. If the SGTR flow is large, it may be necessary to throttle the AFW delivered to the affected SG to avoid over-filling that SG. In this manner, AFW flow can potentially provide additional confirmatory information that a SGTR has occurred. For very small SGTRs, preferential throttling of AFW flow to the affected SG may not be required. For all SGTRs, AFW should be maintained at least until identification and isolation of the affected SG occurs. Following that, AFW flow to the intact SGs is required to provide a heat sink.

#### A.4.10 CONDENSATE STORAGE TANK LEVEL

This instrumentation is used for these transients in verifying that an adequate water source is available for auxiliary feedwater, i.e., secondary side cooling. It is also used in determining if switchover to a secondary source of water for auxiliary feedwater is necessary.

#### A.4.11 IN-CORE THERMOCOUPLES

This instrumentation is used for these transients as an additional indication of core temperatures and can be used to verify that core cooling is taking place.

#### A.5 PROCEDURES REVIEW

The Emergency Operating Instructions\* provide coverage for current design basis events, e.g., RCS pipe break with single active failure. The EOIs consider situations in which the operator may misdiagnose the event; and in some cases multiple equipment failures have been included. The review of the instructions is carried out by identifying the steps in the instructions which address the function/loss of function pair in the event trees.

---

\*E-0: Immediate Actions and Diagnostics, Rev. 2

E-1: Loss of Reactor Coolant, Rev. 2

E-2: Loss of Secondary Coolant, Rev. 2

E-3: Steam Generator Tube Rupture, Rev. 2

For sequence 1 of the event trees, which represent the design basis cases, the instructions naturally address all of the functions identified for the event. For example, E-0 (Steps C1-3, D1-5) instructs the operator to verify the operability of system functions listed, and sends him to the appropriate instruction based on appropriate instrument readings. E-1 (Notes and steps C1-5) instructs the operator to verify the operability of the monitoring instrumentation, and states the conditions under which safety injection may be terminated and normal makeup and letdown re-established. Finally, E1 (Steps C7-14 and Table E-1.1) lists the instructions for switchover to recirculation (cold and hot leg). Background information, describing the philosophy and basis for developing the instructions and discussing instrument readings, is provided for operator training programs. For the remaining sequences, the steps in the instructions which address particular function/loss of function pairs in the event tree are indicated in the table which follows each event tree status table.

Tables A.3, A.5, A.7, A.9, A.11, and A.13 identify several functions the loss of which are considered to be partially covered by the instruction guidelines. In most cases the guidelines direct the operator to manually or locally effect repairs in order to get critical safety equipment operating. This would include situations where there is partial or total loss of function, e.g., failure to start of one or all safety injection pump(s) respectively. The partial coverage column in these tables is meant to identify those situations in which the possibility exists that the operator may be unable to get critical safety equipment operating from the control room, but in which all of the possible contingency steps have not been incorporated in the instruction guidelines. It should be noted that many of these situations incorporate multiple failures within a system, which result in more than one total loss of function; these sequences are well beyond the current design basis. The probability of occurrence of such failures, coincident with the initiating event, is likely to be small enough to preclude the need for inclusion of contingency steps; alternatively it may be that incorporation of such steps may increase the complexity of the procedure and pose a greater risk of operator error or delay than not incorporating the step.



TABLE A.1 Glossary of Safety Functions

<u>SYMBOL</u>	<u>FUNCTION</u>	<u>DEFINITION OF FUNCTION FAILURE</u>
EP	ELECTRICAL POWER	FAILURE TO PROVIDE AC POWER TO BUSES THAT FURNISH POWER TO ESFS
RPS	REACTOR PROTECTION SYSTEM	FAILURE OF MORE THAN 2 CONTROL ROD ASSEMBLIES TO INSERT IN CORE--ELECTRICAL/MECHANICAL FAULT
AFWS	AUXILIARY FEEDWATER SYSTEM	FAILURE TO DELIVER THE EQUIVALENT OF FULL FLOW OF ONE MOTOR-DRIVEN AFW PUMP
SSR	SECONDARY STEAM RELIEF	
SD/S/R-VO		FAILURE TO OPEN OF ALL STEAM GENERATOR STEAM DUMP, SAFETY AND RELIEF VALVES*
SD/S/R-VR		FAILURE TO RE-CLOSE OF ALL STEAM GENERATOR STEAM DUMP, SAFETY AND RELIEF VALVES
SDC		FAILURE TO OPERATE OF ALL STEAM DUMP VALVES*
PPC	PRIMARY PRESSURE CONTROL	
	SPRAY/AUXILIARY SPRAY	FAILURE TO DELIVER SPRAY FLOW FROM REACTOR COOLANT LOOP COLD LEGS/CVCS
	S/R-VO	FAILURE TO OPEN OF ALL PRESSURIZER SAFETY AND RELIEF VALVES*
	S/R-VR	FAILURE TO RE-CLOSE OF ALL PRESSURIZER SAFETY AND RELIEF VALVES
CVCS	CHEMICAL VOLUME AND CONTROL SYSTEM	FAILURE OF CHARGING AND LETDOWN FUNCTIONS THAT PREVENT COOLDOWN OF RCS TO COLD SHUTDOWN
ECI	EMERGENCY COOLANT INJECTION	FAILURE TO DELIVER BORATED WATER FROM AT LEAST 3 ACCUMULATORS OR 1 LHSI PUMP TO RCS COLD LEGS (LARGE LOCA) OR FAILURE TO DELIVER FLOW FROM AT LEAST 1 TRAIN OF HHSI SYSTEM
ECR	EMERGENCY COOLANT RECIRCULATION	FAILURE TO INJECT WATER INTO RCS FROM AT LEAST 1 HHSI OR LHSI PUMP, OR FAILURE TO RE-ALIGN TO HOT LEG INJECTION
ECI TERMINATION		OPERATOR ACTIONS AND/OR EQUIPMENT FAILURES THAT PREVENT TERMINATION OF FLOW FROM HHSI PUMPS OR FAILURE TO ALIGN VALVES FOR NORMAL CHARGING AND LETDOWN VIA CVCS
MSI	MAIN STEAM ISOLATION	FAILURE TO ISOLATE MAIN STEAM LINE TO FAULTED STEAM GENERATOR OR FAILURE TO TERMINATE AUXILIARY FEEDWATER TO THAT STEAM GENERATOR
RHRS	RESIDUAL HEAT REMOVAL SYSTEM	FAILURE TO DELIVER WATER TO RCS COLD LEG BY AT LEAST 1 TRAIN OF RHRS

\*Note that operation of one or more safety or relief valves constitutes success.

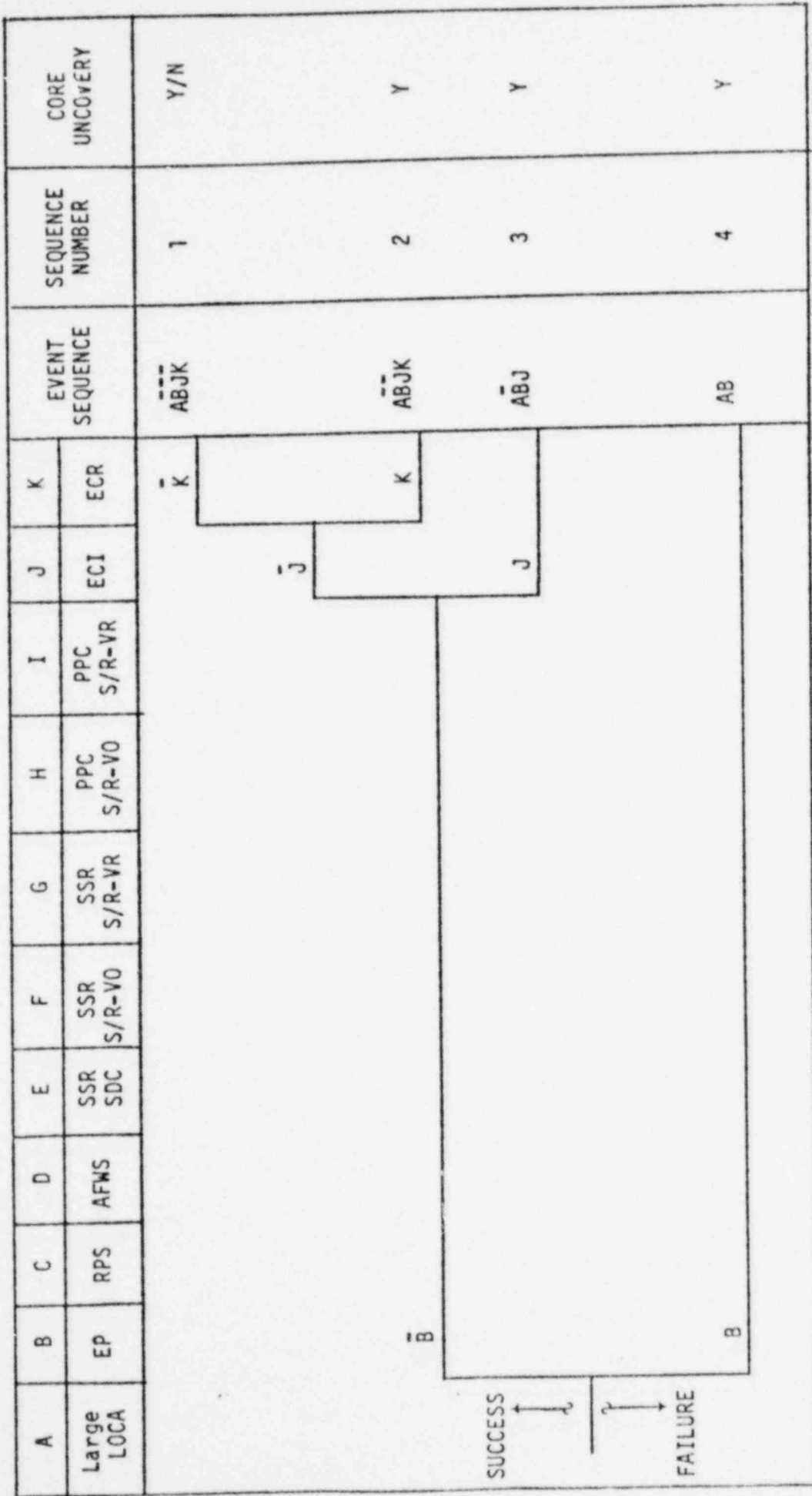


FIGURE A.1 Large LOCA Event Tree  
 10" < Equiv. Dia. < DECLG

SEQUENCE NUMBER	EVENT SEQUENCE	A	B	C	D	E	F	G	H	I	J	K	CORE UNCOVERY	FOOTNOTES
		LARGE LOCA	EP	RPS	AFWS	SSR SDC	SSR S/R-VO	SSR S/R-VR	PPC S/R-VO	PPC S/R-VR	ECI	ECR		
1	ABJK	f		O <sub>A</sub>	O <sub>A</sub>	O <sub>A</sub>	O <sub>A</sub>	O <sub>A</sub>	O <sub>A</sub>	O <sub>A</sub>			Y/N	a
2	ABJK	f		O <sub>A</sub>	O <sub>A</sub>	O <sub>A</sub>	O <sub>A</sub>	O <sub>A</sub>	O <sub>A</sub>	O <sub>A</sub>		f	Y	b
3	ABJ	f		O <sub>A</sub>	O <sub>A</sub>	O <sub>A</sub>	O <sub>A</sub>	O <sub>A</sub>	O <sub>A</sub>	O <sub>A</sub>	f	O <sub>J</sub>	Y	b
4	AB	f	f	O <sub>A</sub>	O <sub>A</sub>	O <sub>A</sub>	O <sub>A</sub>	O <sub>A</sub>	O <sub>A</sub>	O <sub>A</sub>	Z <sub>B</sub>	Z <sub>B</sub>	Y	c

Key:

- f - failure
- f<sub>N</sub> - dependent time-delayed failure caused by failure of "N"
- O<sub>N</sub> - does not matter; operation of function has no effect because of failure of "N"
- P<sub>N</sub> - does not matter; operation of function has no effect because of operation of "N"
- Z<sub>N</sub> - failure predicated by failure of "N"
- Y - core uncover occurs; operator action, short of reversing initial system failure(s), will not mitigate transient
- N - no core uncover occurs, unless operator acts to counter the effects of the safeguards system
- Y/N - core uncover may occur and proper operator action may prevent it

Footnotes:

- a. No loss of critical function. Design Basis Event.
- b. Failure of ECI or ECR leads to core uncover.
- c. Failure of EP prevents operation of other systems.

TABLE A.2 Large LOCA Systems Status

TABLE A.3 PROCEDURES REVIEW: LARGE LOCA EVENT TREE

Function Of Interest	Sequence Number	Pertinent Steps Of <u>W</u> EOI's		Coverage Of Reference Instructions	
		Instruction		Full / Partial*/ None	
	1	E-1		a**	Design Basis Event
ECR	2	E-1	C.4; C.6 .7; C.10; C. Table E-1.1: Prereq. A, C, E, F, Table E-1.2: Contingency Action, Step 1	b,c	Events Beyond Design Basis
A-43 ECI	3	E-0 E-1	C.1.b; C.2.f; C.3.a C.3; C.4	b	
EP	4	E-0 E-1	C.2.b C: Second Caution	b	

\* Partial coverage is defined to mean that contingency action has not been specified in the event that safety function which failed cannot be re-established (e.g., by manual, local, or repair actions).

- \*\* a. No loss of critical function. Design basis event.  
 b. Contingency action in the event of failure of safety system function may be required.  
 c. The need for rapid switchover to recirculation phase for large break LOCA has been addressed.

A-45

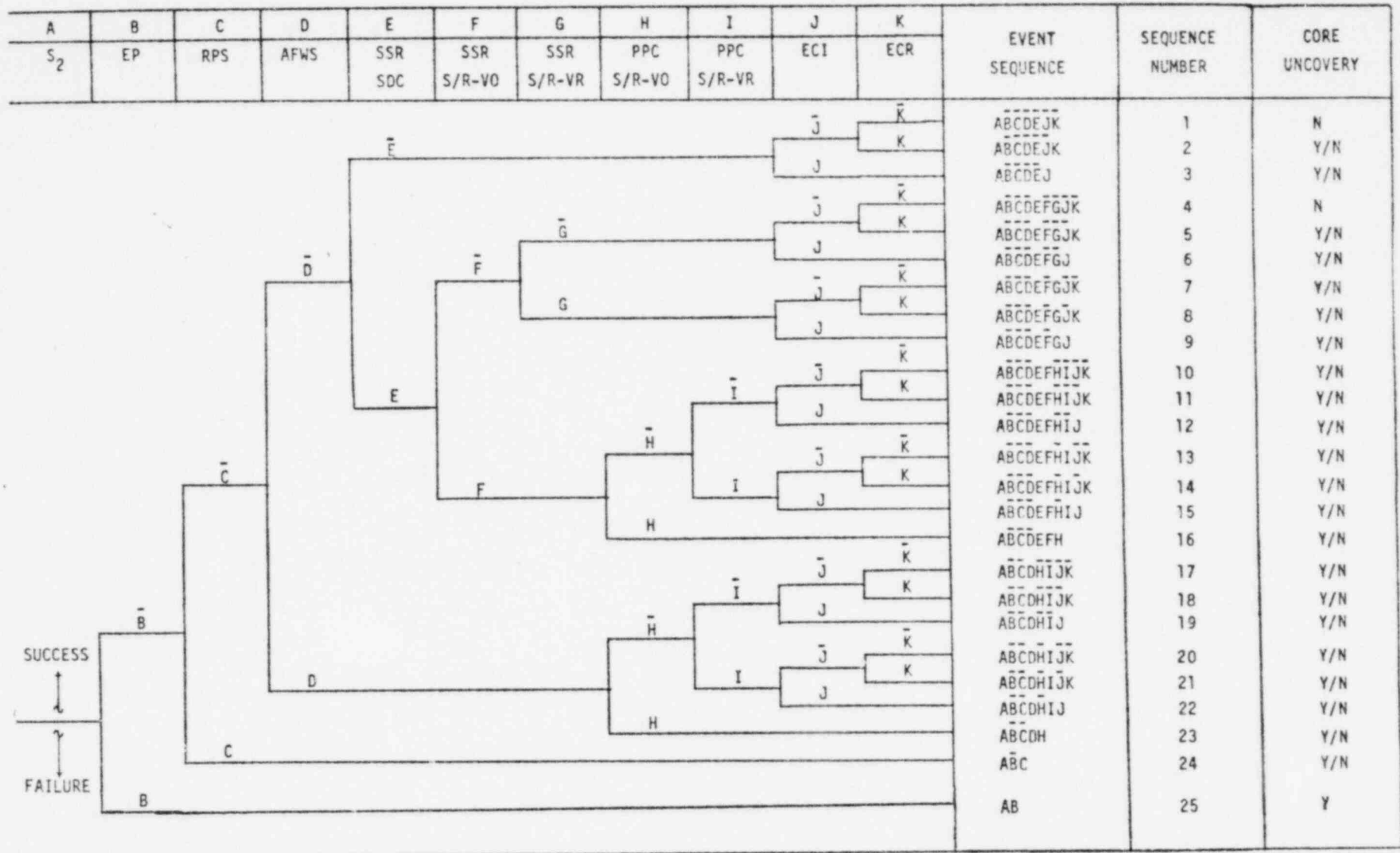


FIGURE A.2 Small LOCA Event Tree  
0.5" < Equiv. Dia. < 2.0"

SEQUENCE NUMBER	EVENT SEQUENCE	A S <sub>2</sub>	B EP	C RPS	D AFWS	E SSR SDC	F SSR S/R-VO	G SSR S/R-VR	H PPC S/R-VO	I PPC S/R-VR	J ECI	K ECR	CORE UNCOVERY	FOOTNOTES
1	ABCDEFJK	f					P <sub>E</sub>	P <sub>E</sub>	P <sub>E</sub>	P <sub>E</sub>			N	a,b
2	ABCDEFJK	f					P <sub>E</sub>	P <sub>E</sub>	P <sub>E</sub>	P <sub>E</sub>		f	Y/N	c
3	ABCDEFJ	f					P <sub>E</sub>	P <sub>E</sub>	P <sub>E</sub>	P <sub>E</sub>	f	O <sub>J</sub>	Y/N	d
4	ABCDEFGJK	f				f			P <sub>FG</sub>	P <sub>FG</sub>			N	e,a,b
5	ABCDEFGJK	f				f			P <sub>FG</sub>	P <sub>FG</sub>		f	Y/N	c
6	ABCDEFGJ	f				f			P <sub>FG</sub>	P <sub>FG</sub>	f	O <sub>J</sub>	Y/N	d
7	ABCDEFGJK	f				f		f	O <sub>G</sub>	O <sub>G</sub>			Y/N	g
8	ABCDEFGJK	f				f		f	O <sub>G</sub>	O <sub>G</sub>		f	Y/N	c, g
9	ABCDEFGJ	f				f		f	O <sub>G</sub>	O <sub>G</sub>	f	O <sub>J</sub>	Y/N	d
10	ABCDEFHIJK	f				f	f	O <sub>F</sub>					Y/N	h
11	ABCDEFHIJK	f				f	f	O <sub>F</sub>				f	Y/N	h,c
12	ABCDEFHIJ	f				f	f	O <sub>F</sub>			f	O <sub>J</sub>	Y/N	h,d
13	ABCDEFHIJK	f				f	f	O <sub>F</sub>		f			Y/N	i,h
14	ABCDEFHIJK	f				f	f	O <sub>F</sub>		f		f	Y/N	i,h,c
15	ABCDEFHIJ	f				f	f	O <sub>F</sub>		f	f	O <sub>J</sub>	Y/N	j
16	ABCDEFH	f				f	f	O <sub>F</sub>	f	O <sub>H</sub>	O <sub>H</sub>	O <sub>H</sub>	Y/N	k,l
17	ABCDEFHIJK	f			f	O <sub>D</sub>	O <sub>D</sub>	O <sub>D</sub>					Y/N	m
18	ABCDEFHIJK	f			f	O <sub>D</sub>	O <sub>D</sub>	O <sub>D</sub>				f	Y/N	m,c
19	ABCDEFHIJ	f			f	O <sub>D</sub>	O <sub>D</sub>	O <sub>D</sub>			f	O <sub>J</sub>	Y/N	m,d
20	ABCDEFHIJK	f			f	O <sub>D</sub>	O <sub>D</sub>	O <sub>D</sub>		f			Y/N	i
21	ABCDEFHIJK	f			f	O <sub>D</sub>	O <sub>D</sub>	O <sub>D</sub>		f		f	Y/N	i,c
22	ABCDEFHIJ	f			f	O <sub>D</sub>	O <sub>D</sub>	O <sub>D</sub>		f	f	O <sub>J</sub>	Y/N	j,d
23	ABCDEFH	f			f	O <sub>D</sub>	O <sub>D</sub>	O <sub>D</sub>	f	O <sub>H</sub>	O <sub>H</sub>	O <sub>H</sub>	Y/N	l,n
24	ABC	f		f	O <sub>C</sub>	O <sub>C</sub>	O <sub>C</sub>	O <sub>C</sub>	O <sub>C</sub>	O <sub>C</sub>	O <sub>C</sub>	O <sub>C</sub>	Y/N	l,o
25	AB	f	f	O <sub>B</sub>	O <sub>B</sub>	Z <sub>B</sub>	O <sub>B</sub>	O <sub>B</sub>	O <sub>B</sub>	O <sub>B</sub>	Z <sub>B</sub>	Z <sub>B</sub>	Y	p

Key:

- f - failure
- f<sub>N</sub> - dependent time-delayed failure caused by failure of "N"
- O<sub>N</sub> - does not matter; operation of function has no effect because of failure of "N"
- P<sub>N</sub> - does not matter; operation of function has no effect because of operation of "N"
- Z<sub>N</sub> - failure predicated by failure of "N"
- Y - core uncovery occurs; operator action, short of reversing initial system failure(s), will not mitigate transient
- N - no core uncovery occurs, unless operator acts to counter the effects of the safeguards systems
- Y/N - core uncovery may occur and proper operator action may prevent it

TABLE A.4 Small LOCA Systems Status

Table A.4 Footnotes\*

- a. No loss of critical function. Design basis event.
- b. Break should be isolated if possible (e.g., in pressurizer vapor space).
- c. Failure of ECR may lead to core uncover. For example, for smaller breaks in this range, extended time (up to 1 day) may be available for the operator to attempt to re-establish ECR (e.g., repair equipment) if he recognizes the failure during the injection phase.
- d. ECI failure, without operator action, may lead to core uncover, and may result in inadequate core cooling. Given the definition of ECI failure in Section A.2.8 for the small break event tree, one potential action for the operator to take is to depressurize the RCS by holding the pressurizer PORV(s) open in order to actuate the accumulators and low head safety injection pumps to recover the core.
- e. This sequence most closely represents the case typically analyzed for plant Safety Analysis Reports since it includes satisfying all of the functions in Table A.4 with the limiting single failure, except steam dump to the condenser which is a consequence of loss of offsite power. Section 3.1 of WCAP-9600 describes the transient response for small breaks in this range (1/2" to 2" equivalent diameter); these breaks exhibit little or no core uncover so that core damage is minimal, even with the limiting single failure and 10CFR50 Appendix K assumptions. With better estimate input/assumptions, these breaks exhibit no core uncover.
- g. For a steam break (safety or relief valve failure), level may be maintained in the steam generators if sufficient auxiliary feedwater is available. Primary system pressure will decrease, safety injection will increase and the system will stabilize with the core covered and safety injection flow matching break flow. If sufficient auxiliary feedwater is not available, event follows note m.

\*Reactor coolant pump trip has not been considered in the construction of the event tree. Criteria for such action are discussed in WCAP-9584.

Table A.4 Footnotes (Continued)

- h. In the unlikely event of complete loss of SSR, primary system pressure will increase as secondary side pressure increases in attempt to equilibrate at RCS pressure. If the pressurizer relief valves operate normally, primary system will stabilize at the valve set pressure and will result in a net loss of inventory. If the operator does not take action to hold open the pressurizer PORV(s) or establish SSR to depressurize the secondary side, then the secondary side will probably rupture.
- i. If pressurizer safety or relief valve fails to reclose, the break may be large enough to depressurize the primary system, increase safety injection and enable the system to equilibrate at a pressure at which safety injection flow equals total break flow, with the core covered. If the total break area is not large enough to depressurize the primary system, RCS will stabilize at the relief valve set pressure and will result in a net loss of inventory.
- j. Depending upon break size and decay heat generation at the time of pressurizer safety or relief valve failure, break may be large enough to depressurize the RCS to the point of actuation of the accumulators and low head safety injection pumps. If the total break area is not large enough to depressurize the primary system, RCS will stabilize at the relief valve set pressure and will result in a net loss of inventory; this sequence is similar to sequence 12 except that the loss of primary inventory will be more rapid.
- k. With the unlikely unavailability of any function to depressurize the primary system and no capability for secondary steam relief, operator action may not prevent core uncover for these coincident failures. The primary and/or secondary system will probably rupture which, depending upon location and size of break, may provide sufficient primary and/or secondary relief capacity to mitigate core uncover.



Table A.4 Footnotes (Continued)

- l. ECCS cannot operate against system pressures anticipated.
- m. Failure to obtain auxiliary feedwater flow will eventually result in primary pressure increase to the pressurizer safety or relief valve set pressure. Normal valve operation would maintain system pressure at the valve setpoint, and would require operator intervention to depressurize the system by manually holding the valve(s) open and allow sufficient safety injection to make up loss. Westinghouse performed analyses described in WCAP-9600 which indicated that the operator had time to initiate auxiliary feed flow or to open all PORVs to prevent core uncover. With the subsequent depressurization, the RCS eventually stabilizes at a pressure at which safety injection flow matches break flow.
- n. In the unlikely event of failure of pressurizer safety and relief valves to open, depending upon location and size of consequential primary system rupture, the break may provide sufficient relief capacity to increase safety injection to prevent core uncover.
- o. Initiating event plus RPS failure is of sufficiently low probability that additional function failures were not considered in event tree evaluation. Due to increase in primary system pressure, core uncover may occur.
- p. Failure of EP prevents operation of other systems.

TABLE A.5 PROCEDURES REVIEW: SMALL LOCA EVENT TREE

Function Of Interest	Sequence Number	Pertinent Steps Of <u>W</u> EOI's		Coverage Of Reference Instructions	
		Instruction	Step	Full / Partial*/ None	
SSR/SDC	1; 4	E-1		a**	Design Basis Events
	5-16	E-1		c	
PPC S/R-VR	13-15;	E-0	D.1.b	x	Events Beyond Design Basis
	20-22	E-1	C.2; C.3		
ECR	2; 5; 8; 10; 14; 18; 21	E-1	C.4; C.10; C.11; Table E-1.1; Prereq. A; Step 5	b	Events Beyond Design Basis
ECI	3; 6; 9; 12; 15; 19; 22	E-0	C.1.b; C.2.f; C.3.a C.3; C.4	b	
		E-1			
SSR S/R-VR	7; 8; 9	E-0	D.4	d,b	
		E-2	C.6		
AFWS	17-23	E-0	C.2.e; C.3.b C.3	b	
		E-1			
EP	25	E-0	C.2.b C: Second Caution	b	
		E-1			
RPS	24	E-0	C.1.a; C.2.a; C.3	e	
SSR S/R-VO	10-16	E-0	C.3.c	e	
PPC S/R-VO	16; 23			e	Events Beyond Design Basis

\* Partial coverage is defined to mean that contingency action has not been specified in the event that safety function which failed cannot be re-established (e.g., by manual, local or repair actions).

\*\* See Footnotes

Table A.5 Footnotes

- a. No loss of critical function. Design basis event.
- b. Contingency action in the event of failure of safety system function may be required.
- c. EOI was written to provide coverage in the event of loss of off-site power, which includes loss of steam dump to condenser.
- d. In the case of multiple function failure which results in multiple events, e.g., LOCA and steam break, explicit instructions may need to be developed.
- e. Failure of total function has very low probability due to system design and need not be addressed.
- X. Denotes full coverage for sequences.

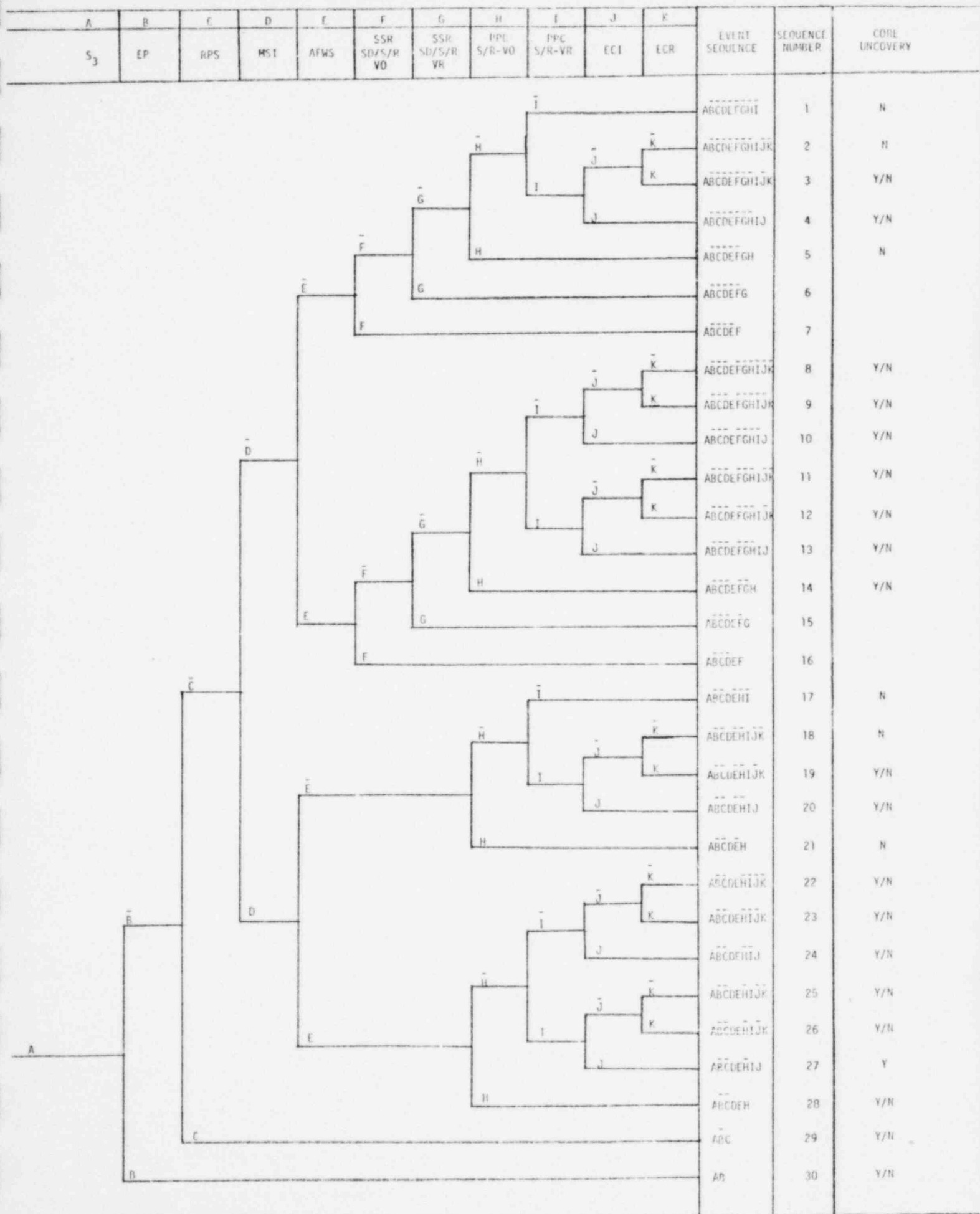


FIGURE A-1 FREEDLINE REACTOR EVENT TREE

SEQUENCE NUMBER	EVENT SEQUENCE	A S <sub>J</sub>	B EP	C RPS	D MSIV	E AFWS	F SSR SD/S/R VO	G SSR SD/S/R/VR	H PPC S/R-VO	I PPC S/R-VR	J ECI	K ECR	CORE UNCOVERY	FOOTNOTES
1	ABCDEF <sup>~</sup> GHI	f									P <sub>I</sub>	P <sub>I</sub>	N	a
2	ABCDEF <sup>~</sup> GHIJK	f								f			N	d
3	ABCDEF <sup>~</sup> GHIJK	f								f		f	Y/N	b
4	ABCDEF <sup>~</sup> GHIJ	f								f	f	O <sub>J</sub>	Y/H	h,c
5	ABCDEF <sup>~</sup> GH	f							f	O <sub>H</sub>	O <sub>H</sub>	O <sub>H</sub>	N	g
6	ABCDEF <sup>~</sup> G	f						f	O <sub>G</sub>	O <sub>G</sub>	O <sub>G</sub>	O <sub>G</sub>		m,j
7	ABCDEF <sup>~</sup>	f					f	O <sub>F</sub>	O <sub>F</sub>	O <sub>F</sub>	O <sub>F</sub>	O <sub>F</sub>		m
8	ABCDEF <sup>~</sup> GHIJK	f				f							Y/N	e
9	ABCDEF <sup>~</sup> GHIJK	f				f						f	Y/N	e,b
10	ABCDEF <sup>~</sup> GHIJ	f				f					f	O <sub>J</sub>	Y/N	e,c
11	ABCDEF <sup>~</sup> GHIJK	f				f				f			Y/N	d
12	ABCDEF <sup>~</sup> GHIJK	f				f				f		f	Y/N	d,b
13	ABCDEF <sup>~</sup> GHIJ	f				f				f	f	O <sub>J</sub>	Y/H	h,c
14	ABCDEF <sup>~</sup> GH	f				f			f	O <sub>H</sub>	O <sub>H</sub>	O <sub>H</sub>	Y/N	f
15	ABCDEF <sup>~</sup> G	f				f		f	O <sub>G</sub>	O <sub>G</sub>	O <sub>G</sub>	O <sub>G</sub>		m
16	ABCDEF <sup>~</sup>	f				f	f	O <sub>F</sub>	O <sub>F</sub>	O <sub>F</sub>	O <sub>F</sub>	O <sub>F</sub>		m
17	ABCDEF <sup>~</sup> HI	f			f						P <sub>I</sub>	P <sub>I</sub>	N	j
18	ABCDEF <sup>~</sup> GHIJK	f			f					f			N	d,j
19	ABCDEF <sup>~</sup> GHIJK	f			f					f		f	Y/N	d,b,j
20	ABCDEF <sup>~</sup> GHIJ	f			f					f	f	O <sub>J</sub>	Y/N	h,c,j
21	ABCDEF <sup>~</sup> GH	f			f				f	O <sub>H</sub>	O <sub>H</sub>	O <sub>H</sub>	N	g,j
22	ABCDEF <sup>~</sup> GHIJK	f			f	f	O <sub>E</sub>	O <sub>E</sub>					Y/N	e,j
23	ABCDEF <sup>~</sup> GHIJK	f			f	f	O <sub>E</sub>	O <sub>E</sub>				f	Y/N	e,b,j
24	ABCDEF <sup>~</sup> GHIJ	f			f	f	O <sub>E</sub>	O <sub>E</sub>			f	O <sub>J</sub>	Y/N	e,c,j
25	ABCDEF <sup>~</sup> GHIJK	f			f	f	O <sub>E</sub>	O <sub>E</sub>		f			Y/N	d,j
26	ABCDEF <sup>~</sup> GHIJK	f			f	f	O <sub>E</sub>	O <sub>E</sub>		f		f	Y/N	d,b,j
27	ABCDEF <sup>~</sup> GHIJ	f			f	f	O <sub>E</sub>	O <sub>E</sub>		f	f	O <sub>J</sub>	Y	h,c,j
28	ABCDEF <sup>~</sup> GH	f			f	f	O <sub>E</sub>	O <sub>E</sub>	f	O <sub>H</sub>	O <sub>H</sub>	O <sub>H</sub>	Y/N	f,j
29	ABCDEF <sup>~</sup>	f		f	O <sub>C</sub>	O <sub>C</sub>	O <sub>C</sub>	O <sub>C</sub>	O <sub>C</sub>	O <sub>C</sub>	O <sub>C</sub>	O <sub>C</sub>	Y/N	k
30	ABCDEF <sup>~</sup>	f	f	O <sub>B</sub>	O <sub>B</sub>	O <sub>B</sub>	O <sub>B</sub>	O <sub>B</sub>	O <sub>B</sub>	O <sub>B</sub>	Z <sub>B</sub>	Z <sub>B</sub>	Y/N	l

Key:

- f - failure
- f<sub>N</sub> - dependent time-delayed failure caused by failure of N
- O<sub>N</sub> - does not matter; operation of function has no effect because of failure of N
- P<sub>N</sub> - does not matter; operation of function has no effect because of operation of N
- Z<sub>N</sub> - failure predicated by failure of N
- Y - core uncovery occurs; i.e. operator action, short of reversing initial system failure(s), will mitigate transient
- N - no core uncovery occurs, unless operator acts to counter the effects of the safeguards systems
- Y/N - core uncovery may occur and proper operator action may prevent it

TABLE A.6 FUEL LINE BREAK SYSTEMS STATUS

Table A.6 Footnotes

- a. No loss of critical function. Design basis event.
- b. Failure of ECR may lead to core uncover. For smaller relief flows, extended time may be available for the operator to attempt to reestablish ECR (e.g., repair equipment) if he recognizes the failure during injection phase.
- c. ECI failure, without operator action, may lead to core uncover, and may result in inadequate core cooling. If the RCS depressurizes, the operator can actuate accumulators and low head safety injection pumps to recover core.
- d. If pressurizer safety or relief valve fails to reclose, the resulting relief may be large enough to depressurize primary system, increase safety injection and enable the system to equilibrate at a pressure at which safety injection flow equals total relief flow, with the core covered.
- e. Failure to obtain auxiliary feedwater flow will eventually result in primary pressure increase to the pressurizer safety or relief valve setpoint. Unless the operator keeps the relief valves open to reduce primary pressure below the high head SI pump cut off head, the valves will cycle and the core may uncover.
- g. With auxiliary feedwater flow injecting into intact steam generators and without primary pressure relief through the pressurizer safety or relief valves, primary pressure should not increase sufficiently to cause a break in the primary system.
- h. Pressurizer safety or relief valve failure to reclose may depressurize the RCS and may lead to LOCA.

Table A.6 Footnotes (Continued)

- i. For an unlikely failure of pressurizer safety and relief valves to open concurrent with the failure to obtain auxiliary feedwater flow, the primary system will probably rupture. In this case, proper operator action may prevent core uncover, assuming the availability of ECI and ECR.
- j. Failure of steamline isolation through the MSIV's or relief valves will decrease the effectiveness of the AFWS. In the case of a feedline break inside containment, MSIV failure will result in a more adverse containment pressurization since the intact steam generators would be able to blowdown through the feedline rupture (assuming no check valves or operator action to isolate the faulted feedline).
- k. Initiating event plus RPS failure is of sufficiently low probability that additional function failures were not considered in event tree evaluation. Due to increase in primary system pressure, core uncover may occur.
- l. Failure of EP prevents operation of other systems.
- m. Leads to combined feedline-steamline break incident. Sequence continues on with event tree, Figure A.4.

TABLE A.7

## PROCEDURE REVIEW - FEEDLINE BREAK EVENT TREE

Function of Interest	Sequence No.	Pertinent Steps of <u>W</u> EOI's		Coverage of Reference Instructions**	
		Instruction	Step	Full/Partial*/None	
	1	E-0 E-2		X	Design Basis Events
PPC S/R-VR	2 thru 4 11 thru 13 18 thru 20 25 thru 27	E-0 E-2	D.1, D.5 C.3, C.6.D A-D	c	Events Beyond Design Basis
ECR	3; 9; 12; 19; 23; 26	E-2	C.5.C, Table E-2.1	a	
ECI	4; 10; 13; 20; 24; 27	E-0 E-2	C.1.b, C.2.f, C.3.a C.5.c, C.6	a	
SSR S/R-VR	6; 15	E-2	C.3, C.6. A-D	c	
SSR SR-VO	7; 16	E-2	C.7.A, C.7.B	b	
AFWS	8 thru 16 22 thru 28	E-0 E-2	C.2.e, C.3.b C.4	c	
MSI	17 E-2	E-0 E-2	C.4, D.4 B, C.3	a	
RPS	29	E-0	C.1.a, C.2.a, C.3	a	
EP	30	E-0 E-2	C.2.b C	a	
PPC SR/VO	5; 14; 21; 28			b	

\* Partial coverage is defined to mean contingency action has not been specified in the event that safety function which failed cannot be re-established (e.g., by manual, local or repair actions).

\*\* In review of the instructions, it is assumed that the operator has entered E-2 from E-0.



Table A.7 Footnotes

- a. Manual actuation identified as contingency action. Contingency action in the event of failure of safety function may be required.
  - b. Failure of total function has very low probability due to system design and need not be addressed.
  - c. In the case of multiple function failures which results in multiple events, e.g., feedbreak and LOCA, explicit instructions may need to be developed.
- X. Denotes full coverage for sequences.

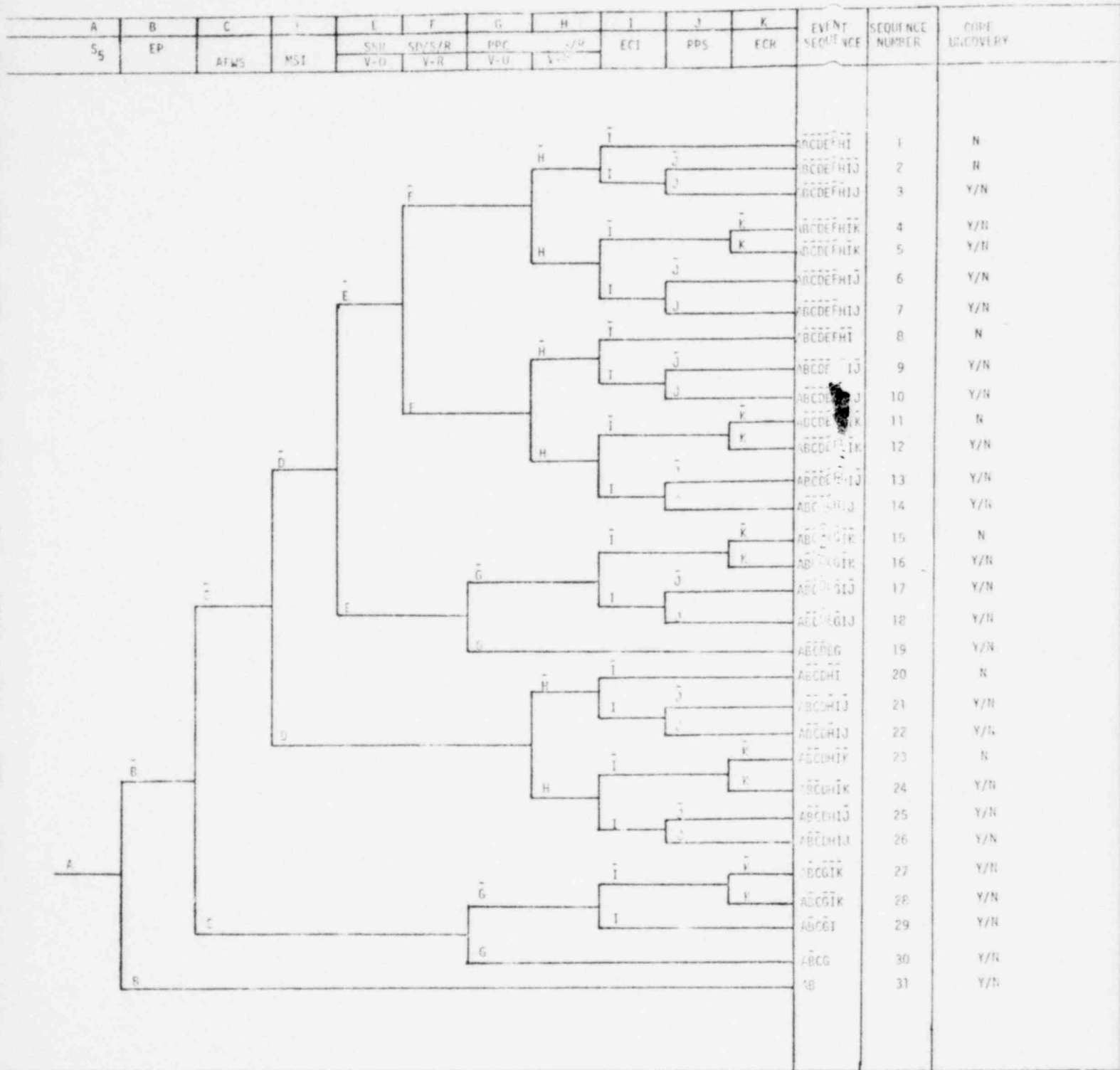


FIGURE A.4 STEAMLANE BREAK EVENT TREE

SEQUENCE NUMBER	EVENT SEQUENCE	A S <sub>5</sub>	B EP	C ATWS	D IMT	E SSR 50/S/R VO	F SSR 50/S/R VR	G PPC VG	H PHE VR	I ECT	J KPS	K ECR	COPE UN-IV-LRY	FOOTNOTES
1	ABCDEFHI	f						P <sub>EC</sub>			P <sub>I</sub>	P <sub>H</sub>	N	a,b
2	ABCDEFHIJ	f						P <sub>EC</sub>		f		P <sub>H</sub>	N	c
3	ABCDEFHIJ	f						P <sub>EC</sub>		f	f	P <sub>H</sub>	Y/N	c,g
4	ABCDEFHIK	f						P <sub>EC</sub>	f <sub>A</sub>		P <sub>I</sub>		Y/N	e
5	ABCDEFHIK	f						P <sub>EC</sub>	f <sub>A</sub>		P <sub>I</sub>	f	Y/N	e,h
6	ABCDEFHIJ	f						P <sub>EC</sub>	f <sub>A</sub>	f		Z <sub>1</sub>	Y/N	e,c,d
7	ABCDEFHIJ	f						P <sub>EC</sub>	f <sub>A</sub>	f	f	Z <sub>1</sub>	Y/N	e,p
8	ABCDEFHI	f					f	O <sub>f</sub>			P <sub>I</sub>	P <sub>H</sub>	N	j,b
9	ABCDEFHIJ	f					f	O <sub>f</sub>		f		Z <sub>1</sub>	Y/N	j,c
10	ABCDEFHIJ	f					f	O <sub>f</sub>		f	f	Z <sub>1</sub>	Y/N	j,g
11	ABCDEFHIK	f					f	O <sub>f</sub>	f <sub>A</sub>		P <sub>I</sub>		N	j,e
12	ABCDEFHIK	f					f	O <sub>f</sub>	f <sub>A</sub>		P <sub>I</sub>	f	Y/N	j,e,h
13	ABCDEFHIJ	f					f	O <sub>f</sub>	f <sub>A</sub>	f		Z <sub>1</sub>	Y/N	j,e,d
14	ABCDEFHIJ	f					f	O <sub>f</sub>	f <sub>A</sub>	f	f	Z <sub>1</sub>	Y/N	j,e,g
15	ABCDEFI	f				f	O <sub>f</sub>		O <sub>E</sub>		P <sub>I</sub>		N	k
16	ABCDEFI	f				f	O <sub>f</sub>		O <sub>E</sub>		P <sub>I</sub>	f	Y/N	k,b
17	ABCDEFI	f				f	O <sub>f</sub>		O <sub>E</sub>	f		O <sub>I</sub>	Y/N	k,d
18	ABCDEFI	f				f	O <sub>f</sub>		O <sub>E</sub>	f	f	O <sub>I</sub>	Y/N	k,d,i
19	ABCDEF	f				f	O <sub>f</sub>	f	O <sub>G</sub>	Z <sub>6</sub>	O <sub>EG</sub>	O <sub>G</sub>	Y/N	k,i
20	ABCDEF	f			f	O <sub>D</sub>	O <sub>D</sub>	O <sub>D</sub>			P <sub>I</sub>	P <sub>H</sub>	N	j,b
21	ABCDEF	f			f	O <sub>D</sub>	O <sub>D</sub>	O <sub>D</sub>		f		Z <sub>1</sub>	Y/N	j,d
22	ABCDEF	f			f	O <sub>D</sub>	O <sub>D</sub>	O <sub>D</sub>		f	f	Z <sub>1</sub>	Y/N	j,d,p
23	ABCDEF	f			f	O <sub>D</sub>	O <sub>D</sub>	O <sub>D</sub>	f <sub>A</sub>		P <sub>I</sub>		N	j,e
24	ABCDEF	f			f	O <sub>D</sub>	O <sub>D</sub>	O <sub>D</sub>	f <sub>A</sub>		P <sub>I</sub>	f	Y/N	j,e,h
25	ABCDEF	f			f	O <sub>D</sub>	O <sub>D</sub>	O <sub>D</sub>	f <sub>A</sub>	f		Z <sub>1</sub>	Y/N	j,e,p
26	ABCDEF	f			f	O <sub>D</sub>	O <sub>D</sub>	O <sub>D</sub>	f <sub>A</sub>	f	f	Z <sub>1</sub>	Y/N	j,e,p,i
27	ABCDEF	f		f	O <sub>C</sub>	O <sub>C</sub>	O <sub>C</sub>		O <sub>C</sub>		P <sub>I</sub>		Y/N	n,l
28	ABCDEF	f		f	O <sub>C</sub>	O <sub>C</sub>	O <sub>C</sub>		O <sub>C</sub>		P <sub>I</sub>	f	Y/N	n,h
29	ABCDEF	f		f	O <sub>C</sub>	O <sub>C</sub>	O <sub>C</sub>		O <sub>C</sub>		O <sub>C</sub>		Y/N	n,p
30	ABCDEF	f		f	O <sub>C</sub>	O <sub>C</sub>	O <sub>C</sub>	f	O <sub>G</sub>	f	O <sub>C</sub>	Z <sub>1</sub>	Y/N	n,l
31	AB	f	f	Z <sub>B</sub>	O <sub>C</sub>	O <sub>C</sub>	O <sub>C</sub>	O <sub>B</sub>	O <sub>C</sub>	Z <sub>B</sub>	O <sub>C</sub>	Z <sub>1</sub>	Y/N	l,n,o

Key:

- f - failure
- f<sub>i</sub> - dependent time-delayed failure caused by failure of i
- O<sub>f</sub> - does not matter; operation of function has no effect because of failure of i
- P<sub>i</sub> - does not matter; operation of function has no effect because of operation of i
- Z<sub>i</sub> - failure predicted by failure of i
- Y - core recovery occurs, no operator action, short of reversing initial system failure(s) will mitigate transient
- N - no core recovery occurs, unless operator acts to counter the effects of the safeguards system
- Y/N - core recovery may occur and proper operator action may prevent it

TABLE A.3 STEAMLINE BREAK SYSTEMS STATUS

Table A.8 Footnotes

- a. No loss of critical function. Design Basis Event.
- b. Operation of the safety injection system assures shutdown of the reactor via boration. Therefore reactor trip is not required to prevent core uncover. Reactor trip is desired to assure rapid shutdown and to maximize subcriticality in the event of consequential failures. Care must be taken to terminate function to prevent overpressurization.
- c. ECI failure requires reactor shutdown via RPS. Reactor trip is required to minimize steam generator cooling requirements with a steam generator isolated and while using the auxiliary feedwater system.
- d. Steam break isolation is accomplished via closure of the Main Steam-line Isolation Valves or via isolation of auxiliary feedwater from the faulted steam line/generator.
- e. Although pressurizer S/R valves were not expected to operate for this sequence, a random or consequential (adverse environment) failure results in the valves opening with a failure to reclose. This results in a vapor space type LOCA. Operator should attempt to isolate/regulate the break and must not terminate safety injection until he has done so. ECI required to prevent core uncover.
- g. Failure of reactor trip could result in inadequate secondary cooling which results in primary system heatup. Result is significant release from pressurizer relief valves and loss of primary coolant inventory.

Table A.8 Footnotes (Continued)

- h. ECR failure could lead to core uncover for cases in which pressurizer relief and safety valves cannot be reclosed or are required for long term cooling. Without significant loss of primary inventory, this function is not required. For small losses of primary inventory, extended time (up to 1 day) may be available for the operator to reestablish ECR (e.g. repair) if he recognizes the failure during injection phase.
- i. Core will uncover, the availability of reactor trip will significantly change time to core uncover.
- j. Cooldown will continue due to failure of valves on unisolated steam generators. Potential exists for core to return critical or for inadequate core cooling due RCS shrinkage and depressurization of primary system if ECI is not available.
- k. In the unlikely event of complete loss of SSR, primary system pressure will increase as secondary side pressure increases in attempt to equilibrate at RCS pressure. If the pressurizer relief valves operate normally, primary system will stabilize at the valve set pressure and will result in a net loss of inventory. If the operator does not take action to hold open the pressurizer PORV(s) or establish SSR to depressurize secondary, then the secondary side will probably rupture.
- l. ECI cannot operate against system pressures anticipated.
- m. Turbine driven auxiliary feedwater pump may be available.
- n. Failure to obtain auxiliary feedwater flow will eventually result in primary pressure increase to the pressurizer safety or relief valve setpressure. Normal valve operation would maintain system pressure at the valve setpoint, and may require operator intervention to depressurize the system by manually holding the valve open and

Table A.8 Footnotes (Continued)

allowing sufficient safety injection to make up loss. Westinghouse performed analyses described in WCAP-9600 indicates that the operator has time to initiate auxiliary feed flow or to open all PORVs to prevent core uncover. With the subsequent depressurization, the RCS eventually stabilizes at a pressure at which safety injection flow matches break flow.

- o. Failure of EP prevents operation of other systems.
- p. Failure of ECI may lead to core uncover without operator action. Given the definition of ECI failure in Section A.2.8 which may result in core uncover, one potential action for the operator to take is to depressurize the RCS by holding the pressurizer PORV(s) open in order to actuate the accumulators and low head safety injection pumps to recover the core.

TABLE A.9

## PROCEDURE REVIEW: STEAMLINE BREAK EVENT TREE

Function of Interest	Sequence No.	Pertinent Steps of <u>W</u> EGI's		Coverage of Reference Instructions**	
		Instruction	Step	Full/Partial*/None	
	1	E-0 E-2		X	Design Basis Event
SSR/V-0	15-19	E-2 E-0	C.7.A, C.7.B C.3.C	c	Events Beyond Design Basis
ECR	5, 12, 16 24, 28	E-2	C.5.c, Table E.2-1	a	Events Beyond Design Basis
RPS	3, 7, 10, 14 18, 22, 26	E-0	C.1.d, C.2.a C.3	a	
ECI	2, 3, 6, 7, 9, 10, 13, 14, 17, 18 21, 22, 25, 26, 29	E-0 E-2	C.1b, C.2.f, C.3.a C.5.C, C.6	a	
PPC/V-R	4-7, 11-14, 23-26	E-2 E-0	C.6 A-D, C.5.C D.1, D.5	b	
EP	31	E-0 E-2	C.2.b C.	a	
PPC/V-0	19, 30			c	
SSR/V-R	8-14	E-2	C.6.D, C.3	d	
MSI	20-26	E-0 E-2	C.4 B, C.3	a	
AFWS	27-30	E-0 E-2	C.2.e, C.3.b C.4	a	

\* Partial coverage is defined to mean contingency action has not been specified in the event that safety function which failed cannot be re-established (e.g., by manual, local or repair actions).

\*\* In review of the instructions, it is assumed that the operator has entered E-2 from E-0.

Table A.9 Footnotes

- a. Manual actuation identified as contingency action. Contingency action in the event of failure of safety function may be required.
  - b. Potential for failure not identified. ECI termination criteria will ultimately transfer to correct procedure without violation of safety limits.
  - c. Failure of total function has very low probability and need not be addressed for this event.
  - d. Reinitiation of event not specifically addressed in procedures. ECI termination and restart procedures will assure adequate coverage.
- X. Denotes full coverage for sequences.



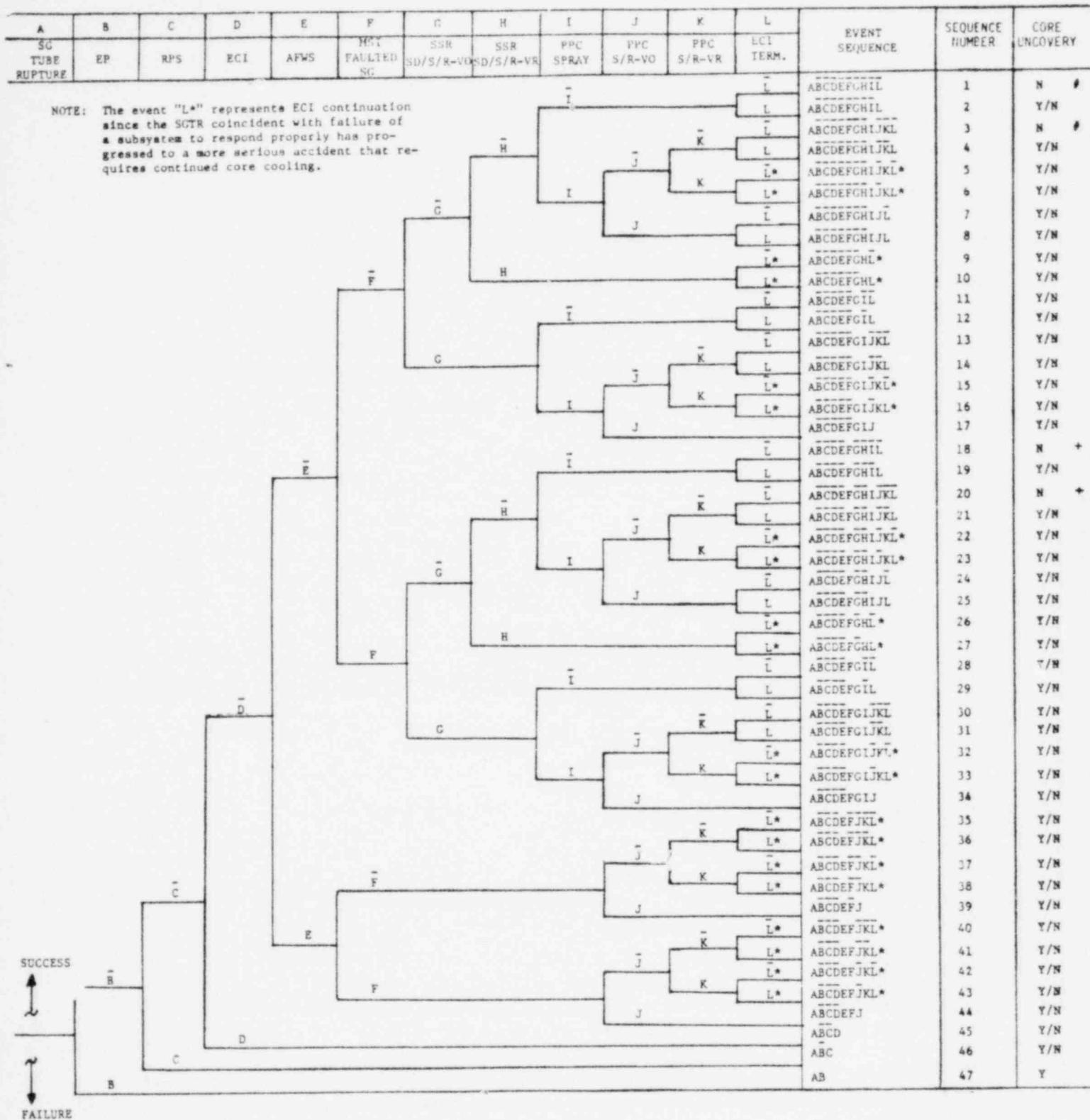


FIGURE A.5 Steam Generator Tube Rupture Event Tree - No. 1

SEQUENCE NUMBER	EVENT SEQUENCE	A	B	C	D	E	F	G	H	I	J	K	L	CORE UNCOVERY	FOOTNOTES
		SG TUBE RUPTURE	LP	RPS	ECI	AWNS	MSIV FAULTED SG	SSR SD/S/R-V0	SSR SD/S/R-VK	PPC SPRAY	PPC S/R-V0	PPC S/R-VK	ECI TERM.		
1	ABCDEFGHIJL	f									P <sub>J</sub>	P <sub>J</sub>		N	a
2	ABCDEFGHIJL	f									P <sub>J</sub>	P <sub>J</sub>	f	Y/N	c,d
3	ABCDEFGHIJKL	f								f				N	e, a
4	ABCDEFGHIJKL	f								f			f	Y/N	c,d,e
5	ABCDEFGHIJKL*	f								f		f	*	Y/N	e,g
6	ABCDEFGHIJKL*	f								f		f	f*	Y/N	h,e,g
7	ABCDEFGHIJL	f								f	f	O <sub>K</sub>		Y/N	i
8	ABCDEFGHIJL	f								f	f	O <sub>K</sub>	f	Y/N	i,j
9	ABCDEFGHI*	f						f		O <sub>I</sub>	O <sub>I</sub>	O <sub>I</sub>	*	Y/N	k
10	ABCDEFGHI*	f						f		O <sub>I</sub>	O <sub>I</sub>	O <sub>I</sub>	f*	Y/N	h,k
11	ABCDEFGHI	f						f	O <sub>H</sub>		P <sub>J</sub>	P <sub>J</sub>		Y/N	l
12	ABCDEFGHI	f						f	O <sub>H</sub>		P <sub>J</sub>	P <sub>J</sub>	f	Y/N	d,l
13	ABCDEFGHIJKL	f						f	O <sub>H</sub>	f				Y/N	l,e
14	ABCDEFGHIJKL	f						f	O <sub>H</sub>	f			f	Y/N	d,l,e
15	ABCDEFGHIJKL	f						f	O <sub>H</sub>	f		f	*	Y/N	m
16	ABCDEFGHIJKL*	f						f	O <sub>H</sub>	f		f	f*	Y/N	m,h
17	ABCDEFGHIJ	f						f	O <sub>H</sub>	f	f	O <sub>K</sub>	O <sub>K</sub>	Y/N	n,o
18	ABCDEFGHI	f					f				P <sub>J</sub>	P <sub>J</sub>		N	p
19	ABCDEFGHI	f					f				P <sub>J</sub>	P <sub>J</sub>	f	Y/N	q,d,p
20	ABCDEFGHIJKL	f					f			f				N	e,p
21	ABCDEFGHIJKL	f					f			f			f	Y/N	q,d,p
22	ABCDEFGHIJKL*	f					f			f		f	*	Y/N	g,p
23	ABCDEFGHIJKL*	f					f			f		f	f*	Y/N	h,g,p
24	ABCDEFGHIJL	f					f			f	f	O <sub>K</sub>		Y/N	r,p
25	ABCDEFGHIJL	f					f			f	f	O <sub>K</sub>	f	Y/N	q,r,p
26	ABCDEFGHI*	f					f		f	O <sub>I</sub>	O <sub>I</sub>	O <sub>I</sub>	*	Y/N	k,p
27	ABCDEFGHI*	f					f		f	O <sub>I</sub>	O <sub>I</sub>	O <sub>I</sub>	f*	Y/N	h,k,p
28	ABCDEFGHI	f					f		O <sub>H</sub>		P <sub>J</sub>	P <sub>J</sub>		Y/N	l,p
29	ABCDEFGHI	f					f		O <sub>H</sub>		P <sub>J</sub>	P <sub>J</sub>	f	Y/N	d,l,p
30	ABCDEFGHIJKL	f					f		O <sub>H</sub>	f				Y/N	d,l,p
31	ABCDEFGHIJKL	f					f		O <sub>H</sub>	f				Y/N	d,l,p
32	ABCDEFGHIJKL*	f					f		O <sub>H</sub>	f		f	*	Y/N	m,p
33	ABCDEFGHIJKL*	f					f		O <sub>H</sub>	f		f	f*	Y/N	m,h,p
34	ABCDEFGHIJ	f					f		O <sub>H</sub>	f	f	O <sub>K</sub>	O <sub>K</sub>	Y/N	n,o,p
35	ABCDEFGHI*	f				f		O <sub>E</sub>	O <sub>E</sub>		O <sub>E</sub>		*	Y/N	s
36	ABCDEFGHI*	f				f		O <sub>E</sub>	O <sub>E</sub>		O <sub>E</sub>		f*	Y/N	s,h
37	ABCDEFGHI*	f				f		O <sub>E</sub>	O <sub>E</sub>		O <sub>E</sub>		*	Y/N	s,g
38	ABCDEFGHI*	f				f		O <sub>E</sub>	O <sub>E</sub>		O <sub>E</sub>	f	f*	Y/N	s,g,h
39	ABCDEFJ	f				f		O <sub>E</sub>	O <sub>E</sub>		O <sub>E</sub>	f	O <sub>K</sub>	Y/N	t,o
40	ABCDEFJKL*	f				f	f	O <sub>E</sub>	O <sub>E</sub>		O <sub>E</sub>		*	Y/N	s,u
41	ABCDEFJKL*	f				f	f	O <sub>E</sub>	O <sub>E</sub>		O <sub>E</sub>		f*	Y/N	s,h,u
42	ABCDEFJKL*	f				f	f	O <sub>E</sub>	O <sub>E</sub>		O <sub>E</sub>	f	*	Y/N	s,g,u
43	ABCDEFJKL*	f				f	f	O <sub>E</sub>	O <sub>E</sub>		O <sub>E</sub>	f	f*	Y/N	s,g,h,u
44	ABCDEFJ	f				f	f	O <sub>E</sub>	O <sub>E</sub>		O <sub>E</sub>	O <sub>K</sub>	O <sub>K</sub>	Y/N	t,o,u
45	ABCD	f				f	O <sub>D</sub>	O <sub>D</sub>	O <sub>D</sub>		O <sub>D</sub>	O <sub>D</sub>	O <sub>D</sub>	Y/N	v
46	ABC	f		f	O <sub>C</sub>	O <sub>C</sub>	O <sub>C</sub>	O <sub>C</sub>	O <sub>C</sub>		O <sub>C</sub>	O <sub>C</sub>	O <sub>C</sub>	Y/N	w,o
47	AB	f	f	O <sub>B</sub>	Z <sub>B</sub>	O <sub>B</sub>	O <sub>B</sub>	O <sub>B</sub>	O <sub>B</sub>		O <sub>B</sub>	O <sub>B</sub>	O <sub>B</sub>	Y	x

TABLE A.10 STEAM GENERATOR TUBE RUPTURE EVENT TREE NO. 1 - SYSTEMS STATUS

Key (Table A.10):

- f - failure
- $f_N$  - dependent time-delayed failure caused by failure of "N"
- $O_N$  - does not matter; operation of function has no effect because of failure of "N"
- $P_N$  - does not matter; operation of function has no effect because of operation of "N"
- $Z_N$  - failure predicated by failure of "N"
- \*
- success is ECI continuation; f\* constitutes failure to continue safety injection
- # - sequence continues on with event tree, Figure A.6. Note that the sequence does not continue if functions that have failed in the first tree are called upon in the second
- + - sequence may continue on with event tree, Figure A.6, if faulted steam generator can eventually be isolated after repair of failed function
- Y - core uncover occurs; operator action, short of reversing initial failure(s), will not mitigate transient
- N - no core uncover occurs, unless operator acts to counter the effects of the safeguards systems
- Y/N - core uncover may occur and proper operator action may prevent it

Table A.10 - Footnotes

- a. No loss of critical function. Design basis event.
- c. Failure of operator to terminate ECI may lead to pressurization of faulted steam generator to S/R valve setpoint, with eventual filling of the faulted steam generator and subsequent water relief with potential valve failure. Operator would have  $\geq 1\text{-}1/2$  hrs, depending on break size, to terminate safety injection before filling the steam generator; he may be able to reduce primary pressure to that of the faulted steam generator by use of steam dump to the condenser (if available) or through the atmospheric relief valves in the intact loops once the faulted steam generator has been isolated.
- d. Failure to terminate ECI will prevent equilibration and may result in primary system going water solid with water relief through pressurizer S/R valves.
- e. Although utilization of normal pressurizer spray system is preferred mode of reducing primary system pressure, alternate mode is use of PORV.
- g. Failure of pressurizer PORV to reclose results in LOCA in pressurizer vapor space. Operator should attempt to isolate/regulate the PORV break.
- h. Termination of ECI results in RCS water inventory loss and may lead to core uncover and potentially to inadequate core cooling.
- i. With pressurizer spray and S/R valves unavailable, operator may be able to reduce primary pressure to that of the faulted steam generator by use of steam dump to the condenser in the intact loops. Faulted steam generator must be isolated prior to the start of the cooldown.
- j. Similar to note (c), except that failure of pressurizer S/R valves may lead to overpressurization of the RCS.

Table A.10 - Footnotes (Continued)

- k. If coincident SGTR and steambreak (steam dump, safety or relief valve failure) were to occur on the faulted steam generator, an alternative for the operator may be to hold open pressurizer PORV(s) to provide water to the containment sump for continued core cooling during recirculation phase; system depressurization would then occur.

If coincident SGTR and steambreak (steam dump, safety or relief valve failure) were to occur on the non-faulted steam generator, the operator may be required to maintain SI flow to the RCS to compensate for the resultant shrinkage.

- l. In the unlikely event of complete loss of SSR, primary and secondary side pressures increase. If pressurizer S/R valves operate normally, primary system will stabilize at valve set pressure and will result in a net loss of inventory. If sufficient time exists operator may attempt to depressurize by use of pressurizer PORV(s) before secondary side ruptures.
- m. Valve failure corresponds to action recommended to operator in note (1). Failure may yield break large enough to depressurize primary system with secondary to follow suit, if time (before rupture) permits.
- n. With the unlikely unavailability of any function to depressurize primary or secondary systems, operator action may not terminate break flow to faulted steam generator for these coincident failures. System rupture will probably occur.
- o. ECCS cannot operate against system pressures anticipated.
- p. Sequences 18-34 are similar to 1-17, respectively, except for failure to isolate faulted steam generator which would lead to increased radiological releases for sequences 18-34, when such release occurs. It is important to note that with failure to isolate, operator will be unable to meet the subcooling criterion

Table A.10 - Footnotes (Continued)

(in loops with non-faulted steam generators) for safety injection termination. In this instance, then, operator would have to be cautioned to disregard that criterion when he cannot isolate the faulted steam generator and to rely on pressurizer level and RCS pressure to decide on safety injection termination.

If the steam line isolation valve to the faulted steam generator cannot be closed, the steam line isolation valves to the other steam generators may be closed in order to isolate the affected steam generator. Steam relief can then proceed from the intact steam generators using the atmospheric steam dump without resulting in release of radioactive steam.

- q. Failure to terminate ECI leads to pressurization of secondary system to S/R valve setpoint, and filling of the steam generators at a more rapid rate than in note (c). Operator would have some time to terminate safety injection before filling secondary; he would need to utilize steam relief to reduce RCS pressure.
- r. With pressurizer spray and S/R valves unavailable, operator may be able to reduce primary pressure by utilizing steam relief to bring down secondary pressure and re-establish normal charging and let-down; however, with these coincident failures, there is increased probability of filling faulted steam generator.
- s. Failure to obtain auxiliary feedwater flow eventually results in primary pressure increase to pressurizer S/R valve setpoint. Normal valve operation would maintain system pressure at valve setpoint and would require operator intervention to depressurize the system by manually holding the valve(s) open and allow sufficient safety injection to make up loss. Operator response time calculated in WCAP-9600 for initiating auxiliary feed flow or opening all PORVs would be extended somewhat in this instance since water is being supplied to the faulted steam generator through the rupture.

Table A.10 - Footnotes (Continued)

- t. In the unlikely failure of pressurizer safety and relief valves to open, depending on location of consequential primary system rupture and ability to isolate break, proper operator action may prevent core uncover, assuming availability of ECI.
- u. Sequences 40-44 are similar to 35-39, respectively, except for failure to isolate faulted steam generator. Since in sequences 40-44 reactor coolant leaks to that generator, increased radiological releases may occur.

If the steam line isolation valve to the faulted steam generator cannot be closed, the steam line isolation valves to the other steam generators may be closed in order to isolate the affected steam generator. Steam relief can then proceed from the intact steam generators using the atmospheric steam dump without resulting in release of radioactive steam.

- v. ECI failure without operator action may lead to core uncover, and may result in inadequate core cooling; however, depressurization would minimize break flow and would give operator more time to act. Intermediate situations may exist which may permit operator action to recover core.
- w. Initiating event plus RPS failure is of sufficiently low probability that additional function failures were not considered in event tree evaluation. Due to increase in primary system pressure, core uncover may occur.
- x. Failure of EP prevents operation of other systems.

TABLE A.11 PROCEDURES REVIEW - STEAM GENERATOR TUBE RUPTURE EVENT TREE NO. 1

Function of Interest	Sequence Number	Pertinent Steps of <u>W</u> EOI's		Coverage of Reference Instructions	
		Instruction	Step	Full / Partial*/ None	
	1; 3;	E-3		a**	Design Basis Events
ECI Termination	2; 4; 8; 12; 14; 19; 21; 25; 29; 31	E-3	C.13; C.14	b	Events Beyond Design Basis
PPC S/R-VR	5; 6; 15; 16; 21; 22; 32; 33; 37; 38; 42; 43	E-0 E-3	D.1.b C.1; C.11; C.13	b,c	
SSR SD/S/R-VR	9; 10; 26; 27	E-3 E-2 E-0	C.11-C.14 C.3; C.4; C.6 D.4	b,c	
MSI Faulted SG	18-34	E-3	C.9	b	
AFWS	35-44	E-0 E-3	C.2.e; C.3.b C.6	b	
ECI	45	E-0	C.1.b; C.2.f; C.3.a	b	
RPS	46	E-0	C.1.a; C.2.a; C.3	d	
EP	47	E-0 E-3	C.2.b C.7	b	
SSR SD/S/R-VO	11-17; 28-34	E-0	C.3.c	d	
PPC S/R-VO	7; 8; 24; 25; 34; 39; 44			d	

\*Partial coverage is defined to mean contingency action has not been specified in the event that safety function which failed cannot be re-established (e.g., by manual, local, or repair actions.)

\*\*See footnotes



Table A.11 Footnotes

- a. No loss of critical function. Design basis event.
- b. Contingency action in the event of failure of safety system function may be required.
- c. In the case of multiple function failure which results in multiple events, e.g., LOCA and steam break, explicit instructions may need to be developed.
- d. Failure of total function has very low probability due to system design and need not be addressed.

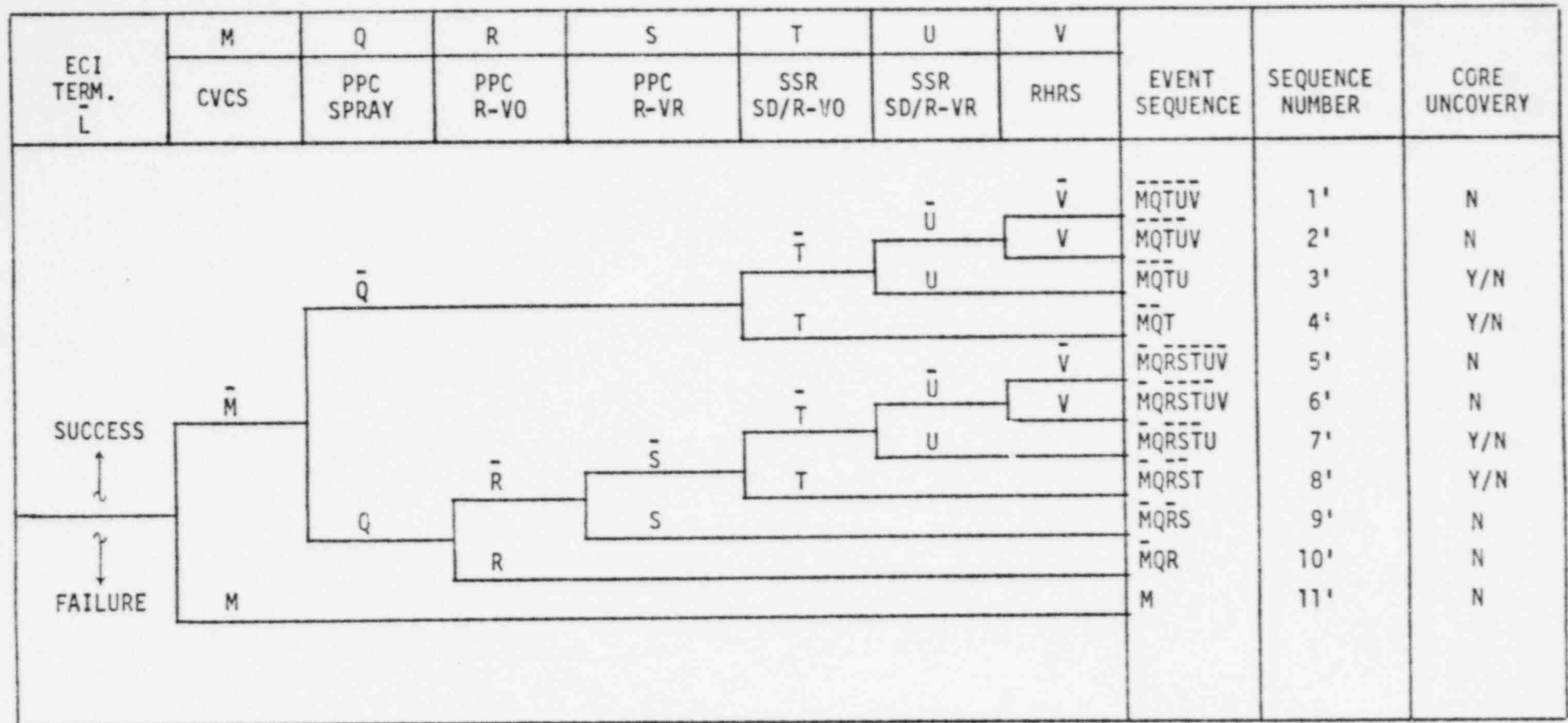


FIGURE A.6 Steam Generator Tube Rupture Event Tree - No. 2

A-20

SEQUENCE NUMBER	EVENT SEQUENCE	M	Q	R	S	T	U	V	CORE UNCOVERY	FOOTNOTES
		CVCS	PPC SPRAY	PPC R-VO	PPC R-VR	SSR SD/R-VO	SSR SD/R-VR	RHRS		
1'	$\overline{M} \overline{Q} \overline{T} \overline{U} \overline{V}$			$P_Q$	$P_Q$				N	a
2'	$\overline{M} \overline{Q} \overline{T} \overline{U} \overline{V}$			$P_Q$	$P_Q$			f	N	b
3'	$\overline{M} \overline{Q} \overline{T} \overline{U}$			$P_Q$	$P_Q$		f	$O_U$	Y/N	c
4'	$\overline{M} \overline{Q} \overline{T}$			$P_Q$	$P_Q$	f	$O_T$	$O_T$	Y/N	d
5'	$\overline{M} \overline{Q} \overline{R} \overline{S} \overline{T} \overline{U} \overline{V}$		f						N	e
6'	$\overline{M} \overline{Q} \overline{R} \overline{S} \overline{T} \overline{U} \overline{V}$		f					f	N	b,e
7'	$\overline{M} \overline{Q} \overline{R} \overline{S} \overline{T} \overline{U}$		f				f	$O_U$	Y/N	c,e
8'	$\overline{M} \overline{Q} \overline{R} \overline{S} \overline{T}$		f			f	$O_T$	$O_T$	Y/N	d,e
9'	$\overline{M} \overline{Q} \overline{R} \overline{S}$		f		f	$O_S$	$O_S$	$O_S$	N	g
10'	$\overline{M} \overline{Q} \overline{R}$		f	f	$O_{QR}$	$O_{QR}$	$O_{QR}$	$O_{QR}$	N	h
11'	M	f	$O_M$	$O_M$	$O_M$	$O_M$	$O_M$	$O_M$	N	i

## Key:

- f - failure
- $f_N$  - dependent time-delayed failure caused by failure of N
- $O_N$  - does not matter; operation of function has no effect because of failure of N
- $P_N$  - does not matter; operation of function has no effect because of operation of N
- $Z_N$  - failure predicated by failure of N
- Y - core uncovery occurs; operator action, short of reversing initial system failure(s), will not mitigate transient
- N - no core uncovery occurs, unless operator acts to counter the effects of the safeguards systems
- Y/N - core uncovery may occur and proper operator action may prevent it

TABLE A.12 Steam Generator Tube Rupture Event Tree No. 2 - Systems Status

Table A.12 - Footnotes

- a. No loss of critical function. Design basis event.
- b. Steam generator heat removal capability should be re-established while RHR equipment is repaired. Heat removal may take place via natural circulation or via forced convection flow if RCP operation criteria are satisfied. If failure occurs for a long period, RCS will tend to stabilize near saturation pressure, as faulted and non-faulted steam generators tend to equilibrate. Slight differential pressure from primary to secondary will remain in order to permit continued heat removal; in this instance there is some leakage to the faulted steam generator. Operator should attempt to maintain pressurizer level and minimize leakage. If safety injection re-initiation criteria are met, operator should re-establish SI.
- c. If coincident SGTR and steam break (steam dump or relief valve failure) were to occur on non-faulted steam generator, the operator may be required to maintain SI flow to the RCS to compensate for the resultant shrinkage; if he is able to isolate the steam break, he may be able to recover and proceed to normal residual heat removal mode.

If coincident SGTR and steam break (steam dump or relief valve failure) were to occur on the faulted steam generator which cannot be isolated, an alternative for the operator may be to hold open the pressurizer PORV(s) to provide water to the containment sump for continued core cooling during ECCS recirculation phase; if safety injection re-initiation criteria are met, operator should re-establish SI.

- d. If secondary steam dump and relief valves are unavailable on the non-faulted steam generators, the secondary side will pressurize to the safety valve set pressure; primary side will stabilize at slightly higher pressure to permit heat removal. Operator should hold system in this state until repair of function failure can be effected.

Table A.12 - Footnotes (Continued)

If secondary steam dump and relief valves are unavailable on the faulted steam generator, an alternative to depressurize the faulted steam generator would be drain back from secondary into RCS. Close attention should be paid to boron concentration in RCS.

- e. With normal and auxiliary pressurizer spray unavailable, the operator may still depressurize the primary side by use of the pressurizer PORV.
- g. If pressurizer PORV fails to reclose, RCS will depressurize with net loss of inventory. ECCS re-initiation by operator is assumed if loss of inventory is greater than normal makeup capability of CVCS.
- h. With these failures, primary pressure can only be reduced very slowly. Function failure should be repaired.
- i. If CVCS is unavailable, operator should make up water via safety injection until equipment is repaired.

TABLE A.13 PROCEDURES REVIEW: STEAM GENERATOR TUBE RUPTURE EVENT TREE NO. 2<sup>+</sup>

Function of Interest	Sequence Number	Pertinent Steps of <u>W</u> EOI's		Coverage of Reference Instructions
		Instruction	Step	Full / Partial*/ None
	1'; 5'	E-3		a**
RHRS	2'; 6'	E-3	C.24; C.27	b
SSR SD/R-VR	3'; 7'	E-3	C.18; C.19; C.23; C.25	b,c
SSR SD/R-V0	4'; 8'	E-3	C.18; C.19; C.23; C.25	d
PPC R-VR	9'	E-3	C.15-Caution C.20-Caution	b,c
CVCS	11'	E-3	C.15-Caution	b
PPC R-V0	10'	E-3	C.20	d

A-99

+ Review of Instructions begins with E-3: C.15

\* Partial coverage is defined to mean that contingency action has not been specified in the event that safety function which failed cannot be re-established (e.g., by manual, local or repair actions).

\*\* See Footnotes

Table A.13 Footnotes

- a. No loss of critical function. Design basis event.
- b. Contingency action in the event of failure of safety system function may be required.
- c. In the case of multiple function failure which results in multiple events, e.g., LOCA and steam break, explicit instructions may need to be developed.
- d. Failure of total function has very low probability due to system design and need not be addressed.

APPENDIX B  
ANALYSIS OF NON-LOCA PRE-TRIP ACCIDENTS  
(Control Event Trees)

B.1 CONTROL EVENT TREE DEFINITIONS

B.1.1 INITIATING EVENT

For the control event tree construction, a spectrum of initiating events was assumed. For example, a loss of normal feedwater accident may not result in a total loss of feedwater as shown in the FSAR but rather a slow closing of the feedwater control valve. If this sequence occurs, reactor trip on low steam generator level could be delayed sufficiently that a significant number of control interactions could occur. Thus the control event trees are constructed to provide for both the worst case and less limiting failures. This method addresses the concern that bounding analysis may not be limiting, since interactions could result in a more limiting approach to safety limits in this longer term.

B.1.2 CONTROL EVENT TREE METHODOLOGY

The purpose of this appendix is to systematically show the impact of control system interactions up until reactor trip. The concerns being addressed are: 1) Could operator or system actions in this time interval significantly affect post-trip/cool-down conditions? 2) Could these actions change transient trends to the extent that procedurally prescribed actions are inappropriate?

The first task in this effort was to combine all of the control systems into groups based on function (i.e., the function Rod Control is composed of automatic and manual control rod movement systems, control rod blocks, etc.). These groups are listed and defined in Section B.1.3. Event trees were developed for each initiating event and are provided in Section B.2.



The functions were defined as having three operating conditions for impact on the system. For example, the steam generator power-operated relief valves can fail open, fail closed or respond normally (open when required). Another example is feedwater flow control where control may be excessive, inadequate or normal (steam generator level is maintained). The event tree starts with an initiating event (see Section B.1.1). For each function three modes of operation are postulated. If a path results in a tripped condition (denoted by R in the event diagram), that branch is terminated. Review would continue in the posttrip tree. However, an assessment of the conditions existing at the time of trip is made to define if a LOCA, Steambreak, Feedbreak or Non-Loss of Primary/Secondary Coolant sequence has developed. In addition, alternate modes are reviewed to assess whether a sequence of events could develop into an accident more severe or significantly different than the initiating event. For example, if a steam generator relief valve opens during a partial loss of electrical load event and then the valve fails to close, the transient of importance to operator action is the credible steamline break transient, not the loss of load. This is significant since the operator's responses and system trends are reversed from the initiating event. Thus the potential for misoperation is significantly increased. For these paths, the trees show an exit to the transient of most importance. Thus, it is possible for an initiating event to result in several iterations of event trees until the most limiting sequence is identified. Based on these sequences, the most limiting or critical functions can be identified. It is possible that recovery from the initiating event can be achieved for some branches. This would result in a new steady state condition and is denoted by SS in the event trees.

### B.1.3 CONTROL EVENT TREE FUNCTION DEFINITIONS

The following is an explanation or definition of each of the functions listed in Table B.1 which are used in the development of the control event tree. The reasoning behind grouping different systems together in the same function is also discussed. The operation of systems in the

same function in opposing directions under certain conditions will be discussed in the specific transient sections. Manual operations, causing or preventing the functioning of each system described below, are also included.

Table B.1

Control Event Tree Functions

Pressurizer Power Operated Relief Valves (PRSZR PORV)

Steam Generator Power Operated Relief Valves (SG PORV)

Feedwater Control (FW CONT)

Rod Control (ROD CONT)

Pressurizer Level Control by Charging and Letdown (PRSZR LEV)

Pressurizer Pressure Control by Spray and Heaters (PRSZR PRS)

Steam Load Control by Turbine Throttle Valves and Steam Dump Valves  
(STM LD CONT)

B.1.3.1 Pressurizer Power Operated Relief Valves (PRSZR PORV)

Pressurizer pressure control for this function is the control of primary pressure by means of the power operated relief valves (PORV). The operation of these valves can help to maintain primary pressure for transients in which the pressure tends to increase. PORV actuation might also delay or prevent a reactor trip on high primary pressure or the actuation of pressurizer safety valves.

The three modes of operation for this function are 1) normal - the PORV's operate normally on demand to open and close as required to maintain pressure 2) failed open - the PORV's fail in the stuck open condition, causing a primary depressurization and potentially a LOCA sequence, 3) failed close - the PORV's will not open on demand and remain fully closed, which could start a primary overpressurization.

#### B.1.3.2 Steam Generator Power Operated Relief Valve (SG PORV)

This function concerns the control of steam generator pressure by means of the steam generator PORV's. It also augments the steam dump system in providing a means of heat removal from the secondary. Loss of both steam dump and the PORV function would require reliance on the steam generator safety valves for steam relief. Inadvertent actuation of the PORV's could initiate a cooldown transient. Actuation of the PORV's can help to maintain steam pressure below the safety limits and reduce the need for steam generator safety valve actuation.

The three modes of operation for this function are 1) normal - the PORV's operate normally on demand to open and close as required to maintain steam pressure, 2) failed open - the PORV's fail in the stuck open condition, potentially causing a primary cooldown event similar to a steambreak, and 3) failed close - the PORV's will not open on demand and remain fully closed, which could lead to reliance on steam generator safety valves for ultimate steam relief.

#### B.1.3.3 Feedwater Control (FW CONT)

For this function feedwater control consists of maintaining a secondary heat sink via the main and auxiliary feedwater control systems. Excessive feedwater flow via a feedwater control valve malfunction, for example, can initiate a cooldown transient. Bypass of a feedwater heater chain could have a similar effect. A decrease in or termination of feedwater flow could lead to a heatup event with the potential for loss of heat sink.

The three modes of operation of this function are 1) normal - the feedwater control system operates normally to maintain steam generator inventory at the programmed level, 2) excessive - the control system provides excessive feedwater which can lead to a cooldown event, and 3) inadequate - the control system provides insufficient inventory in the steam generators to maintain a secondary heat sink.

#### B.1.3.4 Rod Control (ROD CONT)

This function includes the operation of the automatic rod control system, manual rod control, and rod withdrawal blocks. Automatic and manual rod control can function to alleviate a slow heatup transient where rod motion can minimize any increase in  $T_{AVG}$ . Switching to manual control may alleviate an automatic rod control misoperation such as a rod withdrawal. A rod withdrawal block could halt any further rod withdrawal during an overpower transient on a high nuclear flux or over-temperature signal before a reactor trip occurs.

The three modes of operation for this function are 1) normal - the rod control system operates as designed to maintain primary coolant temperature, the rod blocks can function to limit overpower transients, or switching to manual control can alleviate control system misoperation, 2) overcompensate - too much position reactivity is inserted into the core via automatic or manual operation of the rod control system, and 3) undercompensate - the rod control system does not compensate for primary coolant temperature swings or the rods are in manual operation and no action is taken.

#### B.1.3.5 Pressurizer Level Control By Charging and Letdown (PRSZR LEV)

For this function the chemical and volume control system (CVCS) controls primary inventory through charging and letdown, both of which can have opposite effects under different conditions. The charging operation can help to maintain inventory during a primary depressurization event. Conversely excessive charging during a pressure increase or heatup event could tend to overpressurize the primary. The letdown operation can

help to maintain proper primary inventory during a heatup or pressurization event. Excessive letdown during a depressurization event could aggravate the transient. Charging and letdown are also important for insuring the effectiveness of pressurizer pressure control. The failure of the CVCS to operate properly could eliminate or reduce the effectiveness of pressurizer heaters or spray. Event trees which are affected by CVCS operation will specify which mode of operation is of importance for operator decision making.

The three modes of operation for this function are 1) normal - charging and letdown operate normally to maintain the programmed primary inventory, 2) excessive - primary inventory becomes excessive because of too much charging versus letdown, possibly leading to primary overpressurization and water relief from the pressurizer, and 3) deficient - primary inventory decreases because of too much letdown versus charging, possibly leading to primary depressurization.

#### B.1.3.6 Pressurizer Pressure Control By Spray and Heaters (PRSZR PRS)

Pressurizer pressure control for this function is the control of primary pressure by means of pressurizer heaters and spray.

The heaters may act to maintain primary pressure during transients in which the pressure tends to decrease. The functioning of heaters and spray may depend on the correct operation of other functions such as charging and letdown by the CVCS. Pressurizer spray may act to control pressure for cases where the pressure trends are downward.

The three modes of operation for this function are 1) normal - heaters and spray are available and function properly to maintain the nominal pressure, 2) over pressurization - heaters operate excessively and spray does not come on or is not available, resulting in primary overpressurization, and 3) depressurization - spray operates excessively and heaters don't function or aren't available, resulting in primary depressurization.

### B.1.3.7 Steam Load Control By Turbine Throttle Valves and Steam Dump Valves (STM LD CONT)

This function consists of controlling the plant steam load by means of manual turbine load changes, automatic turbine runback, and the steam dump system. The operator can determine the need for a load change and manually adjust the load via the turbine throttle valves. Automatic turbine runback will reduce turbine load on a high overtemperature signal possibly before a reactor trip.

The function of steam dump control serves to augment the reactor load when turbine load is reduced or lost. It also supplies a means of heat removal from the secondary if needed before and after a reactor trip. Inadvertent actuation of steam dump initiate a cooldown transient. Steam dump can be controlled on either average primary temperature or secondary steam pressure.

The three modes of operation for this function are 1) normal - steam load is controlled as designed through the turbine control system and steam dump, 2) failed open - excessive steam flow through the turbine throttle valves or steam dump potentially results in a cooldown transient, and 3) failed closed - loss of the turbine or steam dump will require some other system such as the steam generator PORV's to maintain heat dissipation capability.

## B.2 CONTROL EVENT TREE DESCRIPTIONS

This section presents a discussion of the control event trees for the transients listed in Table B.2. These transients are the events specified in Section 15 of the Final Safety Analysis Report (FSAR). For each event a transient description is provided which briefly discusses the nature and cause of the event. The control event tree diagram is shown for each transient. The effects of the operation of the control functions defined in Section B.2 on the course of each transient are briefly described in tabular format.

Control event trees are not presented for some of the Section 15 transients because they are covered by the event trees of other transients or they do not apply. Feedwater system malfunctions causing a reduction in feedwater temperature and an excessive increase in secondary steam flow are covered by the event tree for a spectrum of main steamline breaks. The effect of the operation of the control functions defined in Section B.2 would be similar for these three transients all of which are essentially an increase in secondary load. Loss of nonemergency AC power to the plant auxiliaries is covered by the event trees of other transients which would result from such an event such as loss of reactor coolant flow and loss of normal feedwater.

Uncontrolled rod cluster control assembly (RCCA) bank withdrawal from a subcritical or low startup condition and a single RCCA withdrawal are both covered by the event tree for an uncontrolled RCCA bank withdrawal at power event. All three events are power excursions in which the control functions defined in Section B.2 would have essentially the same effect.

A statically misaligned RCCA is not addressed since this transient would not be expected to result in either a reactor trip or a violation of any core safety limits. A dropped RCCA and a dropped RCCA bank are not addressed. For plants whose protection system design provides an immediate reactor trip on these events, there would be no control function interactions. For plants whose design does not provide an immediate reactor trip the effect of the control functions on the course of these two events would be covered by the event tree for the RCCA bank withdrawal at power.

Inadvertent loading of a fuel assembly into an improper position is not addressed since the effects are either detectable during startup physics testing or are inconsequential. Chemical and volume control system malfunction that increases reactor coolant inventory is not treated since it is covered by boron dilution and inadvertent operation of ECCS during power operation.

TABLE B.2

CONTROL EVENT TREE TRANSIENTS

Feedwater System Malfunctions Causing a Reduction in Feedwater Temperature

Feedwater System Malfunctions Causing an Increase in Feedwater Flow

Excessive Increase in Secondary Steam Flow (Excessive Load Increase)

A Spectrum of Main Steamline Breaks

Loss of External Electrical Load/Turbine Trip

Loss of Nonemergency AC Power to the Plant Auxiliaries (Loss of Offsite Power)

Loss of Normal Feedwater

Feedwater System Pipe Break

Loss of Forced Reactor Coolant Flow (Complete and Partial)/Locked Rotor

Uncontrolled Rod Cluster Control Assembly (RCCA) Bank Withdrawal From a Subcritical or Low Startup Condition

Uncontrolled Rod Cluster Control Assembly Bank Withdrawal at Power

Rod Cluster Control Assembly Misoperation (Including a dropped RCCA, a dropped RCCA Bank, a statically misaligned RCCA, and withdrawal of a single RCCA)

Startup of an Inactive Reactor Coolant Loop at an Incorrect Temperature

Chemical and Volume Control System Malfunction That Results in a Decrease in Boron Concentration in the Reactor Coolant (Boron Dilution)

Inadvertent Loading of a Fuel Assembly Into an Improper Position

Spectrum of Rod Cluster Control Assembly Ejection Accidents

Inadvertent Operation of ECCS During Power Operation

Chemical and Volume Control System Malfunction That Increases Reactor Coolant Inventory

Inadvertent Opening of a Pressurizer Safety or Relief Valve

Steam Generator Tube Rupture

Loss of Coolant Accidents



## B.2.1 FEEDWATER SYSTEM MALFUNCTIONS CAUSING AN INCREASE IN FEEDWATER FLOW

### B.2.1.1 Transient Description

Additions of excessive feedwater will cause an increase in core power by decreasing reactor coolant temperature. Such transients are attenuated by the thermal capacity of the secondary plant and of the RCS. The overpower-temperature protection (neutron overpower, overtemperature, and overpower delta-T trips) prevents any power increase which could violate core safety criteria.

An example of excessive feedwater flow would be a full opening of a feedwater control valve due to a feedwater control system malfunction or an operator error. At power this excess flow causes a greater load demand on the RCS due to increased subcooling in the steam generator. With the plant at no-load conditions, the addition of cold feedwater may cause a decrease in RCS temperature and, thus, a reactivity insertion due to the effects of the negative moderator coefficient of reactivity.

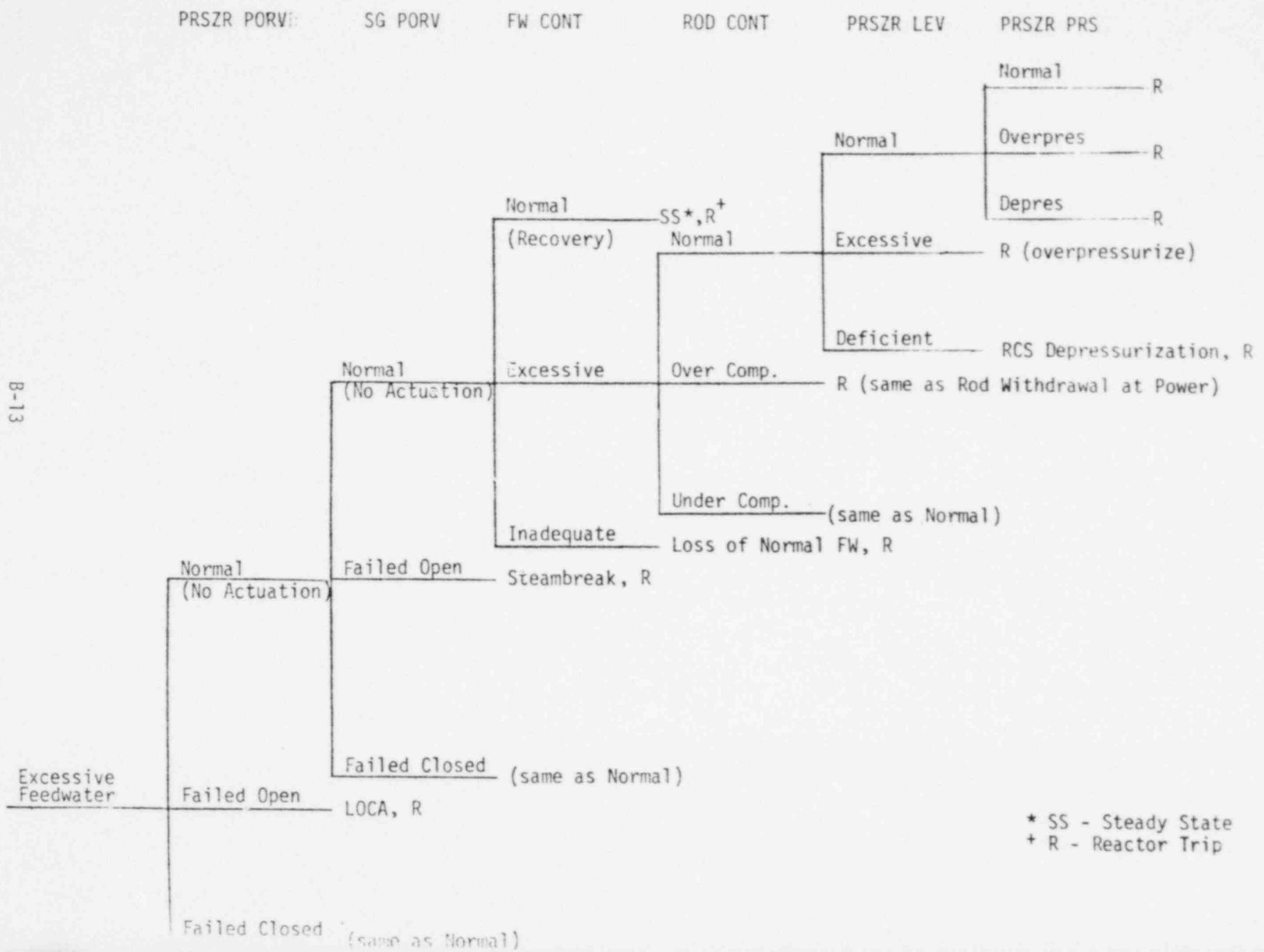
Continuous addition of excessive feedwater is prevented by the steam generator high-high level trip, which closes the feedwater isolation valves.

An increase in normal feedwater flow is classified as an ANS Condition II event, a fault of moderate frequency.

### B.2.1.2 Discussion of Control Event Tree

The control event tree for the addition of excessive feedwater is shown in Figure B.2.1-1. The control functions used in the tree and their effect on the transient are shown in Table B.2.1-1. The functions not included in the tree and the reasons for not using them are shown in Table B.2.1-2.

FIGURE B.2.1-1  
EXCESSIVE FEEDWATER EVENT



B-13

TABLE B.2.1-1

DECISION POINTS FOR EXCESSIVE FEEDWATER

<u>Function</u>	<u>Discussion</u>
PRSZR PORV	Would not be expected to actuate since pressure doesn't increase significantly. FAILED CLOSED is same as NORMAL mode. FAILED OPEN leads to LOCA event.
SG PORV	Would not be expected to actuate since turbine carries the load until trip. FAILED CLOSED is same as NORMAL mode. FAILED OPEN leads to Steambreak event.
FW CONT	Recovery from transient may lead to new steady state (SS) or reactor trip if recovery too late. Transient would continue under EXCESSIVE mode. INADEQUATE mode would lead to loss of normal feed-water (LONF) event.
ROD CONT	NORMAL mode would tend to increase $T_{avg}$ after initial cooldown. OVER COMPENSATE mode would lead to rod withdrawal at power (RWAP) event. UNDER COMPENSATE or no rod movement would lead to essentially same results as NORMAL mode.
PRSZR LEV	NORMAL mode would maintain appropriate pressurizer level. EXCESSIVE mode would lead to reactor trip on over-pressurization. DEFICIENT mode could lead to depressurization.
PRSZR PRS	All modes would lead to reactor trip, but possibly on different initiating signals.

TABLE B.2.1-2

FUNCTIONS NOT USED FOR EXCESSIVE FEEDWATER EVENT TREE

<u>Function</u>	<u>Discussion</u>
STM LD CONT	Effects of operation of this function would be the same as steam generator PORV functioning.

## B.2.2 A SPECTRUM OF MAIN STEAMLIN BREAKS

### B.2.2.1 Transient Description

Excessive steam releases from the secondary system cause an increase in the heat extraction rate from the reactor coolant system, resulting in a reduction of primary system temperature and pressure. Through control systems or through the inherent load following nature of an under-moderated PWR, core power will increase in an effort to equalize the thermal load caused by the steam leak. The overpower-temperature protection (neutron overpower, overtemperature and overpower delta-T trips) prevents power increases which could violate core safety criteria while the steamline break protection (low steamline pressure safety injection (SI) and steamline isolation, low pressurizer pressure SI) provide immediate trips for large breaks. Furthermore, for breaks occurring inside containment, various containment pressure signals provide reactor trip, safety injection, steamline isolation and other containment system actuations.

Breaks of various sizes at different locations may be postulated to occur in the main steam system. For example, a steamline break having a one square foot area could occur on the main steam header, outside containment. The incremental steam load would cause a rapid primary and secondary depressurization and cooldown. If the plant is at full power, a power increase could result due to the cooldown in the presence of a large negative temperature coefficient of reactivity (end of life). The reactor is tripped on overpower signals or on low steamline pressure (SI). If the plant is at hot shutdown, sufficient cooldown could occur to allow a return to criticality.

A second example of a steamline break would be a single failed open steam dump, steam generator safety or steam generator relief valve. Because this "break" is small, plant control systems may be capable of maintaining pressurizer pressure, pressurizer level, steam generator level and reactor power below protection system setpoints, establishing a new steady state condition.

Steamline breaks may be classified as an ANS Condition II, III, or IV event. The failed open safety, relief and steam dump valves are Condition II events, faults of moderate frequency. Actual pipe ruptures are classified as Condition III or Condition IV events, depending on their size.

#### B.2.2.2 Discussion of Control Event Tree

The control event tree for pretrip events for the steamline break transients is shown in Figure B.2.2-1. The control functions used in the tree and their effect on the transient are shown in Table B.2.2-1. The functions not included in the tree and the reasons for not using them are shown in Table B.2.2-2.

FIGURE B.2.2-1

SPECTRUM OF STEAMLINE BREAKS

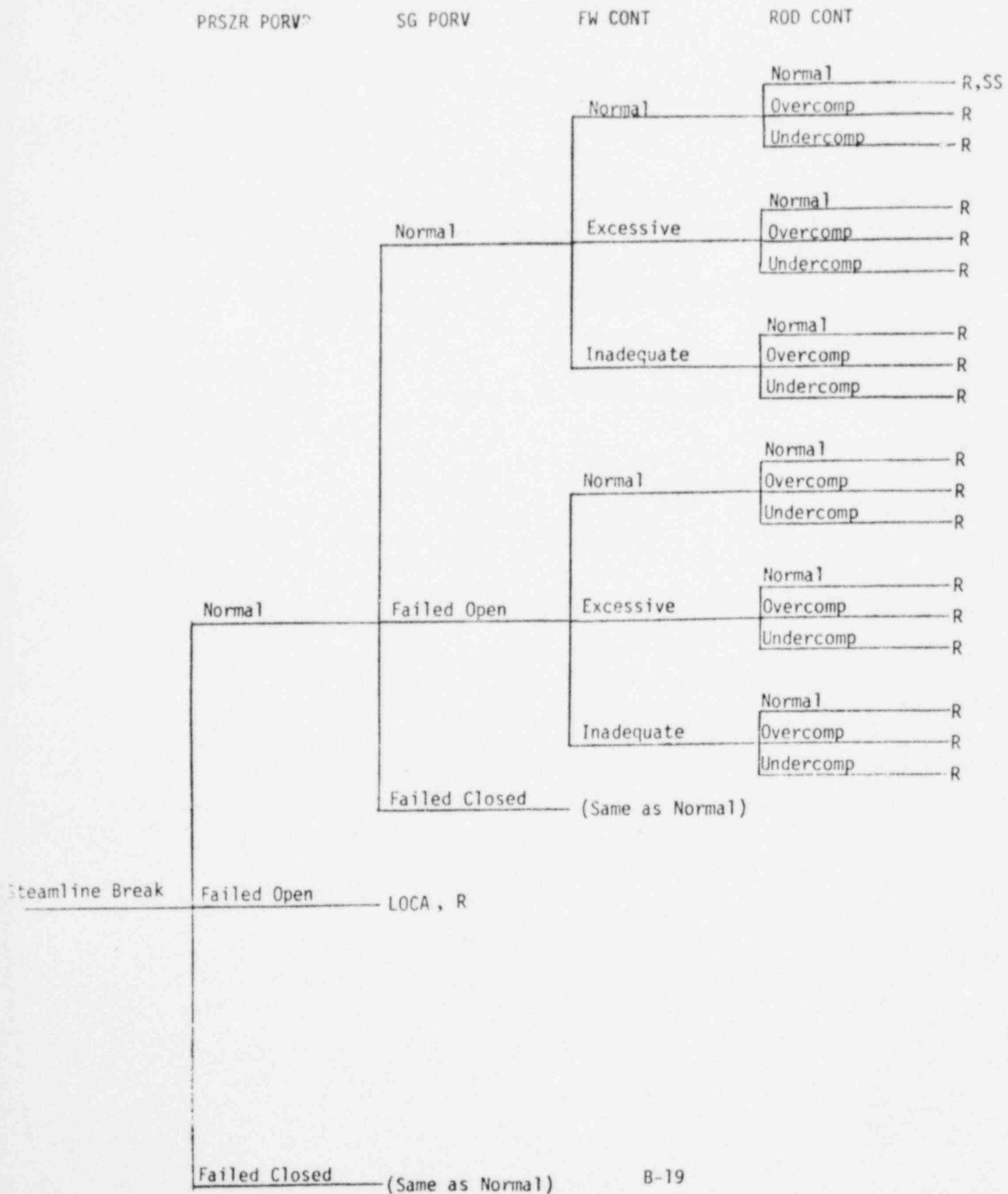


TABLE B.2.2-1

DECISION POINTS FOR A SPECTRUM OF MAIN STEAMLINE BREAKS

<u>Function</u>	<u>Discussion</u>
PRSZR PORV	Would not be expected to actuate since pressure is expected to decrease for all cases, pretrip. FAILED closed would be equivalent to NORMAL mode. FAILED open leads directly to a LOCA event, discussed by a different pretrip event tree. This case is considered only because of possible control system-environment interaction for breaks inside containment.
SG PORV	Would not be expected to actuate since pressure is expected to decrease for all cases, pretrip. FAILED closed would be equivalent to NORMAL mode. FAILED open has little effect on the pre trip steamline break events but could lead to a nonstandard precondition for post trip conditions. This case is considered only due to possible control system-environment interaction for breaks outside containment.
FW CONT	This function is only considered for <u>very</u> small breaks where recovery from the transient is possible. Transient would continue for EXCESSIVE mode, at a slightly greater rate. INADEQUATE mode is the expected mode for the majority of steamline break sizes. EXCESSIVE mode is considered only as a consequence of control system-environment interaction for breaks inside containment.
ROD CONT	NORMAL mode (automatic) could produce a new steady state for very small break sizes, or a safety actuation. Other modes should result in safety actuation.

TABLE B.2.2-2

FUNCTIONS NOT USED FOR A SPECTRUM OF MAIN STEAMLINE BREAKS

<u>Function</u>	<u>Discussion</u>
PRSZR LEV	Operation of this function does not significantly change the course of events for this transient.
PRSZR PRS	Operation of this function does not significantly change the course of events for this transient.
STM LD CONT	Operation of this function would only tend to make one break size appear to be another break size.



## B.2.3 Loss of External Electrical Load/Turbine Trip

### B.2.3.1 Transient Description

Major load loss on the plant can result from loss of external electrical load or from a turbine trip. For either case off site power is available for the continued operation of plant components such as the reactor coolant pumps.

For a turbine trip, the reactor would be tripped directly (unless below approximately 10 percent power) from a signal derived from the turbine autostop pressure (Westinghouse Turbine) and turbine stop valves. The automatic steam dump system would accommodate the excess steam generation. Reactor coolant temperatures and pressure do not significantly increase if the steam dump system and pressurizer pressure control system are functioning properly. If the turbine condenser was not available, the excess steam generation would be dumped to atmosphere.

For a loss of external electrical load without subsequent turbine trip, no direct reactor trip signal would be generated. Plants with full load rejection capability would be expected to continue without a reactor trip. Plants with lesser load rejection capability would be expected to trip from the Reactor Protection System. A continued steam load of approximately 5 percent would exist after total loss of external electrical load because of the steam demand of plant auxiliaries.

In the event the steam dump valves fail to open following a large loss of load, the steam generator safety valves may lift and the reactor may be tripped by the high pressurizer pressure signal, the high pressurizer water level signal or the over-temperature  $\Delta T$  signal. The steam generator shell side pressure and reactor coolant temperatures will increase rapidly. The pressurizer safety valves and steam generator safety valves are, however, sized to protect the Reactor Coolant System and steam generator against overpressure for all load losses without assuming the operation of the steam dump system, pressurizer spray, pressurizer power operated relief valves, automatic rod cluster control assembly control nor direct reactor trip on turbine trip.

### B.2.3.2 Discussion of Control Event Tree

The control event tree for loss of load is shown in Figure B.2.3-1. All the control functions were used in the tree and their effect on the transient is shown in Table B.2.3-1.

Figure B.2.3-1

LOSS OF EXTERNAL ELECTRICAL LOAD/TURBINE TRIP

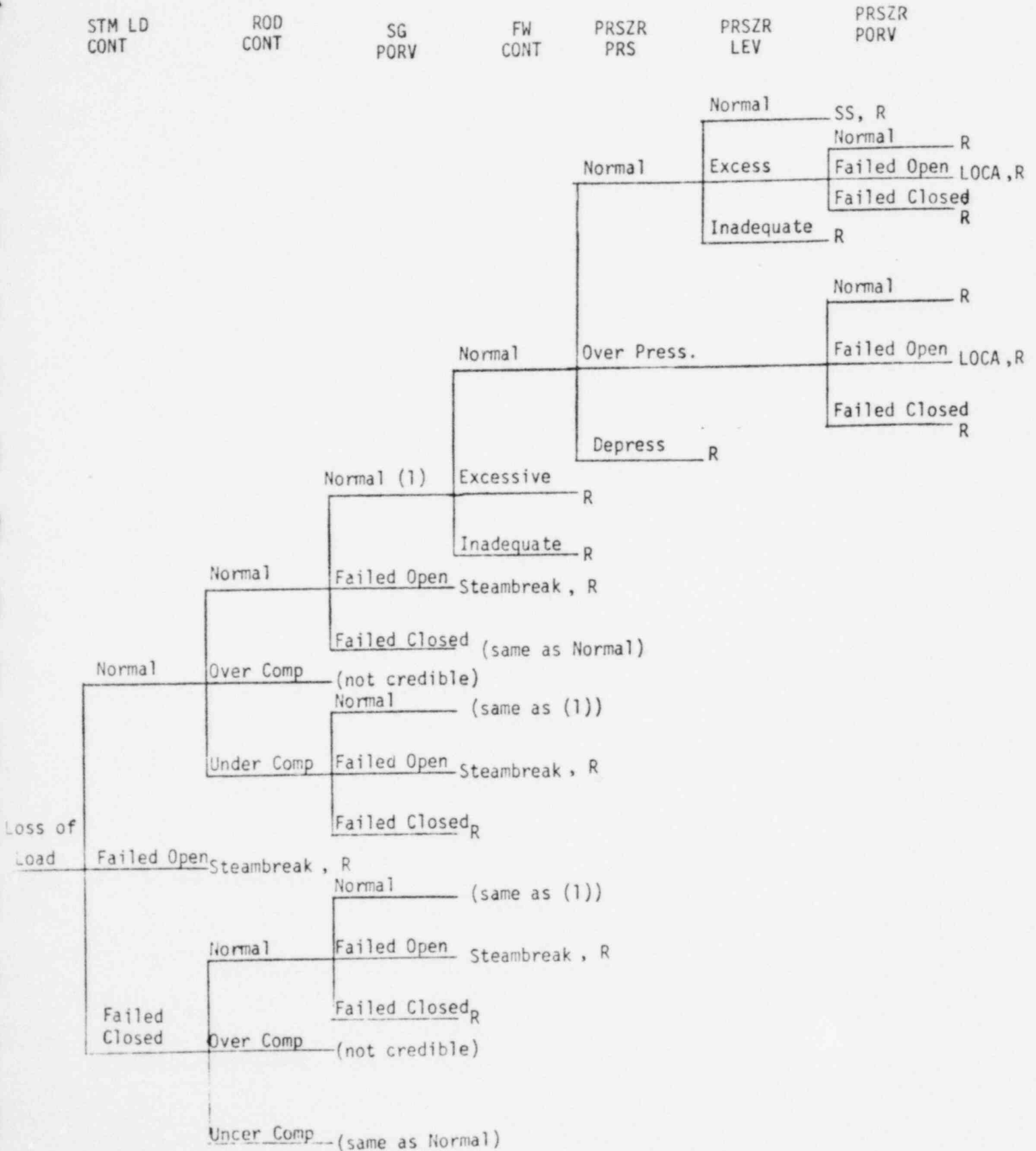


TABLE B.2.3-1

DECISION POINTS FOR A LOSS OF EXTERNAL ELECTRICAL  
LOAD/TURBINE TRIP

<u>Function</u>	<u>Discussion</u>
STM LD CONT	Steam dump assumes the load under NORMAL mode. FAILED OPEN mode leads to steambreak. FAILED CLOSED mode will lead most likely to a reactor trip since secondary heat removal has been interrupted.
ROD CONT	NORMAL mode may control primary temperature and power if initial power imbalance is not too large or if STM LD CONT functions properly. OVER COMPENSATE mode is not credible. If steam dump fails closed UNDER COMPENSATE mode will be the same as NORMAL mode and a new steady state will be difficult to achieve without a reactor trip. If steam dump functions properly UNDER compensate mode won't be as likely to result in reactor trip.
SG PORV	NORMAL mode if required, will assist in taking up load. FAILED OPEN mode will lead to steambreak. FAILED CLOSED mode will most likely result in reactor trip unless the steam dump functions properly and the rod control system maintains the proper primary temperature.
FW CONT	NORMAL mode will maintain appropriate steam generator level. EXCESSIVE mode will overflow steam generator and result in reactor trip. INADEQUATE mode will empty steam generator and result in reactor trip.
PRSZR PRS	NORMAL mode will maintain nominal primary pressure. OVERPRESSURIZATION mode will increase primary pressure towards relief valve setpoint or reactor trip. DEPRESSURIZATION mode will decrease primary pressure until reactor trip results.
PRSZR LEV	NORMAL mode will maintain inventory in pressurizer. EXCESSIVE mode will tend to fill pressurizer and result in reactor trip. DEFICIENT mode will tend to empty pressurizer and result in reactor trip.

TABLE B.2.3-1 (Continued)

DECISION POINTS FOR A LOSS OF EXTERNAL ELECTRICAL  
LOAD/TURBINE TRIP

<u>Function</u>	<u>Discussion</u>
PRSZR PORV	NORMAL mode will open and close as required to relieve pressure. FAILED OPEN mode will lead to LOCA. FAILED CLOSED mode will result in reactor trip.

## B.2.4 LOSS OF NORMAL FEEDWATER FLOW

### B.2.4.1 Transient Description

A loss of normal feedwater (from pump failures, valve malfunctions, or loss of offsite AC power) results in a reduction in capability of the secondary system to remove the heat generated in the reactor core. If an alternative supply of feedwater were not supplied to the plant, core residual heat following reactor trip would heat the primary system water to the point where water relief from the pressurizer would occur, resulting in a substantial loss of water from the Reactor Coolant System (RCS).

Reactor trip and auxiliary feedwater initiation occurs on a low steam generator water level in a single steam generator. The steam generator power-operated relief valves are used to dissipate the residual decay heat. The primary side responds to the loss of heat removal capability with increased temperatures and pressures prior to reactor trip. Following the loss of feedwater flow to at least one steam generator numerous control systems will attempt to mitigate the consequences of the loss of heat sink prior to reactor trip. However, no system will prevent a reactor trip from occurring.

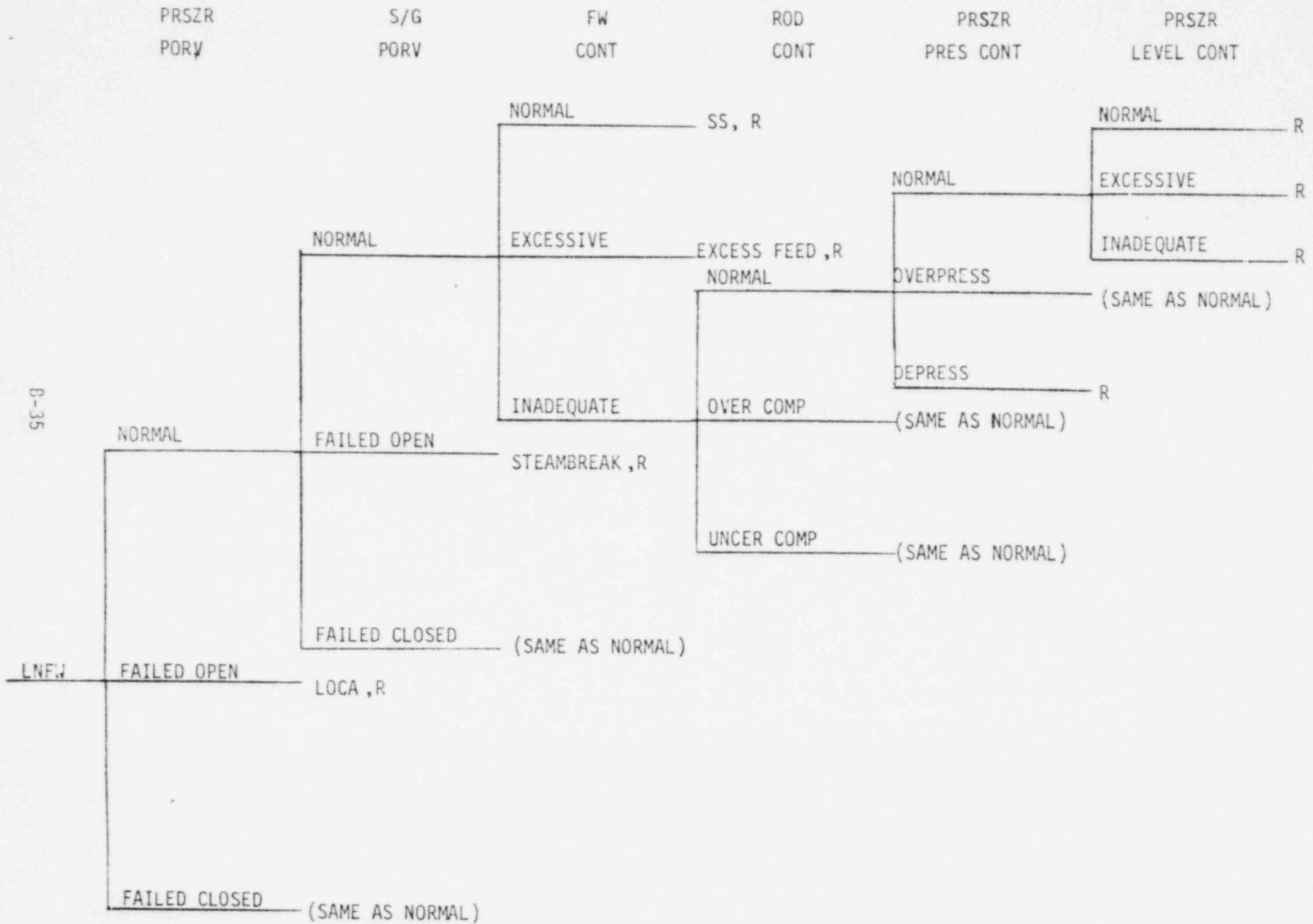
A loss of normal feedwater is classified as an ANS Condition II event, fault of moderate frequency.

### B.2.4.2 Discussion of Control Event Tree

The control system event tree for loss of feedwater flow is shown in Figure B.2.4-1. The control functions used in the tree and their effects on the transient are shown in Table B.2.4-1. The functions not included in the tree and the reasons for not using them are shown in Table B.2.4-2.

Figure B.2.4-1

LOSS OF NORMAL FEEDWATER



B-35

TABLE B.2.4-1

DECISION POINTS FOR LOSS OF NORMAL FEEDWATER

<u>Function</u>	<u>Discussion</u>
PRSZR PORV	<p>NORMAL: The pressurizer PORV would not be expected to open before a reactor trip.</p> <p>FAILED OPEN: Leads to a LOCA event.</p> <p>FAILED CLOSED: Same as the NORMAL mode.</p>
SG PORV	<p>NORMAL: Would not be expected to actuate before a reactor trip.</p> <p>FAILED OPEN: Leads to a Steambreak event.</p> <p>FAILED CLOSED: Same as the NORMAL mode.</p>
FW CONT	<p>NORMAL mode: Recovery from the transient to a new steady-state might be possible, but a reactor trip may still occur.</p> <p>INADEQUATE mode: The initiating event is unaltered.</p> <p>EXCESSIVE mode: This mode could lead to an excessive feedwater event, but most likely the initiating event (loss of feedwater) would not be altered.</p>
ROD CONT	<p>NORMAL: The rod control system may adequately compensate for the primary side transient.</p> <p>OVERCOMPENSATES: Would lead to control rod insertion, the effect of which would be negligible prior to reactor trip.</p> <p>UNDERCOMPENSATES: The severity of the temperature transient would increase, however, the basic trend is not affected leading to results similar to "NORMAL" compensation.</p>
PRSZR PRS	<p>NORMAL: Pressurizer spray functions to try to limit the primary pressure increase.</p> <p>OVERPRESSURIZATION: Prior to reactor trip the pressurizer control system (heaters) would have a very small effect on the transient.</p> <p>DEPRESSURIZATION: Excessive pressurizer spray could cause a depressurization with a resulting reactor trip.</p>
PRSZR LEV	<p>Prior to reactor trip on loss of normal feedwater the pressurizer level control has negligible impact.</p>



TABLE B.2.4-2

FUNCTIONS NOT USED FOR A LOSS OF NORMAL FEEDWATER

<u>Function</u>	<u>Discussion</u>
STM LD CONT	Prior to reactor trip on loss of normal feedwater the steam demand will have only a minor effect on the transient.

## B.2.5 FEEDWATER SYSTEM PIPE BREAK

### B.2.5.1 Transient Description

A feedwater line rupture reduces the ability to remove heat generated by the core from the RCS. Feedwater flow to the steam generators could be reduced. Since feedwater is subcooled, its loss may cause reactor coolant temperatures to increase prior to reactor trip. Fluid in the steam generator may be discharged through the break and would then not be available for decay heat removal after trip. The break may be large enough to prevent the addition of any main feedwater to the steam generators. Depending upon the size of the break and the plant operating conditions at the time of the break, the break could cause either a RCS cooldown (by excessive energy discharge through the break) or a RCS heatup.

For a small feedbreak normal plant control systems are capable of maintaining nominal or near nominal operating conditions. An intermediate size line rupture is lower bounded by those sizes in which the normal plant control systems are unable to maintain approximate nominal plant operating conditions and upper bounded by those sizes in which the protective functions do not occur within approximately five minutes following initiation of the event. The double ended main feedline rupture system response is characterized by a rapid decrease in steam generator water level in at least one steam generator. After the low or low-low water level setpoint is reached in one steam generator, a reactor trip occurs and auxiliary feedwater is initiated.

Numerous control system functions can be actuated to mitigate the consequences of the accident for small and intermediate sized breaks. For double ended feedline ruptures the control functions will be insufficient to prevent a rapid reactor trip on low steam generator level.

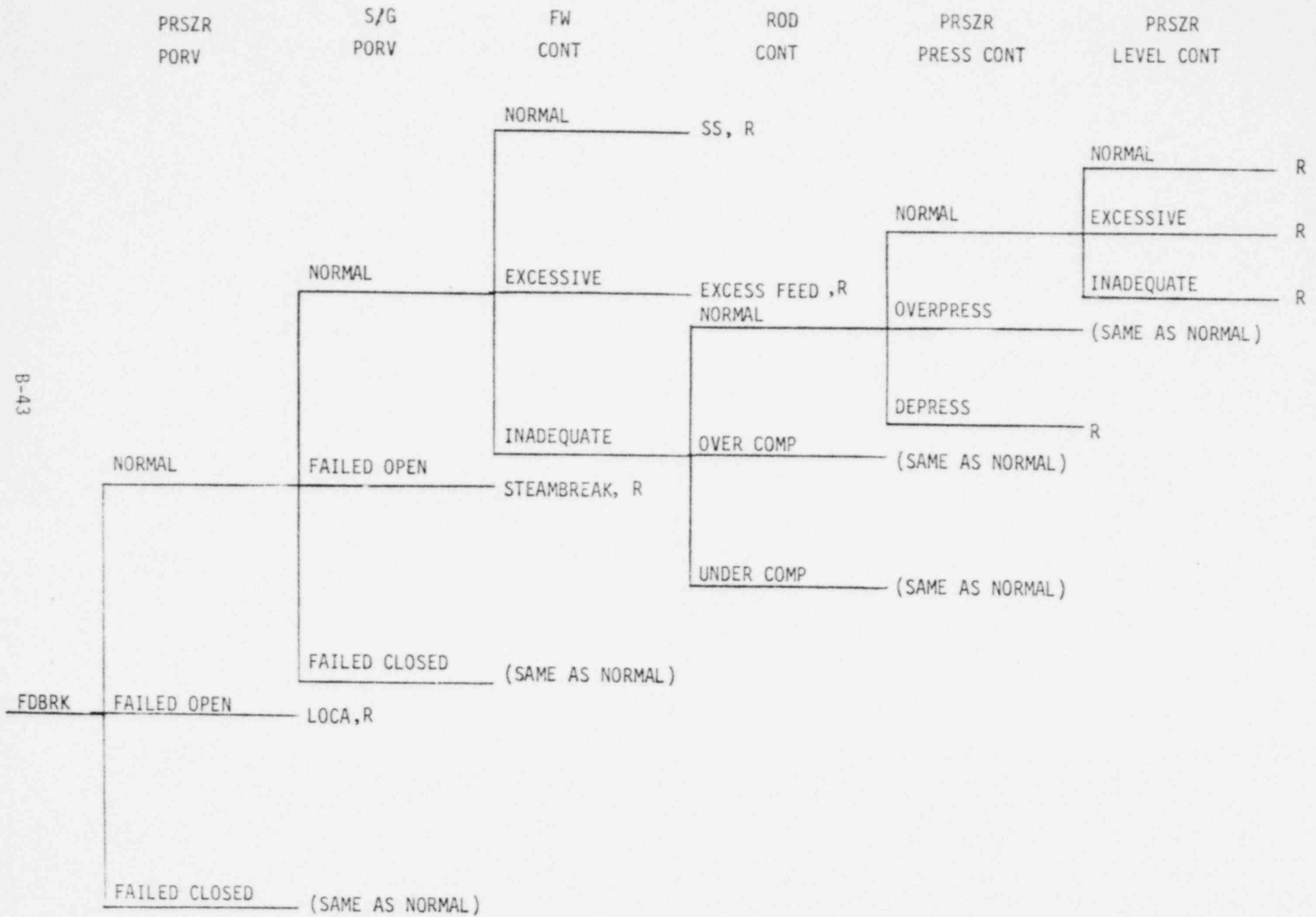
#### B.2.5.2 Discussion of Control Event Trees

The control system event tree prior to reactor trip for a feedline rupture is shown in Figure B.2.5-1. The control functions used in the tree and their effect on the transient are shown in Table B.2.5-1. The functions not included in the tree and the reasons for not using them are shown in Table B.2.5-2.

The feedline rupture transients are significantly different in many aspects depending on the design of the steam generator. Therefore, the following discussion is divided into two broad design categories, "feeding" and "preheat," and addressed separately when necessary. The control function event trees, however, are the same for both designs.

Figure B.2.5-1

FEEDWATER SYSTEM PIPE BREAK



B-43

TABLE B.2.5-1

FEEDWATER SYSTEM PIPE BREAK

<u>Function</u>	<u>Discussion</u>
PRSZR PORV	<p>NORMAL: Feeding - The pressurizer PORVs would not be actuated prior to reactor trip since the primary system pressure does not increase. Preheat - The PORV would be actuated for large and intermediate sized breaks but not for small breaks. FAILED OPEN: Leads to a LOCA event FAILED CLOSED: Feeding - Since the PORVs are not expected to actuate this is the same as the NORMAL mode. Preheat - Would increase the severity of the pressure transient for large and intermediate sized breaks but not change the trend of increasing pressure; same as NORMAL mode for small breaks.</p>
	<p>NOTE: A feedline rupture inside containment could cause an environment resulting in a consequential failure of a PORV transmitter or controller.</p>
SG PORV	<p>NORMAL: Feeding - The steam pressure decreases until time of reactor trip so these valves would not be expected to actuate. Preheat - The steam pressure increases until time of reactor trip, however, not sufficiently to actuate the PORVs. FAILED CLOSED: Since the PORVs are not expected to actuate this is the same as the NORMAL mode. FAILED OPEN: Leads to a steambreak event.</p>
	<p>NOTE: A feedline rupture outside containment could cause an environment resulting in a consequential failure of a PORV.</p>
FW CONT	<p>NORMAL: The feedwater control system may be able to compensate for small break flows, but a reactor trip may still occur. EXCESSIVE: Failure of the control system overcompensate for break flow on small breaks; same results as an excessive feedwater event. INADEQUATE: The feedwater control system fails to deliver flow demanded of it or functions normally but cannot compensate for break flow.</p>

TABLE B.2.5-1 (cont)

DECISION POINTS FOR FEEDWATER SYSTEM PIPE BREAK

<u>Function</u>	<u>Discussion</u>
ROD CONT	<p>NORMAL: The rod control system may adequately compensate for the primary side transient but only for small breaks.</p> <p>OVERCOMPENSATES: Would lead to control rod insertion, the effect of which would be negligible prior to reactor trip.</p> <p>UNDERCOMPENSATES: Would lead to essentially the same results as NORMAL.</p>
	<p>NOTE: Temperature transients for feedline rupture events are small for all break sizes prior to reactor trip.</p>
PRSZR PRS	<p>NORMAL:</p> <p>Feeding - The pressurizer heaters can compensate for the small primary pressure transient for all break sizes.</p> <p>Preheat - The pressurizer spray can compensate for the pressure transient resulting from small breaks.</p> <p>OVERPRESSURIZE:</p> <p>Feeding - Leads to a reactor trip on overpressurization.</p> <p>Preheat - No effect for large or intermediate sized breaks; overpressurization for small breaks.</p> <p>Depressurization - Leads to a reactor trip on low pressurizer pressure.</p>
PRSZR LEV	<p>NORMAL: Maintains appropriate pressurizer level for small breaks.</p> <p>EXCESS: Leads to reactor trip.</p> <p>DEFICIENT: Leads to a reactor trip.</p>

TABLE B.2.5-2

FUNCTIONS NOT USED FOR A FEEDWATER SYSTEM PIPE BREAK

<u>Function</u>	<u>Discussion</u>
STM LD CONT	Prior to reactor trip the steam demands will have only a minor effect on the transient.

## B.2.6 LOSS OF FORCED REACTOR COOLANT FLOW (COMPLETE AND PARTIAL)/LOCKED ROTOR

### B.2.6.1 Transient Description

Complete loss of forced reactor coolant flow may result from a simultaneous loss of electrical supplies to all reactor coolant pumps. This event is classified as an ANS Condition II event.

A partial loss of forced reactor coolant flow can result from a mechanical or electrical failure in a reactor coolant pump, or from a fault in the power supply to the pump supplied by a reactor coolant pump bus. This event is classified as an ANS Condition II event.

Normal power for the reactor coolant pumps is supplied through individual buses connected to the generator. When a generator trip occurs, the buses are automatically transferred to an offsite power supply. The pumps will continue to supply coolant flow to the core. Following any turbine trip where there are no electrical faults or thrust bearing failure, which require tripping the generator from the network, the generator remains connected to the network for approximately 30 seconds. This ensures full flow for approximately 30 seconds after the reactor trip before any transfer is made.

A locked rotor or reactor coolant pump shaft break may result from an instantaneous seizure of a reactor coolant pump rotor or an instantaneous failure of a reactor coolant pump shaft. This event is classified as an ANS Condition IV event.

The loss of flow/locked rotor events are protected by the following trips:

1. Low Reactor Coolant Flow
2. Low Reactor Coolant Pump Supply Undervoltage
3. Low Reactor Coolant Pump Supply Underfrequency



#### B.2.6.2 Discussion of Control Event Tree

The control event tree for loss of flow/locked rotor is shown in Figure B.2.6-1. The only control functions used are those which lead directly to another transient, i.e., LOCA, steambreak (See Table B.2.6-1). All other control functions are not included since a loss of flow/locked rotor event is terminated very rapidly by a reactor trip and these control functions cannot appreciably affect the RCS pre-conditioning prior to trip (See Table B.2.6-2).

The termination point for all branches of this tree is the initiation of another transient or a reactor trip.

FIGURE B.2.6-1

LOSS OF FORCED REACTOR COOLANT FLOW  
(COMPLETE AND PARTIAL)/LOCKED ROTOR

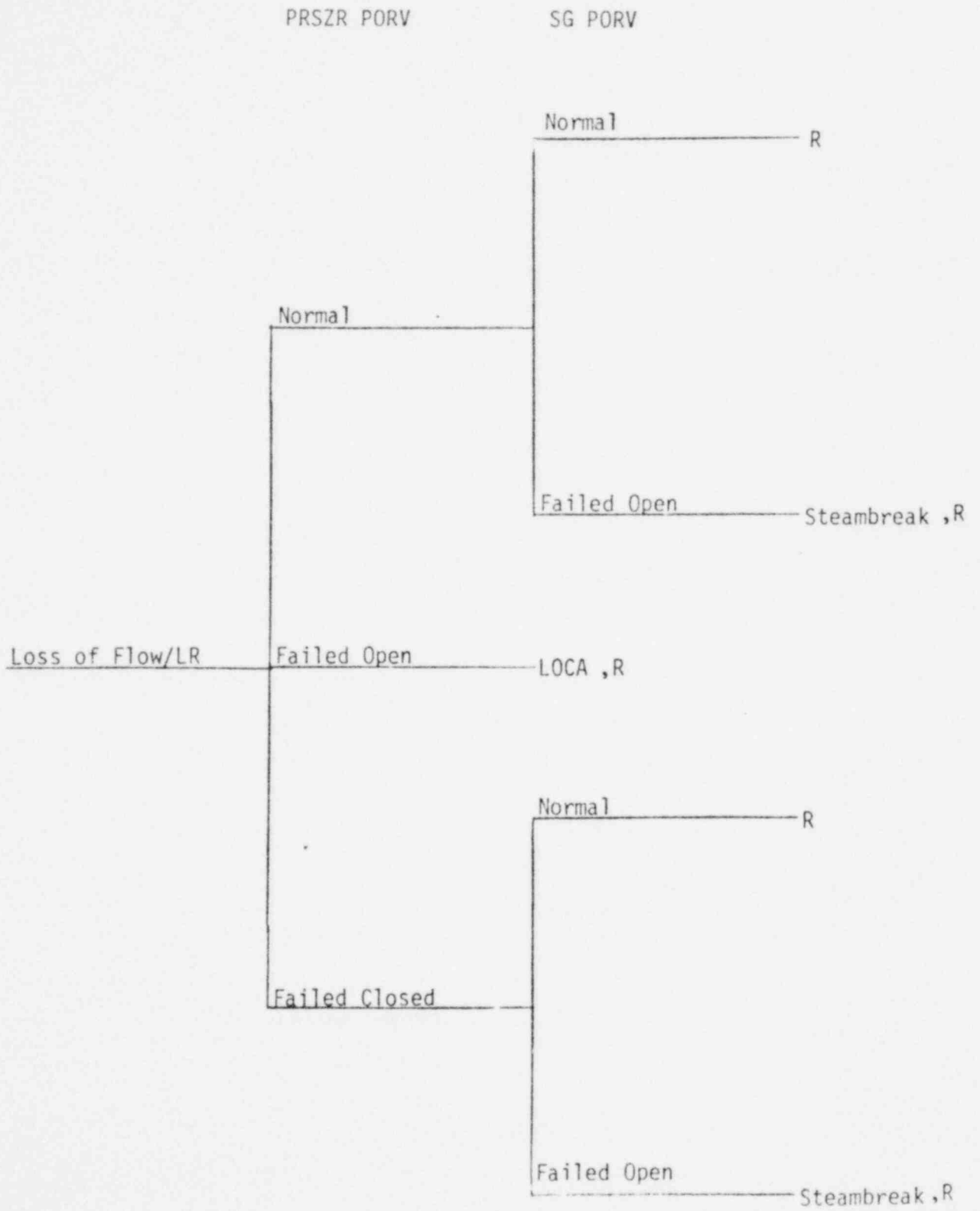


TABLE B.2.6-1

DECISION POINTS FOR LOSS OF FLOW/LR

<u>Function</u>	<u>Discussion</u>
PRSZR PORV	Pressure increase events, PORV may actuate. Failed open leads to LOCA event.
SG PORV	Not expected to actuate prior to trip. Closed and normal mode are the same. Failed open mode leads to steambreak event.

TABLE B.2.6-2

FUNCTIONS NOT USED IN LOSS OF FLOW/LR

<u>Function</u>	<u>Discussion</u>
FW CONT	Transient terminated by reactor trip too quickly to affect RCS pre-conditioning
ROD CONT	Transient terminated by reactor trip too quickly to affect RCS pre-conditioning
PRSZR LEV	Transient terminated by reactor trip too quickly to affect RCS pre-conditioning
PRSZR PRS	Transient terminated by reactor trip too quickly to affect RCS pre-conditioning
STM 'D CONT	Transient terminated by reactor trip too quickly to affect RCS pre-conditioning

## B.2.7 UNCONTROLLED ROD CLUSTER CONTROL ASSEMBLY BANK WITHDRAWAL AT POWER

### B.2.7.1 Transient Description

Uncontrolled RCCA bank withdrawal at power results in an increase in the core heat flux. Since the heat extraction from the steam generator lags behind the core power generation until the steam generator pressure reaches the relief or safety valve setpoint, there is a net increase in the reactor coolant temperature. Unless terminated by manual or automatic action, the power mismatch and resultant coolant temperature rise could eventually result in DNB. Therefore, in order to avert damage to the fuel clad the Reactor Protection System (RPS) is designed to terminate any such transient before the DNB limits are exceeded.

The RCCA bank withdrawal can occur with a spectrum of initial power levels and reactivity insertion rates. The automatic features of the RPS which prevent core damage following the postulated event include overtemperature and overpower  $\Delta T$  reactor trips, high neutron flux reactor trips (power range), and high pressurizer pressure and water level reactor trips. In addition, RCCA withdrawal blocks are actuated on high neutron flux and overpower and overtemperature  $\Delta T$  signals at setpoints slightly below the above reactor trips.

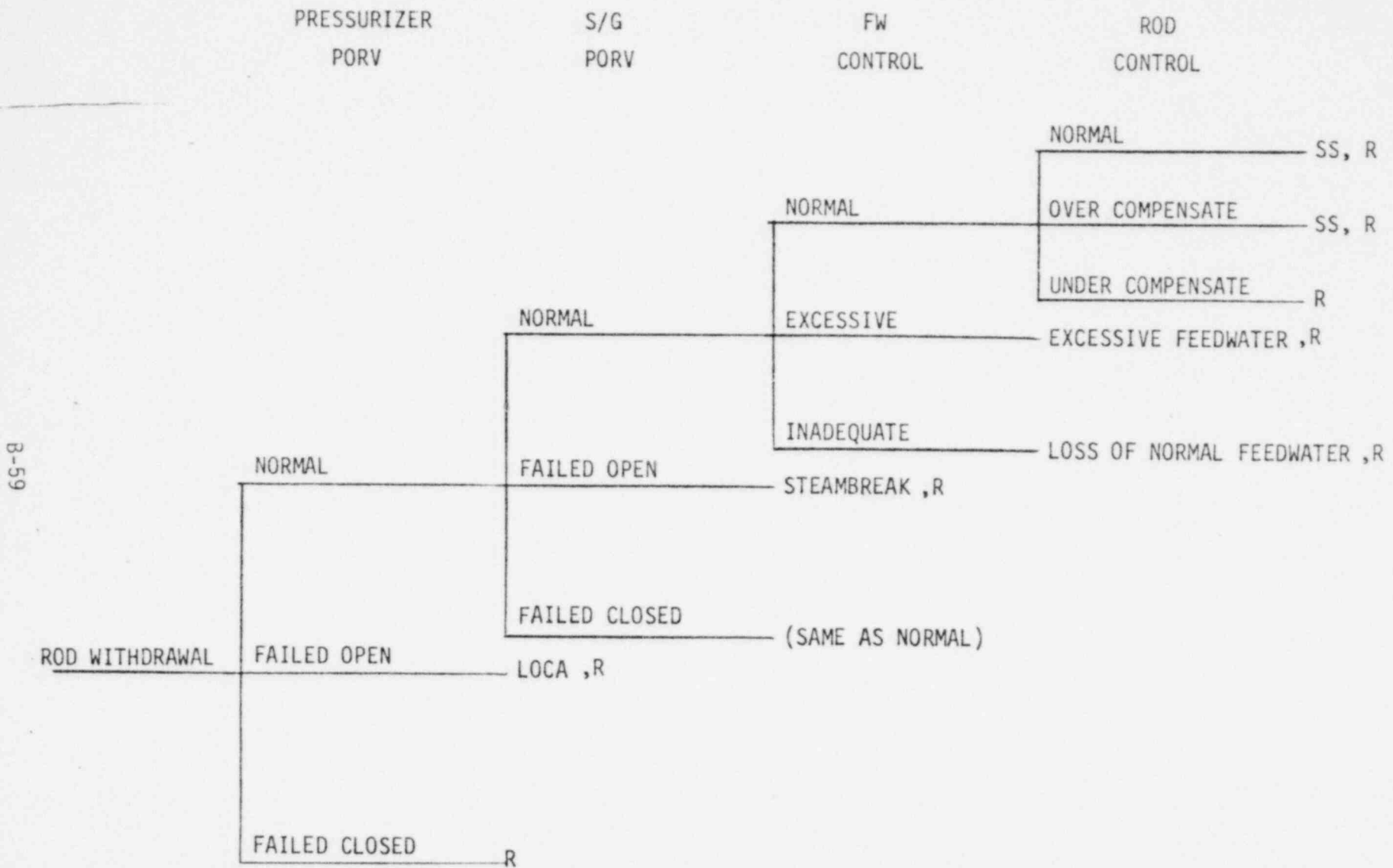
This event is classified as an ANS Condition II incident (an incident of moderate frequency).

### B.2.7.2 Discussion of Control Event Tree

The control event tree for the uncontrolled RCCA bank withdrawal at power is shown in Figure B.2.8-1. The control functions used in the tree and their effect on the transient are shown in Table B.2.8-1. The functions not included in the tree and the reasons for not using them are shown in Table B.2.8-2.

Figure B.2.7-1

RCCA BANK WITHDRAWAL AT POWER



B-59

TABLE B.2.7-1

DECISION POINTS FOR RCCA BANK WITHDRAWAL AT POWER

<u>Function</u>	<u>Discussion</u>
PRSZR PORV	NORMAL mode will open and close as required to regulate pressure. May not be called upon to open depending on transient. FAILED OPEN mode leads to LOCA. FAILED CLOSED mode would most likely lead to reactor trip on high pressure.
SG PORV	NORMAL mode will open and close as required to regulate steam pressure. FAILED OPEN mode leads to Steambreak event. In FAILED CLOSED mode steam pressure may increase to safety valve setpoint. From that point on this mode would be similar to NORMAL mode.
FW CONT	NORMAL mode would maintain steam generator inventory. EXCESSIVE mode leads to Excessive Feedwater event. INADEQUATE mode leads to Loss of Normal Feedwater event.
ROD CONT	NORMAL mode might lead to recovery or new steady state via the rod withdrawal blocks, or might still give a reactor trip. OVER COMPENSATE mode would be the same as NORMAL mode. UNDER COMPENSATE mode would result in reactor trip.

TABLE B.2.7-2

FUNCTIONS NOT USED FOR RCCA BANK WITHDRAWAL AT POWER

<u>Function</u>	<u>Discussion</u>
PRSZR LEV	Does not appreciably alter the course of the event.
PRSZR PRS	Does not appreciably alter the course of the event.
STM LD CONT	Effects of operation of this function would be the same as steam generator PORV functioning.

## B.2.8 STARTUP OF AN INACTIVE REACTOR COOLANT LOOP AT AN INCORRECT TEMPERATURE

### B.2.8.1 Transient Description

A startup of an inactive reactor coolant pump at greater than 25 percent of full power can only be accomplished by violation of administration procedures. If the idle reactor coolant pump is started, the colder water insertion into the core will cause a reactivity insertion and subsequent power increase. This is classified as an ANS Condition II event.

This transient will be terminated by a reactor trip on low reactor coolant loop flow when the power range neutron flux exceeds the P-8 setpoints.

### B.2.8.2 Discussion of Control Event Tree

The control event tree for the startup of an inactive reactor coolant pump is shown in Figure B.2.8-1. The control functions used in the tree and their effect on the transient are shown in Table B.2.8-1. The functions not included in the tree and the reasons for not using them are shown in Table B.2.8-2.



FIGURE B.2.8-1  
STARTUP OF AN INACTIVE REACTOR COOLANT LOOP (SUIL)

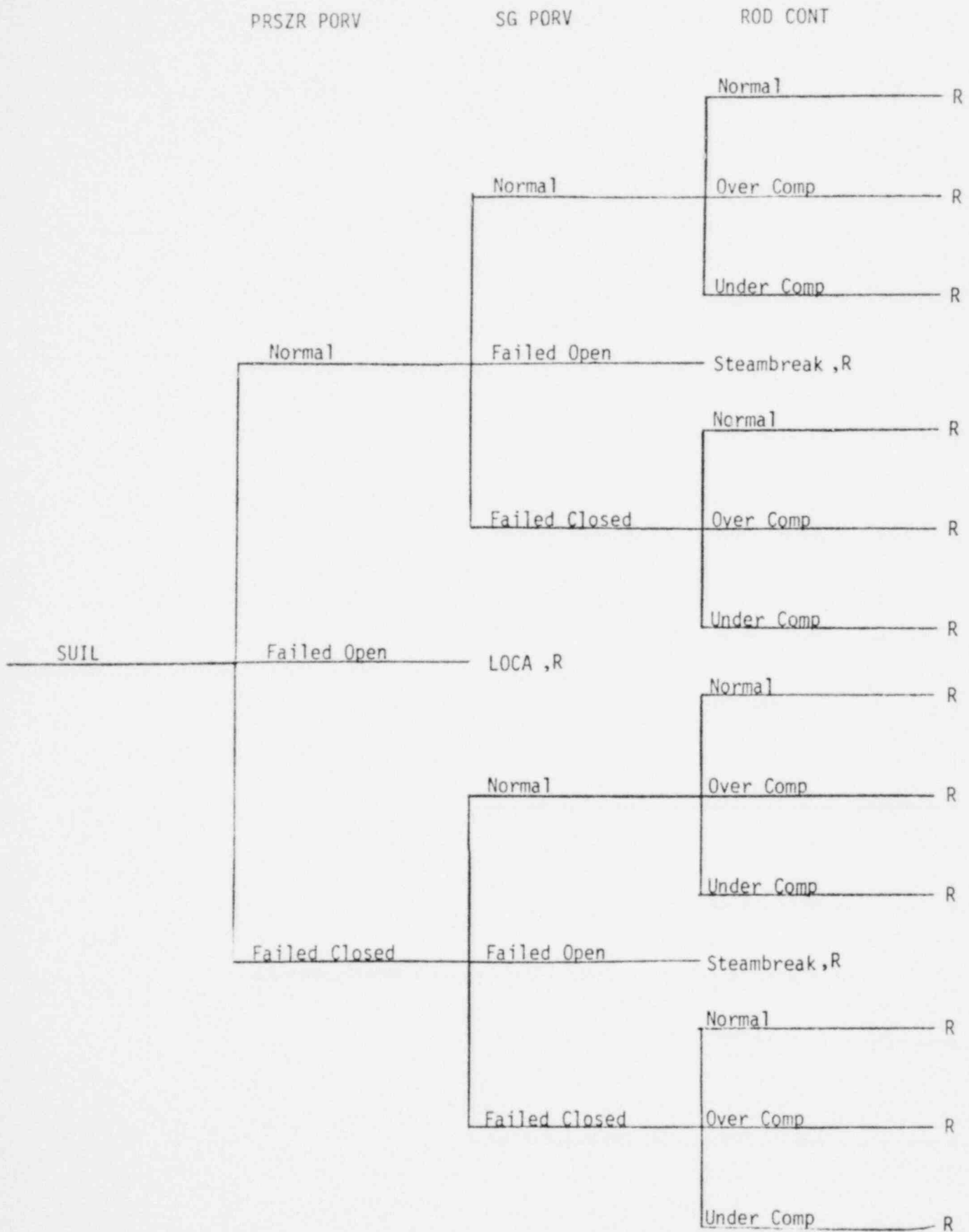


TABLE B.2.8-1

DECISION POINTS FOR STARTUP OF AN INACTIVE REACTOR COOLANT LOOP

<u>Function</u>	<u>Discussion</u>
PRSZR PORV	Pressure increase event, PORV may actuate. Failed open leads to LOCA event.
SG PORV	Would not be expected to open. Failed open leads to steambreak event.
ROD CONT	Normal mode would tend to increase $T_{avg}$ after initial cooldown. Over compensate mode would lead to rod withdrawal at power event. Under compensate or no rod movement would essentially result in normal mode.

TABLE B.2.8-2

FUNCTIONS NOT USED IN STARTUP OF AN INACTIVE REACTOR COOLANT LOOP

<u>Function</u>	<u>Discussion</u>
FW CONT	Because of time of trip ( $\approx 12$ sec) a feedwater control malfunction will have little effect on transient since the trip is within approximately 1 loop transit time.
PRSZR LEV	Charging and letdown (excessive or none) will have minimal effect because of "quick" trip.
PRSZR PRS	Heaters/Sprays have minimal effect on this transient.
STM LD CONT	If steam dump failed open, the increased effect would aid reactivity insertion and trip sooner. Same effects as the rod control system.

## B.2.9 CHEMICAL AND VOLUME CONTROL SYSTEM MALFUNCTION THAT RESULTS IN A DECREASE IN BORON CONCENTRATION IN THE REACTOR COOLANT

### B.2.9.1 Transient Description

Reactivity can be added to the core by feeding primary grade water into the reactor coolant system via the reactor makeup portion of the chemical and volume control system. Boron dilution is a manual operation under strict administrative controls with procedures calling for a limit on the rate and duration of dilution. A boric acid blend system is provided to permit the operator to match the boron concentration of reactor coolant makeup water during normal charging to that in the reactor coolant system. The chemical and volume control system is designed to limit the potential rate of dilution to a value which, after indication through alarms and instrumentation, provides the operator sufficient time to correct the situation in a safe and orderly manner.

Inadvertent opening of the primary water makeup control valve, malfunctions in boric acid blend system or operator miscalculation of required reactor coolant system boron concentrations could result in an uncontrolled boron dilution event. To cover all phases of plant operation, boron dilution analysis is performed for a spectrum of subcritical (refueling operating mode) and critical (power operation in manual and automatic control rod control) initial conditions.

This event is classified as an ANS Condition II incident (an incident of moderate frequency).

The interactions of the control event tree functions during a boron dilution at power would be essentially the same whether the control rods are in manual or automatic control. In automatic control the operator would select manual control when the rod insertion limits are reached. In manual control the boron dilution event is essentially identical to the uncontrolled RCCA bank withdrawal at power event because of the positive reactivity addition. Therefore, a boron dilution at power is covered by the RCCA bank withdrawal event tree in Section B.2.7.

During a boron dilution event from a refueling or cold shutdown condition, there are no significant interactions between the control event tree functions. Therefore, no event tree is presented for these cases.

## B.2.10 SPECTRUM OF ROD CLUSTER CONTROL ASSEMBLY EJECTION ACCIDENTS

### B.2.10.1 Transient Description

A RCCA ejection event could occur as a result of a large pressure differential caused by a passive, mechanical failure of the drive mechanism housing. Most of the RCCAs are fully withdrawn while the reactor is critical. The consequences of an RCCA ejection will therefore most likely be an uncontrolled depressurization event, with a maximum possible break size of approximately 3.25 inches in diameter. Should the RCCA be partially or fully inserted before ejection, the immediate consequences would be a rapid positive reactivity insertion which would cause a rapid increase in core power level together with an adverse core power distribution, possibly leading to localized fuel rod damage. The power increase is limited by the inherent Doppler feedback mechanism, and the reactor would be shut down by a reactor trip on high neutron flux or high rate of neutron flux increase. The RCS pressure would increase in the initial stage of the transient, and decrease due to the break following the reactor trip. No power transient will result if the reactor is initially in a shutdown condition since the reactor will remain subcritical.

This accident is classified as an ANSI Condition IV, Limiting Fault event.

### B.2.10.2 Discussion of Control Event Tree

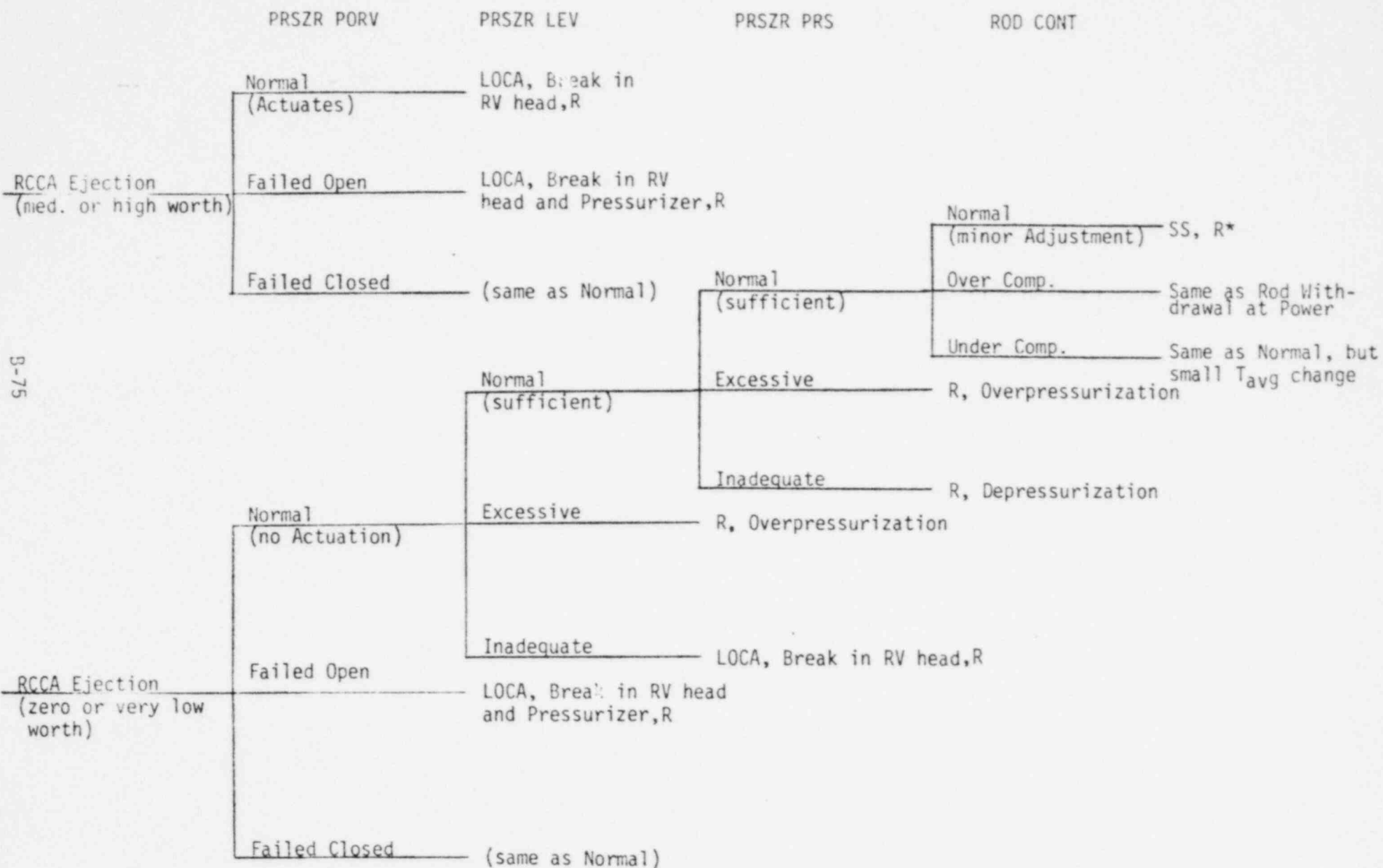
The control event tree for the RCCA ejection accident is shown in Figure B.2.10-1. The control functions used in the tree and their effect on the transient are given in Table B.2.10-1. The functions not included in the tree and the reasons for not including them are shown in Table B.2.10-2.

As shown in the event tree, if the reactivity insertion is of moderate or high worth, an immediate reactor trip will result on either high neutron flux or high rate of flux increase. However, before the rods can be inserted, the power increase may be severe enough to cause the pressurizer PORV to open. Should a PORV fail to close, the effect after reactor trip would be to cause an escape of reactor coolant through the pressurizer in addition to the break in the reactor vessel head. If the PORV is not actuated, or closes after actuation, the reactor would be in a tripped mode with a break in the reactor vessel head only.

If the reactivity insertion is zero or small, corresponding to ejection of a fully withdrawn or only partly inserted RCCA, a reactor trip on high neutron flux or high rate of flux increase may not result. Following along this path, the pressurizer PORV may or may not open depending on the magnitude of the reactivity insertion and size of the break in the RV head. If the PORV opens and fails to close, the reactor will depressurize rapidly through both the break in the RV head and the pressurizer, actuating a reactor trip on low pressurizer pressure. If the PORV does not open, or opens and closes normally, the CVCS flow may be sufficient to maintain pressurizer level depending on the RV head break size. If pressurizer pressure control and rod control system behave normally, then the RCS pressure and average temperature will be maintained and the reactor would be in a steady state condition as long as the CVCS flow is sufficient. If the pressurizer pressure or rod control systems malfunction, this can cause a depressurization or overpressurization or overpower condition as shown in the diagrams.

FIGURE B.2.10-1

SPECTRUM OF ROD CLUSTER CONTROL ASSEMBLY EJECTION ACCIDENTS



S-75

\*Trips if water supply becomes insufficient to cope with break in RV head.

TABLE B.2.10-1

DECISION POINTS FOR RCCA EJECTION EVENT TREE

<u>Function</u>	<u>Discussion</u>
PRSZR PORV	NORMAL - Would be expected to actuate for moderate or severe reactivity insertions, not actuate for zero or very small insertions. FAILED OPEN leads to a loss of coolant path through the pressurizer as well as the RV head. FAILED CLOSED is the same as NORMAL except for a higher pressure rise.
PRSZR LEV	NORMAL - May be sufficient to maintain level for smallbreaks. EXCESSIVE leads to a reactor trip on high level or overpressurization. DEFICIENT mode leads to a reactor trip on depressurization, with a net loss of coolant through the break.
PRSZR PRS	NORMAL mode maintains constant reactor pressure. EXCESSIVE mode leads to a reactor trip on overpressurization. DEFICIENT mode leads to a reactor trip on depressurization.
ROD CONT	NORMAL mode maintains nominal $T_{avg}$ and power, a steady-state condition. OVERCOMPENSATION (withdrawal) is a reactivity insertion event similar to the RCCA Bank Withdrawal at Power. UNDERCOMPENSATION mode may result in a change in $T_{avg}$ to compensate for any reactivity imbalances, but would reach a steady-state condition as in the NORMAL mode.

TABLE B.2.10-2

FUNCTIONS NOT USED FOR RCCA EJECTION EVENT TREE

<u>Function</u>	<u>Discussion</u>
SG PORV	Not actuated for moderate or severe reactivity insertions due to rapid reactor trip on neutron flux. Not called upon to actuate for zero or small reactivity insertions. Considered following reactor trip
FW CONT or STM LD CONT	Not important for moderate or severe reactivity insertions due to rapid reactor trip on neutron flux. Not important for zero or small insertions where CVCS insufficient due to rapid trip on depressurization. For events where CVCS is sufficient, malfunctions of system covered by other events. Considered following reactor trip.



## B.2.11 INADVERTENT OPERATION OF EMERGENCY CORE COOLING SYSTEM DURING POWER OPERATION

### B.2.11.1 Transient Description

Spurious emergency core cooling system (ECCS) operation at power could be caused by operator error or a false electrical actuation signal from any safety injection channel. Following the actuation signal the ECCS forces boric acid solution from either the boron injection tank or the refueling water storage tank into the cold leg of each loop.

A safety injection signal (SIS) normally results in a reactor trip and a turbine trip. However, it cannot be assumed that any single fault that provides an SIS will also produce a reactor trip. If a reactor trip is generated by the spurious SIS signal, the operator will stop the safety injection and maintain the plant in the hot shutdown condition.

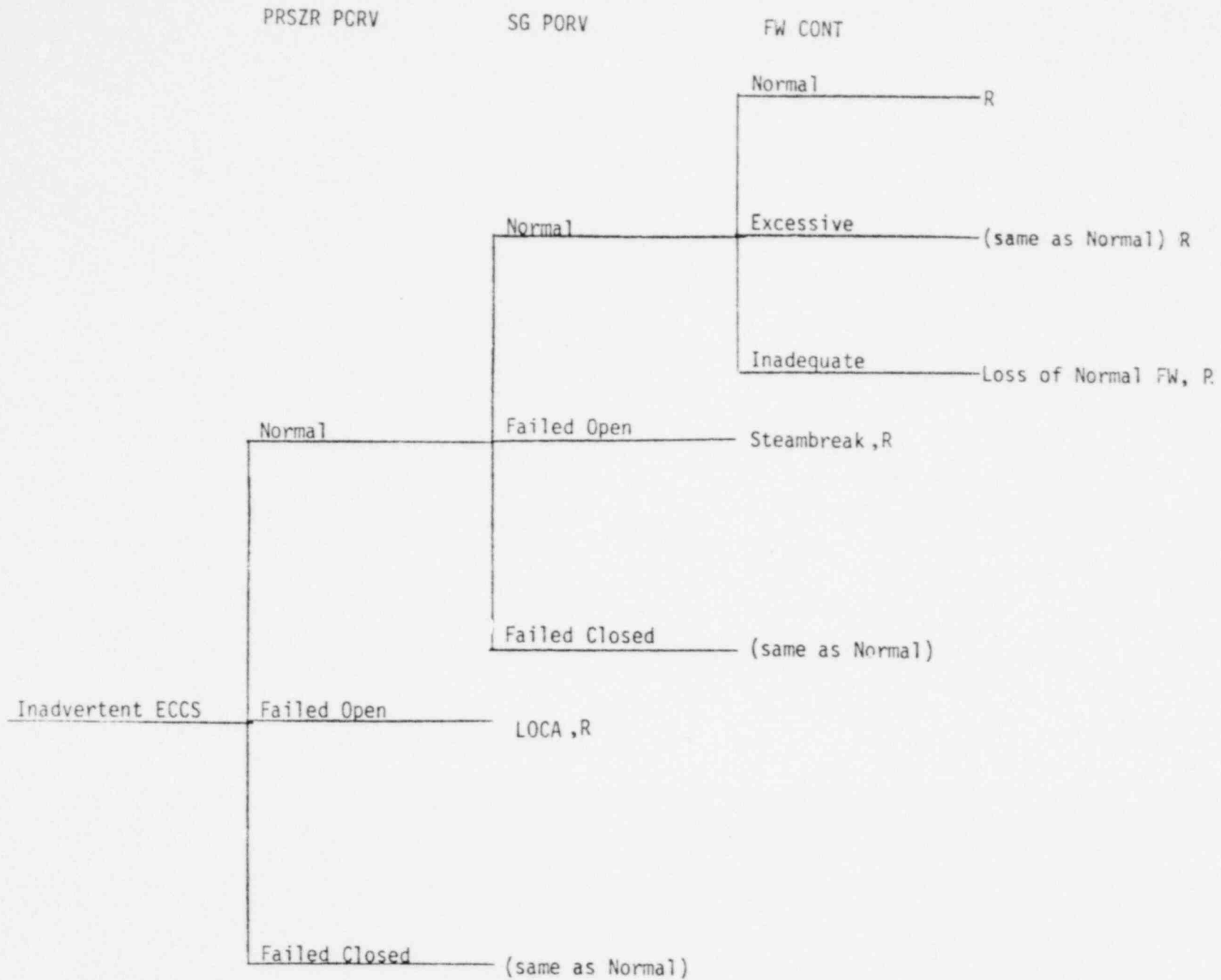
If the reactor protection system does not produce an immediate trip as a result of the spurious safety injection signal, the reactor experiences a negative reactivity excursion due to the injected boron causing a decrease in reactor power. The power mismatch causes a drop in  $T_{avg}$  and consequent coolant shrinkage. Pressurizer pressure and water level drop. Load will decrease due to the effect of reduced steam pressure on load after the turbine governor valve is fully open. If automatic rod control is used, these effects will be lessened until the rods have reached their upper withdrawal limit. The transient is eventually terminated by the reactor protection system low-pressure trip or by manual trip.

This event is classified as a Condition II incident (an incident of moderate frequency).

### B.2.11.2 Discussion of Control Event Tree

The control event tree for the addition of excessive feedwater is shown in Figure B.2.11-1. The control functions used in the tree and their effect on the transient are shown in Table B.2.11-1. The functions not included in the tree and the reasons for not using them are shown in Table B.2.11-2.

FIGURE B.2.11-1  
 INADVERTENT OPERATION OF ECCS



B-83

TABLE B.2.11-1

DECISION POINTS FOR INADVERTENT OPERATION OF ECCS

<u>Function</u>	<u>Discussion</u>
PRSZR PORV	Would not be expected to actuate since pressure decreases. FAILED CLOSED is same as NORMAL mode. FAILED OPEN leads to LOCA event.
SG PORV	Would not be expected to actuate since secondary steam pressure decreases. FAILED CLOSED is same as NORMAL mode. FAILED OPEN leads to steambreak event with safety injection already initiated.
FW CONT	Both NORMAL and EXCESSIVE modes lead to reactor trip since they don't act to significantly change the course of the transient. INADEQUATE mode may lead to loss of normal feedwater event, but reactor trip as above would be just as likely.

TABLE B.2.11-2

FUNCTIONS NOT USED FOR INADVERTENT OPERATION OF ECCS

<u>Function</u>	<u>Discussion</u>
ROD CONT	The different modes of this function would not significantly affect course of transient.
PRSZR LEV	This function cannot keep up with shrinkage due to primary cooldown.
PRSZR PRS	The different modes of this function would not significantly affect course of transient.
STM LD CONT	The different modes of this function would not significantly affect course of transient.

## B.2.12 INADVERTENT OPENING OF A PRESSURIZER SAFETY OR RELIEF VALVE

### B.2.12.1 Transient Description

An accidental depressurization of the Reactor Coolant System (RCS) could occur as a result of an inadvertent opening of a pressurizer relief or safety valve. Since a safety valve is sized to relieve approximately twice the steam flow rate of a relief valve, and will therefore allow a much more rapid depressurization upon opening, the most severe core conditions resulting from an accidental depressurization of the RCS are associated with an inadvertent opening of a pressurizer safety valve. Other causes of a depressurization of an RCS are excessive letdown by the CVCS and excessive spray in the pressurizer. The effect of the pressure decrease is to decrease power via the moderator density feedback; however, the reactor control system (if in the automatic mode) functions to maintain power throughout the initial stage of the transient. The average coolant temperature decreases slowly, but the pressurizer level increases until reactor trip on either low pressurizer pressure or overtemperature  $\Delta T$ .

An inadvertent opening of a pressurizer safety valve, excessive letdown or excessive pressurizer spray are classified as an American Nuclear Society (ANS) Condition II event, a fault of moderate frequency.

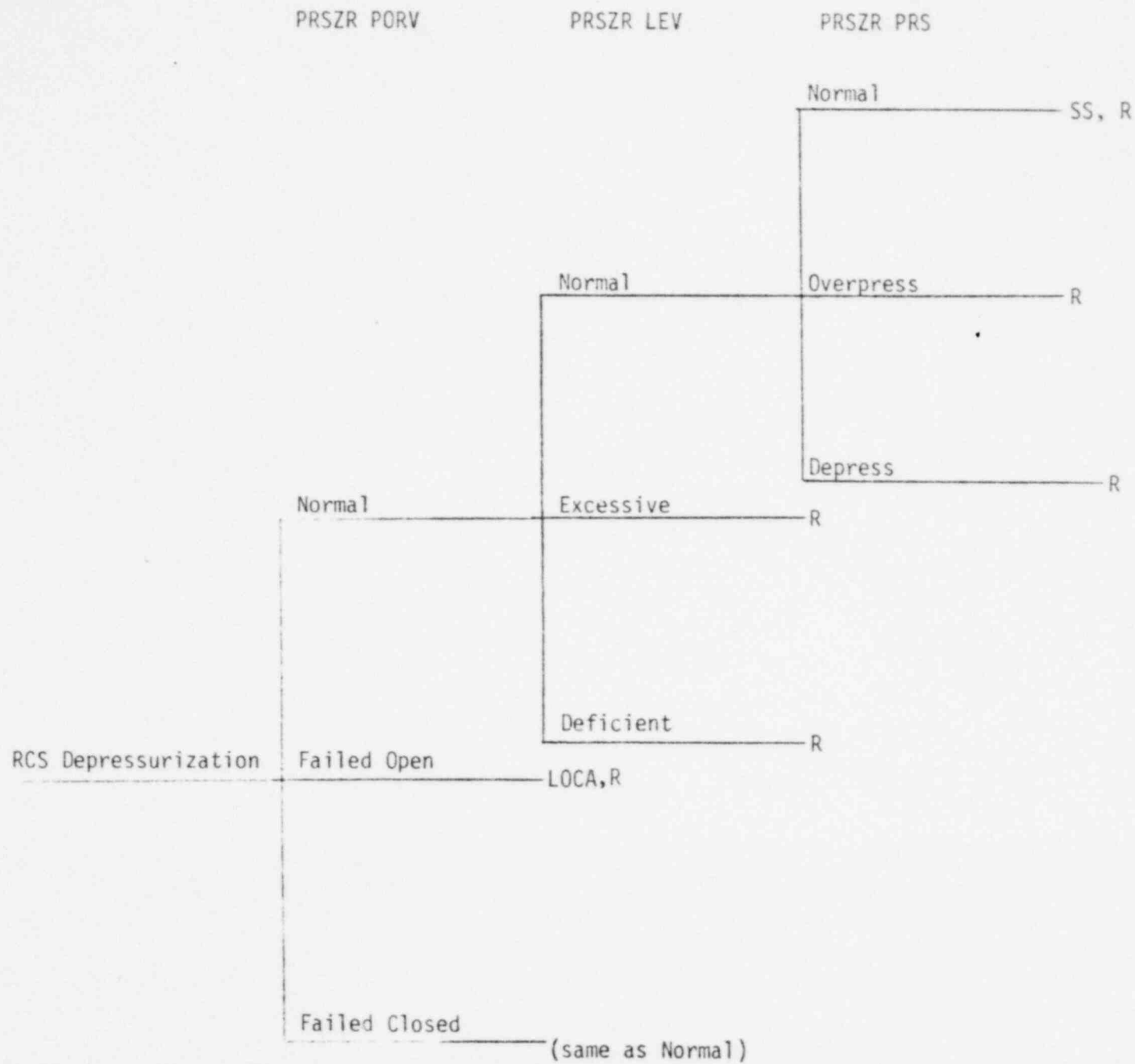
### B.2.12.2 Discussion of Control Event Tree

The control event tree for accidental depressurization of the RCS is shown in Figure B.2.12-1. The control functions used in the tree and their effect on the transient are shown in Table B.2.12-1. The functions not included in the tree and the reasons for not using them are shown in Table B.2.12-2.

## B.3. INSTRUMENTATION

See Section C.3 of Appendix C for a discussion of the instrumentation assumed for determining the status of the control event tree functions.

FIGURE B.2.12-1  
INADVERTENT RCS DEPRESSURIZATION



B-89

TABLE B.2.12-1

DECISION POINTS FOR INADVERTENT RCS DEPRESSURIZATION

<u>Function</u>	<u>Discussion</u>
PRSZR PORV	NORMAL mode implies depressurization caused by something other than stuck open safety or relief valve. FAILED OPEN mode leads to LOCA. FAILED CLOSED mode is the same as NORMAL mode.
PRSZR LEV	NORMAL mode maintains primary inventory and may help to correct depressurization EXCESSIVE mode leads to reactor trip on high pressurizer level. DEFICIENT mode does not change the initial event.
PRSZR PRS	NORMAL mode may maintain RCS pressure and result in a new steady state condition, but reactor trip is still possible. OVERPRESSURIZE and DEPRESSURIZE modes will result in reactor trip.

TABLE B.2.12-2

FUNCTIONS NOT USED FOR INADVERTENT RCS DEPRESSURIZATION

<u>Function</u>	<u>Discussion</u>
SG PORV	Any secondary function does not appreciably affect depressurization
FW CONT	Any secondary function does not appreciably affect depressurization
ROD CONT	Has no significant effect on course of transient
STM LD CONT	Any secondary function does not appreciably affect depressurization

APPENDIX C  
ANALYSIS OF NON-LOCA POST-TRIP ACCIDENTS

C.1 TRANSIENT DESCRIPTION AND METHODOLOGY

The purpose of this section is to identify post-trip critical decision points for the operator, to show alternate event sequences based on his decisions and to qualitatively assess the consequences of the sequence paths being followed for events not covered in the emergency procedures (events which do not initially result in a loss of primary or secondary coolant).

Prior to event tree construction, a review of systems critical to safety was initiated. These systems were then combined into groupings based upon overall system safety functions. Section C.2 defines the functions used in the non-loss of primary and secondary coolant event trees. These functions are intentionally defined at a general level (i.e., SSR-Secondary Steam Relief) in order to maintain the review at the level which emphasizes trends. This assumption also results in the need for only one post-trip event tree being required for these transients (Figure C.1). Included in each Section C.2 description of safety functions is a system tree showing alternate equipment configurations for achieving the safety function; for example, Secondary Steam Relief can be achieved via the Steam Dump System, Steam Generator Power Operated Relief Valves and the Safety Valves (See Figure C.3). With each safety function description is a discussion of how the equipment configurations change depending upon the availability of electric power.

At each decision point in the post-trip event tree, three potential modes of operation are defined. Basically each safety function can be defined as either performing as required, responding excessively or inadequately. Thus, the operator must not only decide if a function is required but also if it is actuated he must verify that the desired function has occurred and responded as expected.



Each sequence must be reviewed for all combinations to assure that sufficient information is available to clearly identify the status of each safety function. Each safety function tree (Figures C.2 - C.5) has a section which identifies the potential for each system configuration to lead into the function states shown in the Post-Trip Event Tree. (Figure C.1). Several configurations show that there is the potential for normal, adequate and excessive function operation to occur. Thus, it is important that the operator has clear indications of function status. Table C.2 provides a listing of what instrumentation is available to monitor the safety functions, together with relative accuracies.

An assessment has been made of what ultimate system failures may occur if the safety functions do not respond as required. Table C.4 lists potential system failure mechanisms for each sequence shown in Figure C.1. It should be noted that the time and the magnitude of failures are highly dependent on the initiating events and equipment configurations. However, these potential failure mechanisms do provide an indication of the potential for entry into the Emergency Operating Instructions.

This review focused on accidents which did not initially result in a loss of primary or secondary coolant. The intent was to verify that entry into the EOIs from one of these paths would not result in improper guidance.

## C.2 SYSTEM'S DESCRIPTIONS

This section defines the safety functions represented in the non-LOCA post-trip event tree. Included is a discussion of the specific systems which result in the overall safety function. Since the scope of this effort is to show that the operator has proper guidance in the procedures and adequate plant indications to make decisions, this review does not require a differentiation between full and impaired operation of systems. When more than one system is available to achieve a safety function, the operation of one system over another could briefly change accident trends. These cases will be noted. The safety functions are defined as follows:

### C.2.1 EP ELECTRIC POWER

Electrical power availability can affect the performance of required safety functions. The systems used to achieve this function are:

1. Fast Bus Transfer
2. Battery supplies DC to vital buses.
3. Diesel Electric Generating Unit  
(Essential Auxiliary Power System)

The normal mode of operation is to rely on Fast Bus Transfer. Following reactor trip the turbine-generation system is allowed to motor (supply power to the station auxiliaries) for ~ 30 seconds. At 30 seconds a transfer of plant electrical loads to offsite power sources is automatically attempted. Failure of this transfer results in loss of power to station auxiliaries. Loss of offsite power sources does not change the structure of the event tree. It does reduce the number of systems available to the operator to assure safety functions are achieved. In addition, the generation of BLACKOUT signals will result in automatic actuation of certain functions (i.e., safety injection). Generation of the BLACKOUT signal after failure of load transfer results in use of the battery system and use of the Essential Auxiliary Power System. This is defined as diesel-generation startup and elimination of non-vital loads from the power bus.

The decision shown in the event tree is binary. Either sufficient electrical power is available to supply the power requirements of the other safety functions or else all on/off site power is lost.

For this study three cases are considered in the discussion of each safety function:

1. Electric power available - offsite.

2. Electric power available - onsite via Essential Auxiliary Power System
3. No electrical power available.

### C.2.2 RT REACTOR TRIP

The purpose of this function is to assure a means of rapidly reducing nuclear-thermal power generation. The reactor trip variations have been reviewed in the Control Event Trees for each transient. Reactor trip is defined in this study as the ability to insert RCCAs into the reactor core. This results in three potential failure paths:

1. Failure of RCCA insertion on demand (ATWT).
2. RCCAs previously inserted.
3. RCCA insertion inadequate in maintaining subcriticality.

The first case is considered as a failure mechanism, however, the sequence constructions are identical to the normal paths. Since the only difference would be a reduction in failure times (operator action times), this case is not specially addressed; however the sequences may be utilized as part of an ATWT review. The consequences of this failure path are not addressed in this review. The next cases represents transients initiated from shutdown modes (i.e., Boron Dilution) or transients where positive reactivity insertions can continue after reactor trip. Although these latter cases could result in returns to power which would require a diverse shutdown mechanism (CVCS boration or Emergency Boration), this study will not differentiate between normal RCCA insertion and these cases in this section. These cases are addressed in a later section. The paths shown in Figure C.1 are defined as:

1. Normal: RCCAs will insert on demand, RCCAs inserted prior to reactor trip signal or RCCAs insertion does not stop positive reactivity addition.

2. ATWT: RCCAs withdrawn and will not insert on demand.

$\bar{B}$

### Loss of Offsite Power Considerations

Loss of offsite power has no impact in meeting the safety function.

### C.2.3 SFS SECONDARY FEEDWATER SUPPLY

The purpose of this function is to assure that sufficient feedwater is available to match the desired steam flow. Figure C.1 shows that the response of the SFS to an event can follow three paths. These paths are defined as:

Adequate: System reponds to maintain steam generator level and match  
C feedwater flow with steam flow. Included in this response is feedwater isolation for excessive steam flows.

Inadequate: System cannot maintain steam generator level and feedwater  
 $\bar{C}$  flow is less than steam flow. This path includes feedline breaks without feedline isolation.

Excessive: System cannot maintain steam generator level and feedwater  
+  
C flow is greater than steam flow. Included in this response is no feedline isolation for excessive steam flows.

The systems utilized in achieving this function are:

1. Condenser or condensate storage tank
2. Main or auxiliary feedwater pumps
3. Feedline isolation valves
4. Feed system control valves and piping

The above represents a significant number of equipment options and configurations available to the operator and protection system for

satisfying the safety function. Figure C.2 shows the paths which may be utilized in achieving the safety function. The paths show whether the system listed is operational and is being utilized (i.e. feedline isolation is being utilized). The status column shows potential responses of the system for each path and which paths could contribute to the overall responses listed in Figure C.1.

#### Loss of Offsite Power Considerations

Loss of offsite power but availability of onsite power will result in the loss of main feedwater pumps and condenser; however all other systems assigned to meet the function are unaffected. Loss of all power to the station would result in loss of the motor driven auxiliary feedwater pumps. The turbine driven auxiliary feedwater pump would be relied upon for feedwater delivery.

#### C.2.4 SSR SECONDARY STEAM RELIEF SYSTEM

The purpose of this function is to assure a path for transferring thermal energy from the steam generators to the environment. Figure C.1 shows that the response of the SSR can be characterized by three paths:

Adequate: Heat removal from steam generators equals heat generation  
D in reactor core or heat removal results in a controlled  
cooldown.

Inadequate: Heat removal from steam generators is less than heat gen-  
D eration in reactor core.

Excessive: Heat removal from steam generator is greater than heat  
† generation in reactor core and results in an uncontrolled  
cooldown.

The systems provided to achieve this function are:

1. Steam generator safety valves
2. Steam generator power operated relief valves

3. Steam dump
4. Main steamline isolation

The above represent a significant number of equipment options or configurations available to the operator and protection system for satisfying the safety function. Figure C.3 (Secondary Steam Relief System) shows the configurations which may be utilized to achieve the safety function or paths in which the systems could adversely affect other safety functions. The Status column shows potential responses of the system for each configuration and which paths could contribute to the overall responses given in Figure C.1.

The normal mode of steam relief after plant trip is via the steam dump system provided the condenser is available. Without condenser availability normal cooldown would be via the steam generator relief valves dumping to the atmosphere. The failure of the above systems would result in steam release from the safety valves dumping to atmosphere. Ultimate loss of cooling function is defined at the loss of all of the three systems defined. Note, that before the safety or relief valves would actuate during a transient, a significant heatup of the secondary system to the pressure setpoints of these valves would occur; however, steam dump would result in a cooldown sequence.

#### Loss of Offsite Power Consideration

Loss of offsite power would result in a loss of steam dump capability. Steam generator safety and relief valve actuation would be unaffected. Steamline isolation would automatically actuate. Coincident loss of emergency power would result in only steam generator safety valves being available to accomplish the function.

#### C.2.5 PIB PRIMARY INVENTORY AND BORON CONCENTRATION

The purpose of this function is to assure that the reactor coolant system is capable of transporting heat out of the reactor core and to maintain the reactor core subcritical via soluble boron. Figure C.1 shows

that the operation of the PIB (Primary Inventory and Boron Concentration Control Systems) is characterized by three overall responses. These responses are defined as:

Adequate: Systems respond to maintain pressurizer level to assure  
E adequate core cooling and to assure that reactor coolant system boron concentration is greater than the value required to maintain the reactor core subcritical.

Inadequate: System cannot maintain pressurizer level above pressurizer  
E heaters. The core boron concentration is insufficient to maintain the reactor core subcritical.

Excessive: Systems cannot maintain pressurizer water level below the  
E pressurizer safety or relief valves.

The systems utilized in achieving this function are:

1. Safety Injection System
2. Chemical and Volume Control System (CVCS) Charging
3. CVCS Boration/Dilution
4. CVCS Letdown

The above represent a number of equipment options and configurations available to the operator and protection system for satisfying the safety function. Figure C.4 shows systems configurations which yield overall responses. The Status column lists equipment configurations which result in specific responses give Figure C.1.

#### Loss of Offsite Power Considerations

Loss of offsite power but availability of onsite power will not cause loss of functions. Complete loss of on-site power will result in loss of entire function.

## C.2.6 PPC PRIMARY PRESSURE CONTROL SYSTEM

The purpose of this function is to assure RCS pressure control. This function is of importance in assuring that vessel stress limits are not exceeded and also to assure adequate subcooling while in natural circulation flow conditions. Figure C.1 shows that the operation of the PPC can be characterized in terms of three responses:

- |                                    |  |
|------------------------------------|--|
| Adequate:<br>F                     | Reactor coolant system pressure is stable at or below the pressurizer safety valve setpoint value. Also this state is defined as a controlled depressurization.            |
| Depressurization:<br>$\bar{F}$     | Reactor coolant system pressure is decreasing abnormally or primary coolant is at saturation.  |
| Overpressurization:<br>$\bar{F}^+$ | Reactor coolant system pressure is greater than the pressurizer safety valve setpoint value or the technical specification vessel nil-ductility curves have been exceeded. |

The systems utilized in achieving this function are:

1. Pressurizer Power Operated Relief Valves
2. Pressurizer Safety Valves
3. Pressurizer Main and Auxiliary Sprays
4. Pressurizer Heaters

The above represent a number of equipment options and configurations available to the operator and protection system for satisfying the safety function. Figure C.5 shows systems configurations which yield overall responses. The Status column lists equipment configurations which result in specific responses given in Figure C-1.



## Loss of Offsite Power Considerations

Loss of offsite or onsite power will not affect operation of the safety valves for achieving the safety function.

### C.3 INSTRUMENTATION

In order to determine the response of the safety functions during a transient, the operator must rely on data supplied by plant instrumentation. He must be aware of the primary instruments available and the limitations of that instrumentation, particularly since the limits or accuracies may change under an accident condition such as could occur for loss of secondary or primary coolant. The operator should be aware that a change in an instrument reading can be due to a change in the process variable being monitored or to a change in the instrument uncertainties.

Table C.2 lists the instrumentation assumed for determining the status of the safety functions described in Appendices A, B and C. The qualification as well as the accuracy under the normal and adverse environments is listed. Also noted are the instruments which are the primary indication of safety function operations. This table is based on the Post Accident Monitoring System (PAMS) developed Post-TMI for standard 412 RESAR 3 type plants. The instruments and accuracies may differ for specific plant designs. However, these differences should not alter the conclusions of this review.

Table C.3 lists the basis for utilizing the instrumentation listed in Table C.2. The table shows which instruments are of primary importance for diagnosing location or type of event. Also included is a listing of process variables or safety functions which can be monitored via this instrumentation. For the loss of primary or secondary coolant events, section A.4 provides specific accident considerations for this equipment.

Table C.1  
Glossary of Functions

<u>Identifier</u>	<u>Function</u>
EP	ELECTRIC POWER
RT	REACTOR TRIP
PIB	PRIMARY INVENTORY AND BORON CONCENTRATION CONTROL
SFS	SECONDARY FEEDWATER SUPPLY
SSR	SECONDARY STEAM RELIEF
PPC	PRIMARY PRESSURE CONTROL

TABLE C.2

Instrumentation Available and Qualification

	Qualification <sup>2</sup>	Accuracy <sup>1</sup>	
		Normal Environment	Adverse Environment
<u>SFS</u>			
SG Wide Range Water Level <sup>4</sup>	I	<u>+4%</u>	<u>+25%</u>
SG Narrow Range Water Level <sup>4</sup>	I	<u>+4%</u>	+35%-20%
Condensate Storage Tank Level	I	<u>+5%</u>	<u>+5%</u>
Aux Feed Water Flow	I	<u>+5%</u>	<u>+10%</u>
RCS Wide Range Temp.			
T <sub>Hot</sub>	I	<u>+4%</u>	<u>+4%</u>
T <sub>Cold</sub>	I	<u>+4%</u>	<u>+4%</u>
RCS Narrow Range Temp. <sup>7</sup>			
T <sub>Hot</sub>	II <sup>3</sup>	<u>+4%</u>	<u>+4%</u>
T <sub>Cold</sub>	II <sup>3</sup>	<u>+4%</u>	<u>+4%</u>

TABLE C.2 (Continued)

Instrumentation Available and Qualification

	Qualification <sup>2</sup>	Accuracy <sup>1</sup>	
		Normal Environment	Adverse Environment
<u>SSR</u>			
Steamline Pressure <sup>4</sup>	-	+4%	+14%
RCS Wide Range Temp. <sup>4</sup>			
T <sub>Hot</sub>	I	+4%	+4%
T <sub>Cold</sub>	I	+4%	+4%
Steamline Flow <sup>5</sup>	II	-	-
RCS Narrow Range Temp. <sup>7</sup>	-	-	-
T <sub>Hot</sub>	II <sup>3</sup>	+4%	+4%
T <sub>Cold</sub>	II <sup>3</sup>	+4%	+4%
MSIV Position Indication	III	-	-
SG PORV Position Indication	III	-	-
<u>PLB</u>			
Pressurizer Level <sup>4</sup>	I	+4%	+35% -20%
Normal Charging Flow	III	-	-
BAT Level	I	+4%	+4%
Boric Acid Flow	III	-	-
RWST Level	I	+4%	+5%
High Head SI Pump Flow	I	+5%	+20%
Low Head SI Pump Flow	I	+5%	+20%
Source Range Excure Detectors <sup>6</sup>	II <sup>3</sup>	-	-

TABLE C.2 (Continued)

Instrumentation Available and Qualification

	Qualification <sup>2</sup>	Accuracy <sup>1</sup>	
		Normal Environment	Adverse Environment
<u>PPC</u>			
Wide Range RCS Pressure <sup>4</sup>	I	+3%	+4%
Pressurizer Pressure	II <sup>3</sup>	+3%	+13%
PRT Pressure	III	-	-
PRT Level	III	-	-
Pressurizer Level	I	+4%	+35% -20%
Pressurizer Spray Valve Indication	III	-	-
Pressurizer Heater Status Lights	III	-	-
Pressurizer PORV Indications	III	-	-
<u>RT</u>			
Rod Position Indication	III	-	-
Intermediate Range Excore Detectors <sup>6</sup>	II <sup>3</sup>	-	-
Source Range Excore Detectors <sup>6</sup>	II <sup>3</sup>	-	-

TABLE C.2 (Continued)

Instrumentation Available and Qualification

	Qualification <sup>2</sup>	Accuracy <sup>1</sup>	
		Normal Environment	Adverse Environment
<u>Diagnostic Aids</u>			
Containment Pressure	I	+4%	+4%
Containment Building Water Level	I	+4%	+4%
Condenser Air Ejector Radiation	I	+15%	+15%
Steam Generator Blowdown Radiation	I	+15%	+15%
Containment Radiation	I	+20%	+40%
Core Exit Thermocouples	I	+1%	+2%

NOTES to TABLE C.2

1. Accuracies are in percent of span unless otherwise noted.
2. The following categories apply for qualification status:
  - I Protection Grade Adverse Environmental Qualified
  - II Protection Grade Qualified
  - III Control Grade Qualified - Although this category is control grade the instrumentation may have limited environmental or seismic qualification.
3. May have limited range
4. Primary indication that safety function is being achieved.
5. Accuracies are generally nominal near full rated flow but deteriorate rapidly for lower flows.
6. For certain physical situations accuracies may be indeterminate.
7. Depends on availability of reactor coolant pumps.

TABLE C.3

INSTRUMENT FUNCTIONS

<u>FUNCTION</u>	<u>INITIAL EVENT DIAGNOSIS*</u>	<u>MONITORING</u>
Containment Pressure	-Determine if break is inside or outside of containment	-Monitor containment conditions following a break inside containment -Verify accident is properly controlled
Steamline Pressure	-Determine if high energy secondary line rupture occurred	-Maintain an adequate reactor heat sink -Verify AFW to steam generator associated with pipe rupture is isolated -Monitor secondary side pressure to -verify operation of pressure control steam dump system -maintain plant in safe shutdown condition -monitor RCS cooldown rate
Narrow Range Steam Generator Water Level	-Determine if malfunction of secondary side system has occurred	-Monitor heat sink -Maintain steam generator water level -Determine whether high head S.I. should be terminated
Wide Range Steam Generator Water Level	-None	-Determine if heat sink is being maintained -Determine which steam generator is associated with high energy line rupture
Boric Acid Tank Level	-None	-Verify RCS boration system functions
Condensate Storage Tank Level	-None	-Maintain adequate water supply for auxiliary feedwater pumps

\*Certain indications on this table are used as secondary diagnoses as the operator proceeds through Post Incident Recovery.



TABLE C.3 (Continued)

INSTRUMENT FUNCTIONS

<u>FUNCTION</u>	<u>INITIAL EVENT DIAGNOSIS*</u>	<u>MONITORING</u>
Refueling Water Storage Tank Level	-None	<ul style="list-style-type: none"> <li>-Verify ECCS and containment spray system are functioning</li> <li>-Determine time for initiation of cold leg recirculation following a LOCA</li> </ul>
Wide Range $T_h$ and $T_c$	-None	<ul style="list-style-type: none"> <li>-Maintain adequate reactor heat sink</li> <li>-Maintain the proper relationship between RCS pressure and temperature                             <ul style="list-style-type: none"> <li>-verify vessel NDTT criteria</li> <li>-maintain primary inventory sub-cooled (particularly with loss of offsite power)</li> <li>-maintain safe shutdown condition</li> <li>-maintain RHR considerations for cooldown</li> <li>-monitor RCS heatup and cooldown rate</li> <li>-determine if plant is in a safe shutdown condition</li> <li>-determine whether high head S.I. should be terminated</li> </ul> </li> </ul>
Pressurizer Water Level	-None	<ul style="list-style-type: none"> <li>-Confirm if plant is in a safe shutdown condition</li> <li>-Determine if water level exists in pressurizer</li> <li>-Maintain pressurizer water level</li> <li>-Determine whether high head S.I. should be terminated</li> </ul>

C-25

\*Certain indications on this table are used as secondary diagnoses as the operator proceeds through Post Incident Recovery.

TABLE C.3 (Continued)

INSTRUMENT FUNCTIONS

<u>FUNCTION</u>	<u>INITIAL EVENT DIAGNOSIS*</u>	<u>MONITORING</u>
System Wide Range Pressure	-None	<ul style="list-style-type: none"> <li>-Determine if plant is in a safe shutdown condition</li> <li>-Maintain the proper relationship between RCS pressure and temperature               <ul style="list-style-type: none"> <li>-verify vessel NDTT criteria</li> <li>-maintain primary inventory sub-cooled (particularly with loss of offsite power)</li> <li>-maintain RHR considerations for cooldown</li> <li>-determine whether RCP operation should be continued</li> <li>-determine whether high head S.I. should be terminated</li> </ul> </li> </ul>
Containment Building Water Level	-Determine whether high energy line rupture has occurred inside or outside containment	<ul style="list-style-type: none"> <li>-Determine NPSH for recirculation mode cooling</li> <li>-Determine which equipment in containment is submerged</li> </ul>
Condenser Air Ejector Radiation	-Determine if steam generator tube leak has occurred	<ul style="list-style-type: none"> <li>-Monitor radioactivity release path to environment</li> </ul>
Steam Generator Blowdown Radiation	-Determine if steam generator tube leak has occurred	<ul style="list-style-type: none"> <li>-Monitor radioactivity release path to environment</li> </ul>
Containment Radiation	-Determine if high energy line break or fuel mishandling accident	<ul style="list-style-type: none"> <li>-Monitor radioactivity release path to environment</li> <li>-Determine accessibility to containment building</li> <li>-Determine if significant fuel damage has occurred</li> </ul>

\*Certain indications on this table are used as secondary diagnoses as the operator proceeds through Post Incident Recovery.

TABLE C.3 (Continued)

INSTRUMENT FUNCTIONS

<u>FUNCTION</u>	<u>INITIAL EVENT DIAGNOSIS*</u>	<u>MONITORING</u>
Auxiliary Feedwater Flow	-None	-Determine if sufficient flow exists to maintain heat sink -Determine which steam generator is associated with secondary high energy line rupture
High Head Safety Injection Flow	-None	-Determine that ECCS is delivering flow -Monitor ability to keep core covered
Low Head Safety Injection Flow	-None	-Determine that ECCS is delivering flow -Monitor ability to keep core covered -Infer spray operation
Area Radiation Monitoring in Auxiliary Building and Control Room	-Determine if source of accident is outside containment building	-Monitor accessibility to plant zones/equipment -Monitor radioactivity release path to environment -Monitor effectiveness of cleanup/holdup systems -Monitor integrity of long-term cooling system -Monitor habitability of the control room
Core Exit Thermocouples	-None	-Determine if core is being cooled

\*Certain indications on this table are used as secondary diagnoses as the operator proceeds through Post Incident Recovery.

FIGURE C1  
NON-LOCA POST-TRIP EVENT TREE

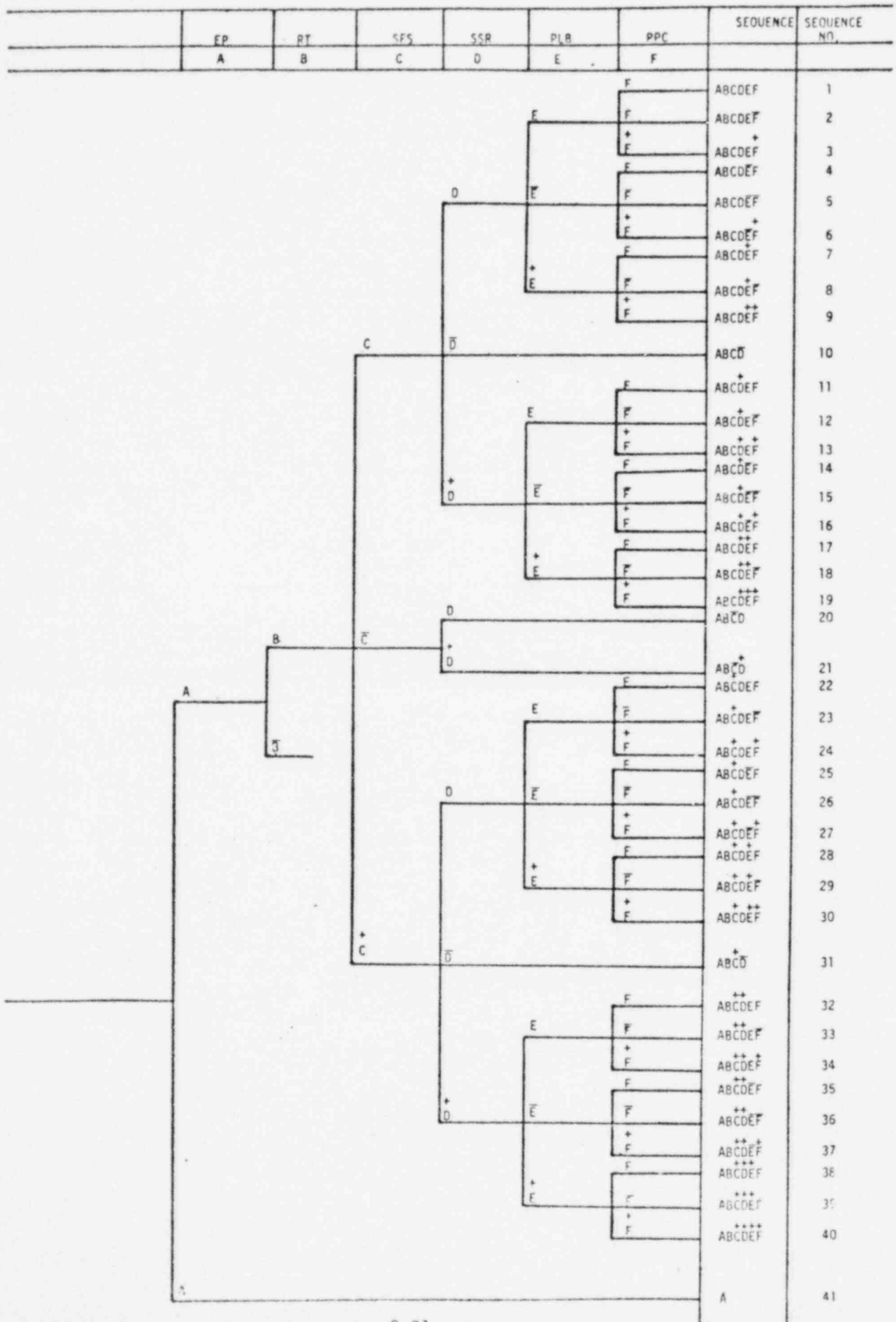


FIGURE C2  
SECONDARY FEEDWATER SYSTEM

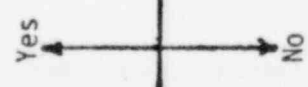
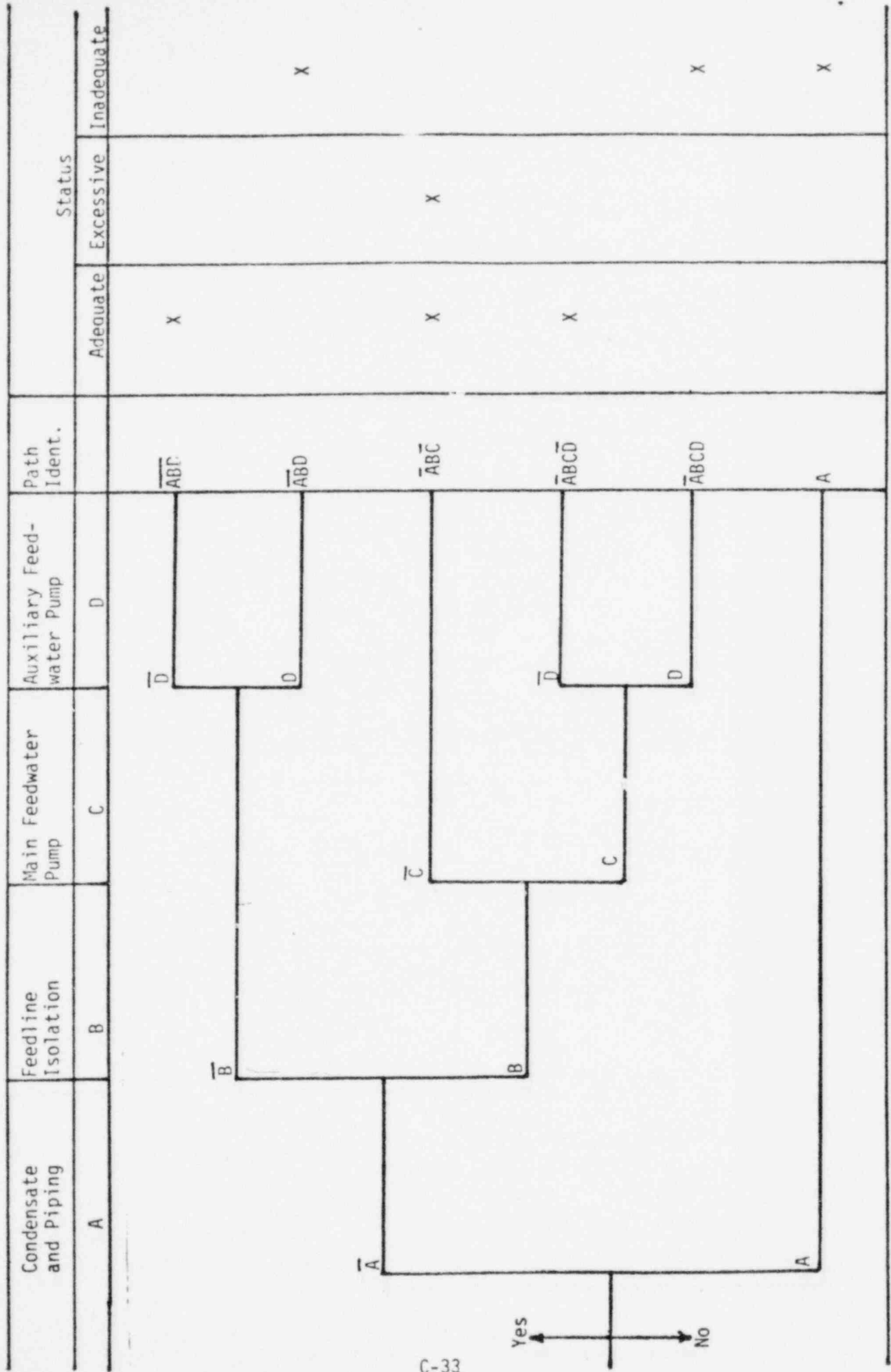
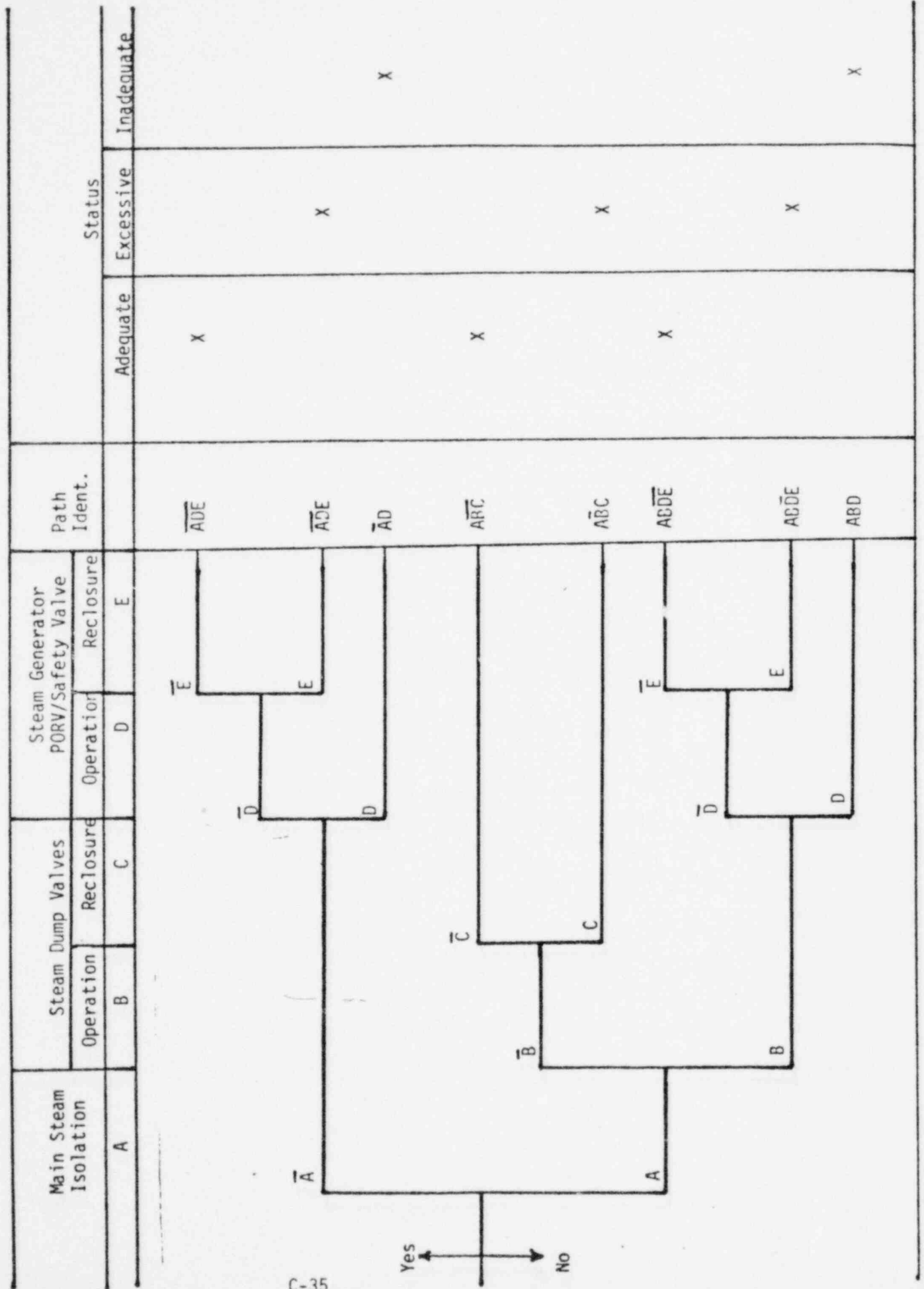


FIGURE C3  
SECONDARY STEAM RELIEF



Yes  $\leftarrow$   $\rightarrow$  No

FIGURE C-4  
PRIMARY INVENTORY AND BORON CONTROL

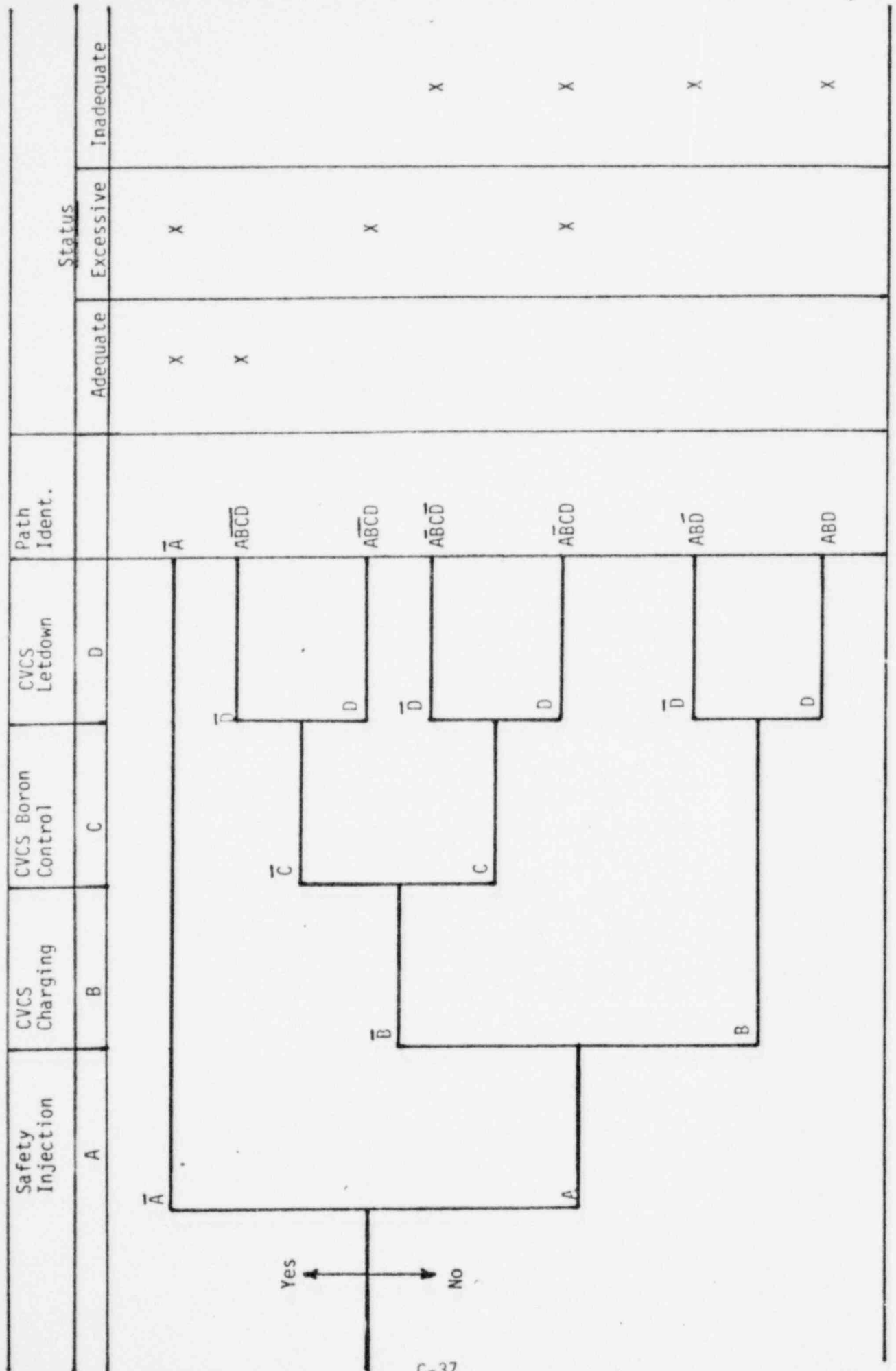


FIGURE C5  
PRESSURIZER PRESSURE CONTROL SYSTEMS

Pres. Spray (Main & Aux.)	Pressurizer Heaters	Pressurizer Relief/ Safety Valves		Path Ident.	Status			
		Operational	Reclose		Adequate	Depressurization	Overpressuriza- tion	
A	B	C	D					
<div style="display: flex; flex-direction: column; align-items: center;"> <span>C-39</span> <div style="margin: 10px 0;"> <span>Yes</span> ↑  <span>↓</span> <span>No</span> </div> </div>				$\overline{A}\overline{B}\overline{C}\overline{D}$	X			
				D	$\overline{A}\overline{B}\overline{C}D$		X	
			C		$\overline{A}\overline{B}\overline{C}D$			X
				D	$\overline{A}\overline{B}C\overline{D}$		X	
				D	$\overline{A}\overline{B}CD$		X	
			C		$\overline{A}\overline{B}C\overline{D}$			X
				D	$\overline{A}\overline{B}CD$		X	
				D	$\overline{A}B\overline{C}\overline{D}$			X
				D	$\overline{A}B\overline{C}D$		X	
			C		$\overline{A}B\overline{C}\overline{D}$			X
				D	$\overline{A}B\overline{C}D$		X	
				D	$\overline{A}BC\overline{D}$			X
			D	$\overline{A}BCD$		X		
		C		$\overline{A}BC\overline{D}$			X	
			D	$\overline{A}BCD$		X		
			D	$A\overline{B}\overline{C}\overline{D}$			X	
			D	$A\overline{B}\overline{C}D$		X		
		C		$A\overline{B}\overline{C}\overline{D}$			X	
			D	$A\overline{B}\overline{C}D$		X		
			D	$A\overline{B}C\overline{D}$			X	
			D	$A\overline{B}CD$		X		
		C		$A\overline{B}C\overline{D}$			X	
			D	$A\overline{B}CD$		X		
			D	$ABC\overline{D}$			X	
			D	$ABCD$		X		



TABLE C.4

NON-LOCA FAILURE MECHANISMS

Sequence No.	Sequence	Loss of Primary Inventory (LOCA)	Exceed Primary System Stress Limits (LOCA)	Exceed Secondary System Stress Limits (Feed/ Steamline Break)	Loss of Primary Secondary Heat Transport - (Inadequate Core Cooling)	Reactor Core Returns Critical
1	ABCDEF					
2	ABCDEF <sup>-</sup>					
3	ABCDEF <sup>+</sup>		X			
4	ABCDEF <sup>-</sup>	X			X	
5	ABCDEF <sup>-</sup>	X			X	
6	ABCDEF <sup>+</sup>	X	X		X	
7	ABCDEF <sup>+</sup>					
8	ABCDEF <sup>+</sup>		X			
9	ABCDEF <sup>++</sup>		X			
10	ABCDEF <sup>-</sup>	X		X		
11	ABCDEF <sup>+</sup>					
12	ABCDEF <sup>+</sup>					
13	ABCDEF <sup>++</sup>					
14	ABCDEF <sup>+-</sup>	X			X	X
15	ABCDEF <sup>+-</sup>	X			X	X
16	ABCDEF <sup>+-</sup>	X			X	X

TABLE C.4 (Cont)

NON-LOCA FAILURE MECHANISMS

Sequence No.	Sequence	Loss of Primary Inventory (LOCA)	Exceed Primary System Stress Limits (LOCA)	Exceed Secondary System Stress Limits (Feed/Steamline Break)	Loss of Primary Secondary Heat Transport - (Inadequate Core Cooling)	Reactor Core Returns Critical
17	ABCDEF <sup>++</sup>					
18	ABCDEF <sup>++-</sup>					
19	ABCDEF <sup>+++</sup>	X	X			
20	ABCD <sup>-</sup>	X			X	
21	ABCD <sup>-+</sup>	X			X	
22	ABCDEF <sup>+</sup>			X		
23	ABCDEF <sup>+</sup>			X	X	
24	ABCDEF <sup>++</sup>		X	X		
25	ABCDEF <sup>+-</sup>	X		X	X	X
26	ABCDEF <sup>+-</sup>			X	X	X
27	ABCDEF <sup>++</sup>			X	X	X
28	ABCDEF <sup>++</sup>			X		
29	ABCDEF <sup>+-</sup>		X			
30	ABCDEF <sup>+++</sup>		X			
31	ABCD <sup>+-</sup>			X	X	
32	ABCDEF <sup>++</sup>				X	

TABLE C.4 (Cont)

NON-LOCA FAILURE MECHANISMS

Sequence No.	Sequence	Loss of Primary Inventory (LOCA)	Exceed Primary System Stress Limits (LOCA)	Exceed Secondary System Stress Limits (Feed/Steamline Break)	Loss of Primary Secondary Heat Transport - (Inadequate Core Cooling)	Reactor Core Returns Critical
33	++ - ABCDEF					
34	++ + ABCDEF		X			
35	++ - ABCDEF	X			X	X
36	++ - ABCDEF	X			X	X
37	++ - ABCDEF		X		X	X
38	++ - ABCDEF					
39	++ - ABCDEF					
40	++++ ABCDEF		X			
41	A	X			X	

C-45