1-231-01-052-00

PROBABILISTIC EVALUATION OF LIQUID CHALLENGES TO SALEM UNITS 1 & 2 SAFETY VALVES

Submitted to:

PUBLIC SERVICE ELECTRIC & GAS COMPANY
Nuclear Department

Report Prepared by:

F. E. Gunnison
B. S. Singer

Principal Investigator

R. M. Crawford

SCIENCE APPLICATIONS, INC.
Oak Brook, Illinois
December 30, 1982

QUALITY ASSURANCE AUDIT FOR PROBABILISTIC EVALUATION OF LIQUID CHALLENGES TO SALEM UNITS 1 & 2 SAFETY VALVES

Science Applications, Inc.
Report 1-231-01-052-00
January 28, 1983

Total Pages ________

QUALITY ASSURANCE Sign-off

Prepared by: Forrest E. Gunnison Date 27 Jan 1983

Blake S. Singer Date 26 Jan 1983

Reviewed by: Blake Putney Date 24 Jan 1983

Approved by: Raymond M. Crawford Date 27 Jan 1983

QUALITY ASSURANCE AUDIT FOR PROBABILISTIC EVALUATION OF LIQUID CHALLENGES TO SALEM UNITS 1 & 2 SAFETY VALVES

Science Applications, Inc.
Report 1-231-01-052-00
January 28, 1983

This report was developed using the following materials:

1. B. S. Singer, and R. S. May, "Analysis of Safety/Relief Valve Chatter and Transient Problems," SAI Report to Commonwealth Edison, June 1982.

2. A. Meliksetian and A. M. Sulencar, "Valve Inlet Fluid Conditions for Pressurized Safety and Relief Valves in Westinghouse-Designed Plants," EPRI Research Project V102-19, January 29, 1982.

3. Zion Probabilistic Safety Study. Commonwealth Edison Company.

4. Reactor Safety Study: An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants, "NUREG-75/104, October 1975.

5. A. D. Swain and H. E. Guttman, "Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications," NUREG/CR-1278, October 1980.

6. W. H. Hubble and C. F. Miller, "Data Summaries of Licensee Event Reports of Valves at U.S. Commercial Nuclear Power Plants," NUREG/CR-1363, June 1980.

7. Salem Station, Units 1 & 2, Final Safety Analysis Report, Public Service Electric & Gas Company, July 1982.

8. W. W. Clark, et al. "EPRI/Wyle Power Operated Relief Valve Phase III Test Report; Volume III," EPRI Research Project V102-11, Phase III Interim Report, March 1982.

9. W. Q. Hagen, "Compressed Air and Backup in Nuclear Power Plants," Report by ORNL on a contract for NRC, to be published.

QUALITY ASSURANCE AUDIT (continued)

10. PSE&G Engineering & Construction Dept., Salem Nuclear Generating Station Nos. 1 and 2 Units,
    PSE&G System Description SD-N220, Residual Heat Removal System.
    PSE&G System Description SD-N100, Chemical and Volume Control System.
    PSE&G System Description SD-R200, Reactor Coolant System.
    PSE&G System Description SD-N600, Safety Injection System.

11. Salem Nuclear Power Station Unit 1,
    Operating Instruction II-3.3.2, Operating the Charging Pump.
    Operating Instruction II-3.3.1, Establishing Charging, Letdown, and Seal Injection Flow.
    Operationg Instruction II-1.3.6 Draining the Reactor Coolant System.
    Operating Instruction II-1.3.4 Filling and Venting the RCS.
    Operating Instruction II-6.3.2 Initiating Residual Heat Removal.
    Operating Instruction I-3.6 Hot Standby to Hot Cold Shutdown.
    Operating Instruction I-3.2 Cold Shutdown to Hot Standby.
    Operating Instruction I-3.1 Refueling to Cold Shutdown.

12. Salem Unit 1/Unit 2,
    Emergency Instruction I-4.24 Malfunction - Pressurizer Relief or Safety Valve.
    Emergency Instruction I-4.0 Safety Injection Initiation.
    Emergency Instruction I-4.2 Recovery From Safety Injection.

13. PSE&G, Test Performance Curve No. 34617-D, Pump Number 45604.

14. PSE&G, Test Performance Curve No. 34617-C, Pump Number 45603.

15. QX-300 Pump Performance Curve, Union Pump Company, Battle Creek, Michigan.

16. Salem Unit 1, Technical Specifications,
    3/4.4.4 Pressurizer.
    3/4.4.3 Relief Valves.
    3.4.9.3 Overpressure Protection Systems.

17. Salem Nuclear Generating Station No. 1 Unit Reactor Coolant Piping Diagram, 205201-A-8760.

18. Salem Nuclear Generating Station No. 2 Unit Reactor Coolant Piping Diagram, 205301-A-8762.

19. Salem Nuclear Generating Station No. 1 Unit Chemical & Volume Control Operation Piping Diagram, 205228-A-8761.

20. Salem Nuclear Generating Station No. 1 Unit Residual Heat Removal Piping Diagram, 205232-A-8761.

21. Salem Nuclear Generating Station No. 2 Unit Residual Heat Removal Piping Diagram, 205332-A-8763.

QUALITY ASSURANCE AUDIT (continued)

22. Salem Nuclear Generating Station No. 2 Unit Safety Injection Piping Diagram, 205334-A-8763.

23. Salem Nuclear Generating Station Unit No. 1 Pressurizer Instrument Schematic, 211310-B-9508.

24. Salem Nuclear Generating Station No. 1 & 2 Units - Residual Heat Removal System No. 11SJ44, 21SJ44, 11RH4, 21RH4, 1RH2 & 2RH2 Suction Isolation Valves Schematic Controls 211504-ABL-583, 211505-B-9771.

25. Salem Nuclear Generating Station No. 1 & 2 Units - Residual Heat Removal System No. 12SJ44, 22SJ44, 12RH4, 22RH4, 1RH1 & 2RH1 Suction Isolation Valves Schematic Controls 211507-B-9771.

26. Salem Nuclear Generating Station No. 1 Unit Control Console Bezel, Residual Heat Removal, Pressurizer Relief Tank 202050-B-9461.

27. Salem Nuclear Generating Station No. 2 Unit Control Console Bezel, Residual Heat Removal, Pressurizer Relief Tank 228475-B-9585.

28. Salem Nuclear Generating Station No. 1 & 2 Units - Residual Heat Removal System No. 11SJ44, 21SJ44, 11RH4, 21RH4, 1RH2 & 2RH2 Suction Isolation Valves Logic Diagram 224389-B-9567.

29. Salem Nuclear Generating Station No. 1 & 2 Units - Residual Heat Removal System No. 12SJ44, 22SJ44, 12RH4, 22RH4, 1RH1 & 2RH1 Suction Isolation Valves Logic Diagram 224390-B-9567.

30. Salem Nuclear Generating Station No. 1 & 2 Units - Reactor Coolant System No. 13, 23, 14, & 24 Reactor Coolant Loops Low Flow and Reactor Coolant Pressure Functional Diagram 220413-B-9542.

31. Salem Nuclear Generating Station No. 1 & 2 Units - Reactor Coolant System No. 11, 21, 12, 22, 13, 23, 14, & 24 RC Loops Wide Range Temperature Recorders Functional Diagram 220414-B-9542.

32. Salem Nuclear Generating Station No. 1 & 2 Units - Pressurizer 1PR6, 2PR6, 1PR7, & 2PR7 Pressurizer Relief Stop Valves Logic Diagram 231356-B-9601.

33. Salem Nuclear Generating Station No. 1 & 2 Units - Pressurizer 1PR1, 2PR1, 1PR2, & 2PR2 Pressurizer Power Relief Valves Logic Diagram 231357-B-9601.

34. Salem Nuclear Generating Station No. 1 Unit Pressurizer Power Relief and Stop Valves and Overpressure Protection System Channel 1 Schematic, 241106-B-9661, 241107-B-9661.

35. Salem Nuclear Generating Station No. 1 & 2 Units - Pressurizers Overpressure Protection System Channels I and II RC Temperature and Pressure Channel Selection Schematic, 241108-B-9661, 241109-B-9661.

QUALITY ASSURANCE AUDIT (continued)

36. Salem Nuclear Generating Station No. 1 & 2 Units - Pressurizers Overpressure Protection System Channel I Control and Indications Logic Diagram 242508-B-9673.

37. Salem Nuclear Generating Station No. 1 & 2 Units - Pressurizers Overpressure Protection System Channel II Control and Indications Logic Diagram 242524-B-9673.

38. Salem Nuclear Generating Station No. 1 & 2 Units - Pressurizers Overpressure Protection System Channels I & II Control and Indications Functional Diagram 242880-B-9678.

39. Salem Nuclear Generating Station No. 1 Unit Pressurizer Power Relief and Stop Valves and Overpressure Protection System Channel II Schematic 242881-B-9678, 242882-B-9678.

40. Salem Nuclear Generating Station No. 2 Unit Pressurizer Power Relief and Stop Valves and Overpressure Protection System Channel I Schematic 244082-B-9679.

41. Salem Nuclear Generating Station No. 2 Unit Pressurizer Power Relief and Stop Valves and Overpressure Protection System Channel II Schematic 244084-B-9679, 244085-B-9679.

42. Public Service Electric & Gas Company, Engineering Department, Controls Division, Salem Nuclear Generating Station Unit No. 1 & 2, Functional Specification: CD-S-10, Pressurizer Overpressure Protection System, Rev. 1, 7/19/78.

43. Public Service Electric & Gas Company, Design Memorandum, SGS/M-DM-042, Reactor Coolant System Overpressurization No. 1 & 2 Units, Salem Nuclear Generating Station, 9/1/77.

44. Public Service Electric & Gas Company, Design Memorandum, SGS/M-DM-062, Reactor Coolant System Overpressurization No. 1 & 2 Units, Salem Nuclear Generating Station, 10/21/77.

45. Public Service Electric & Gas Company, Design Memorandum, SGS/M-DM-067, Reactor Coolant System Overpressurization Units No. 1 & 2, Salem Nuclear Generating Station, 1/25/78.

46. Reactor Coolant System Overpressurization Overpressure Protection No. 1 Unit Salem Nuclear Generating Station Docket No. 50-272, October 26, 1977.

QUALITY ASSURANCE AUDIT (continued)

47. "Pressure Mitigating Systems Transient Analysis Results," Westinghouse Electric Corporation, July 1977.

48. Letter from Frank Sullivan, PSE&G, Newark Engg. & Constr., to Mr. Russ Eldridge, Crosby Valve & Gage Co., Wrentham, Mass., Subject: PSE&G P.O. 757343 Mark DA-13 (3L4) Safety Valve, Salem Generating Station.

49. Letter from L. Reiter, Manger-Systems Engineering, PSE&G to E. Liden, Manager-Licensing & Regulation, PSE&G, Subject: NUREG-0737 Item II.D.1, PWR Safety & Relief Valve Test Program, Salem Generating Station Units 1 & 2, June 28, 1982.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1 INTRODUCTION

Based upon the requirements of NUREG-0737[1], owners of nuclear power plants must perform plant-specific evaluations to ensure that the Power Operated Relief Valves (PORVs) and spring-loaded Safety Valves are operable and provide effective pressure relief under the possible range of discharge conditions. The Electric Power Research Institute (EPRI) has conducted the PWR Safety and Relief Valve Test Program[2] to provide a generic basis for addressing these requirements.

The EPRI PORV tests show that PORVs successfully open and reseat for saturated steam, saturated liquid, and subcooled liquid inlet conditions. Thus, the tests demonstrated that PORVs will operate for all expected fluid inlet conditions.

EPRI experimental results, as well as various independent analyses[3,4], have shown that saturated liquid and subcooled liquid discharge constitute the most severe challenges to safety valves and the associated piping networks. There are two major reasons for further investigation of safety valve liquid discharge.

First, safety valves open with stroke times of 50 milliseconds or less, so that the discharge piping may experience large dynamic loads as a wave front of liquid enters pipe segments. PORVs open more slowly over periods of one-half to one second, and thus give rise to smaller dynamic loads. Since piping loads are proportional to mass flow rate, loads associated with liquid flow can be up to six times greater than those associated with steam flow. Thus, from the point of view of discharge piping stresses, liquid discharge through a safety valve represents more severe dynamic loading conditions.

Second, EPRI test results and independent analyses[5] show that plants with long safety valve inlet piping may be subject to continuing chatter oscillations of the spring loaded valve. Such oscillatory behavior is most likely for subcooled liquid discharge, because the high mass flow rate generates waterhammer pressure waves of large amplitude. Short-term oscillatory behavior may also be observed during the expulsion of subcooled liquid loop seals.

For each of these issues, the situation is most severe for far-subcooled liquid discharge, which gives the maximum mass flow rates. Saturated or "slightly-subcooled" liquid discharge are of less concern since flashing at the valve causes two-phase flow effects that substantially reduce the mass flow rate and thus tend to mitigate the event.

Liquid discharge, while admittedly a conceivable transient event, is extremely unlikely when considered in the context of available systems, operating procedures, time for operator action, and frequency of the initiating events. Although a probabilistic analysis of liquid discharge provides no information on valve oscillations or discharge piping stresses, it does provide a rational basis for defining realistic inlet fluid conditions that are significant in the analysis of safety valve performance and discharge piping loads. Further, scenarios which may result in subcooled liquid discharge and the associated high piping stresses can be placed in perspective with a probabilistic analysis. The relative frequency of occurrence of such scenarios will indicate if they merit consideration as a potential loss-of-coolant-accident (LOCA). That is, a subcooled safety valve liquid discharge scenario in which a valve and a discharge piping failure is postulated to occur is not a significant contributor to the probability of a LOCA for the Salem plant unless its frequency is of the same approximate order of magnitude as other LOCA initiators. Even if it is postulated that as the result of a liquid challenge, a safety valve fails open and the discharge piping ruptures, the consequences of this accident are bounded by the Salem Design Basis Accident. Thus, any event which has both a low frequency of occurrence as well as low consequences relative to the design basis, is not a safety concern.

The present study uses techniques[6] from Probabilistic Risk Assessment to evaluate the frequency at which safety valve liquid discharge may be encountered in the Salem Nuclear Stations of Public Service Electric & Gas Company. SAI has performed similar analyses for other PWRs and has also evaluated the risks of liquid discharge in Boiling Water Reactors. Based upon a previous generic analysis by Westinghouse[7], and upon additional plant-specific calculations, event trees are developed to qualitatively describe the event sequences which may cause safety valve liquid discharge, and to identify the system functions and operator actions which may favorably or unfavorably affect the outcome. Fault tree analysis is then used to quantitatively evaluate the failure probabilities for the required system and operator responses. Previous research results[8,9,10,11] for event initiation frequencies, component failure rates, and human error probabilities are used where applicable.

Results show that liquid discharge from the pressurizer safety valves is extremely unlikely for the Salem plants. Subcooled liquid discharge may occur at the rate of 6.0E-8 events/reactor unit-year. Saturated liquid discharge may occur with a frequency of 4.0E-8 events/reactor-year.

2 EVENT TREE ANALYSIS

2.1 Transients That May Result in Pressurizer Safety Valve Liquid Discharge

In support of the EPRI/PWR Safety and Relief Valve Test Program, Westinghouse performed a generic evaluation of the expected range of fluid inlet conditions for pressurizer safety and relief valves for Westinghouse plants. The resulting report[7] provides a comprehensive discussion of all transients with the potential for safety valve discharge as well as bounding calculations for the actual conditions to be expected by 2-loop, 3-loop, and 4-loop plants.

The Westinghouse report provides the starting point for our analysis. However, as a generic bounding analysis the Westinghouse report quite properly assumes multiple system failures without evaluating their likelihood, and fails to take credit for plant-specific characteristics which mitigate the events. The present report modifies the important Westinghouse sequences in accordance with the plant-specific characteristics of Salem Units 1 & 2, and evaluates the frequency of these sequences by incorporating results of fault tree analyses described in Section 3.

Safety valve liquid discharge (of any kind) can occur only if the pressurizer pressure reaches the safety valve setpoint of 2485 psig with the pressurizer water solid. The Westinghouse report identified the transients "potentially" leading to liquid discharge as:

FSAR Events

(a) Feedwater Pipe Rupture
(b) Accidental Depressurization of the Secondary System
(c) Small Steam Line Rupture[+]
(d) Loss of All Feedwater

Extended High Pressure Injection Events

(a) Spurious Safety Injection

[+] Although a small steam line rupture is usually not considered in FSAR analysis, Westinghouse includes this event with the FSAR events.

Cold Overpressurization Events
(a) Mass Input
(b) Heat Input

The feedwater pipe rupture will be the FSAR event analyzed. This selection is based upon the conclusions of the Westinghouse report which state:[7]

> Past analysis indicates that the most limiting transient resulting in liquid discharge through the PORV and safety valve is the feedline break accident. Water discharge through safety and relief valves is predicted during standard SAR analysis of feedline breaks.

For the other FSAR events the operators have on the order of thirty minutes to analyze the situation and take appropriate action. Liquid challenges to the safety valves for these events can be prevented by controlling the safety injection flow. Salem emergency operating procedures specifically describe conditions for which safety injection should be terminated.[12] Thus, considering the time for operator action, Westinghouse's conclusion that the remaining events will not normally result in liquid challenges to the safety valves is appropriate.

A spurious safety injection at power will be analyzed as the extended high pressure injection event.

For cold overpressurization events the mass input event will be analyzed because it is:

1) more likely to occur; and
2) less easily mitigated because it may be a very fast event.

2.2 Feedwater Pipe Rupture Event

A feedwater pipe rupture, if large enough, can prevent the addition of sufficient feedwater into the steam generators to sustain shell-side fluid inventory. Should the large break occur between the check valve and the steam generator, the water can quickly discharge through the break causing a rapid loss of heat sink in the affected loop. Depending upon the size of the break and the plant operating conditions at the time of the break, the break could cause either a reactor coolant system (RCS) cooldown, or a reactor coolant system heatup[3]. The actual RCS pressure and temperature history for this event will depend not only on the break characteristics and the plant operating conditions, but also on factors such as the timing of the reactor trip, safety injection, and auxiliary feedwater initiation. However, the conservative Westinghouse generic report shows that for this event[7], the maximum liquid surge rate for Salem Units 1 & 2 into the pressurizer when the safety valve is passing liquid is 646.3 gpm of approximately 650°F water. The EPRI tests indicate that one Salem PORV can relieve about 1,800 gpm of 643°F water at 2573 psia.[15] Thus, if one PORV is available, this event will not challenge the safety valves.

No credit is taken for operator action in mitigating this event. However, operator action to control the charging pumps would effectively terminate the repressurization. Salem operating procedures[12] require such action once the pressurizer pressure has stabilized and begun its increasing trend.

The initiation frequency of this event is small, because it involves a large break in the relatively short stretch of piping between the check valve and steam generator. Based upon the WASH-1400 pipe failure probability of 4.0E-6/year-section* the initiation frequency is chosen to be 4.0E-6 events/reactor-year. The PORV system failure probability is computed in Section 3 to be 6.0E-4 for Unit 1 and Unit 2. These probabilities are used in the simple event tree shown in Figure 2.1.

The event tree shows that for both Salem Units, liquid challenges to the safety valves as a result of a main feedwater pipe rupture have a small frequency which would be even smaller if operator action were included. Thus, the potential problems associated with such challenges are not a significant factor in considering the plants' safety. Further, should such a challenge result in valve and discharge piping failure, the consequences of the event are bounded by the Salem Design Basis Accident.

* 4.0E -6 = 4×10^{-6} = 0.000004

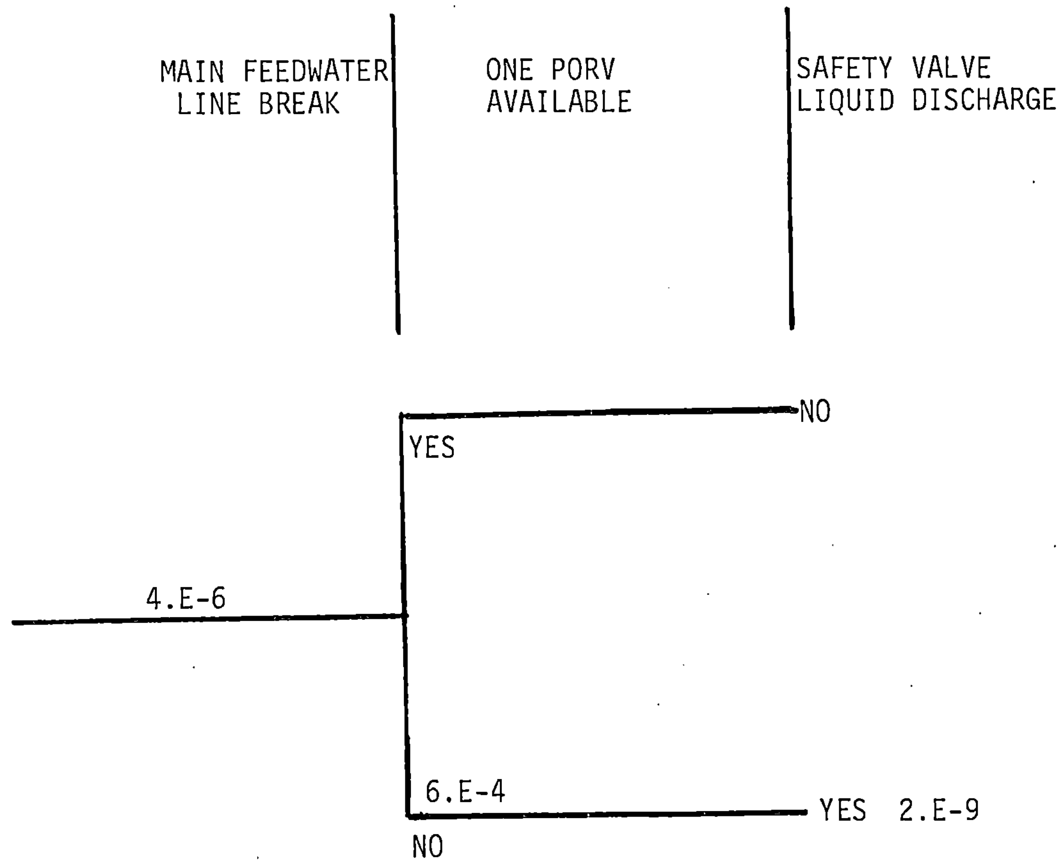


FIGURE 2.1

MAIN FEEDWATER LINE BREAK EVENT TREE

If the PORV block valves are closed because of PORV leakage, the PORVs would not be available to mitigate this event. If it is assumed that both block valves are closed immediately after returning to power from cold shutdown, then the probability of a liquid challenge is just the initiation frequency for the event, 4.0E-6 per reactor year. If both PORVs are isolated at some later time, then the fraction of the year left before shutting down for refueling times this value would give the anticipated frequency. If, however, only one PORV is isolated, then the probability of a liquid challenge is the initiation frequency, 4.0E-6, times the estimated failure probability for the other PORV (9.0E-3 for either Unit 1 or Unit 2). Thus, with one PORV isolated the probability of a liquid challenge is 4.0E-8 per reactor year for Unit 1 or Unit 2. Again, if the isolation is less than a year in duration these values must be reduced for the appropriate time scale.

In summary, a main feedline pipe rupture will present a liquid challenge to the safety valves with the following frequencies:

Condition	Unit 1 (events/reactor yr.)	Unit 2 (events/reactor yr.)
At Power	2.0E-9	2.0E-9
At Power, One PORV Isolated	4.0E-8	4.0E-8
At Power, Both PORVs Isolated	4.0E-6	4.0E-6

2.3 Extended High Pressure Injection at Power

Spurious actuation of the safety injection system can be caused by operator error (manual actuation) or by a false actuating signal in any of the following channels:[13]

1. High containment pressure;
2. High steam line differential pressure; or
3. High steam line flow and low average coolant temperature or low steam line pressure.
4. Pressurizer low pressure.

This event has a fairly high frequency of occurrence, but it is also very easy to detect and terminate. Analysis of generic data[8] for PWRs indicates that the event has a frequency of 1.6×10^{-1} events/reactor-year.

The spurious Safety Injection Signal (SIS) results in a reactor trip and a turbine trip. The letdown is automatically isolated and is, therefore, unavailable for pressure relief. The centrifugal charging pumps force highly borated water into four primary cold legs. Since there is no letdown (which in any case does not have sufficient capacity for mitigation) the primary loop water inventory steadily increases. Following the trip, the pressure first drops due to the coolant contraction but the continuous action of the charging pumps repressurizes the primary coolant system. If the charging pumps are not stopped, the safety valves (assuming the PORVs are not available) would lift on saturated steam and as the pressurizer continued to fill, saturated or slightly subcooled liquid would eventually be discharged. Only if the operators fail indefinitely to recover from the safety injection is there a potential for highly subcooled liquid discharge. The transition from saturated steam to saturated liquid discharge reduces the potential for chatter instability as well as the amplitude of dynamic loads on discharge piping.

The successful operation of only one PORV is sufficient to remove liquid supplied by both charging pumps and thus to eliminate the possibility of safety valve liquid discharge. The first branch of the event tree of Figure 2.2 reflects this fact. In the fault tree evaluation of PORV availability, no credit is taken for operator actuation of the PORVs.

Given that both PORVs fail, a simple mass balance shows that at least 20 minutes is required for the pressurizer bubble to collapse and for liquid discharge to occur. However, there are specific operating procedures[12] for recovery from safety injection which will require the operator to reset the SIS within a few minutes. Further, this is an event which is neither extremely rare nor difficult to interpret, so there is a high likelihood that the event will be successfully terminated by the operator. The human response is analyzed in Section 3.3. The computed human error probabilities are expected to be very conservative, because the 20 minute response time is expected to be a conservative estimate.

Using the numerical results from Section 3, the frequency for safety valve liquid discharge following a spurious safety injection is 4.0E-8 events/reactor-year.

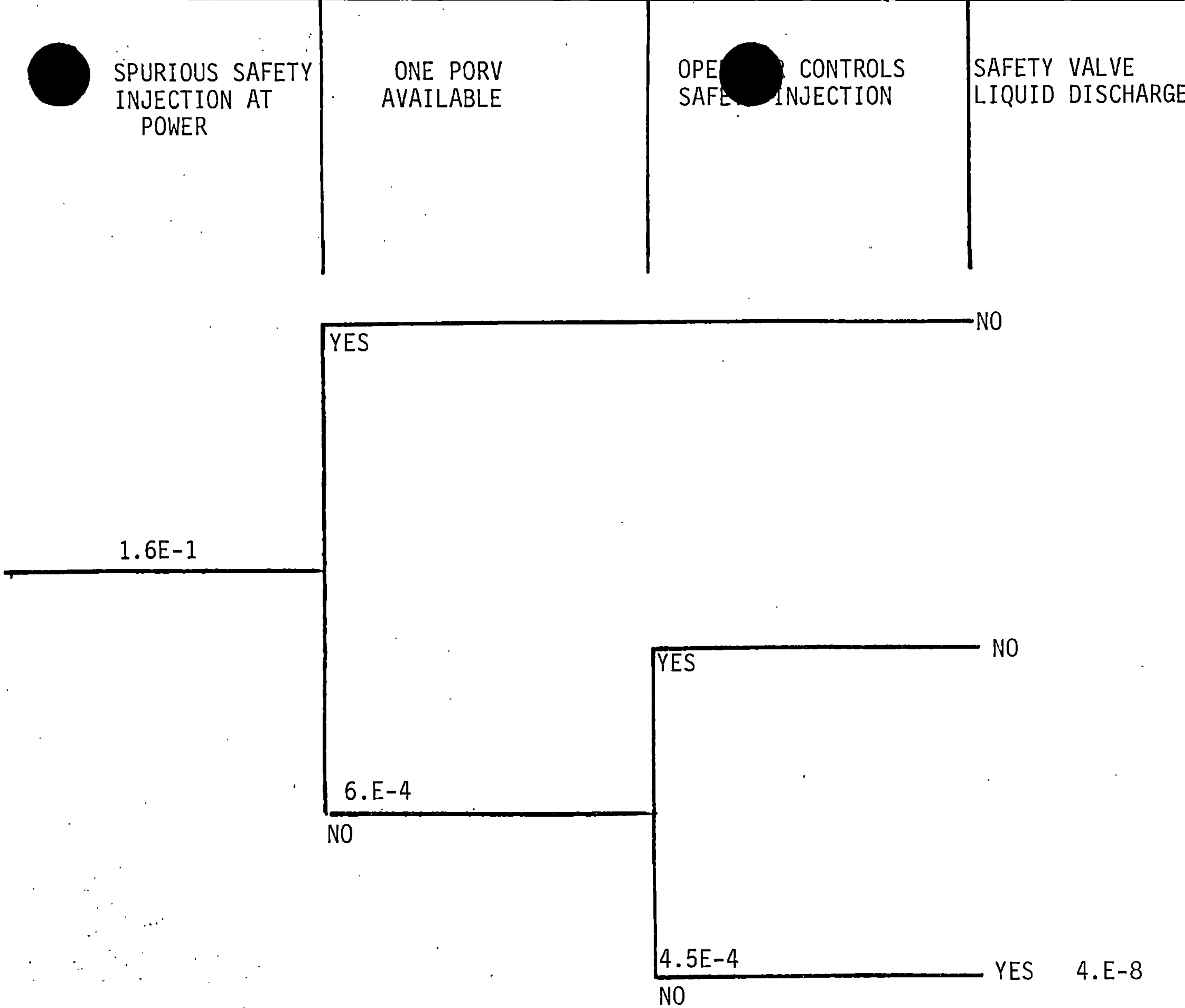


FIGURE 2.2
SPURIOUS SAFETY INJECTION AT POWER EVENT TREE

Again, this frequency is sufficiently small that potential consequences of a liquid challenge are not a concern in plant safety, and in any case, the consequences of such challenges are bounded by the Salem Design Basis Accident.

For this scenario, given that both PORVs are isolated, the probability of a liquid discharge is the initiation frequency (1.6E-1) times the probability that the operators do not terminate the injection (4.5E-4). Thus, for both PORVs isolated, the probability of a liquid challenge is 7.0E-5 per reactor year. If only one PORV is isolated then the frequency of 7.0E-5 must be multiplied by the probability that the remaining PORV fails. For one PORV isolated the frequency of liquid challenge is 6.0E-7 per reactor year.

Thus, a spurious safety injection will present a liquid challenge to the safety valves with the following frequencies:

Condition	Units 1 & 2 (events/reactor yr.)
At Power	4.0E-8
At Power, One PORV Isolated	6.0E-7
At Power, Both PORVs Isolated	7.0E-5

Notice that if both PORVs are isolated for an extended period of time, the frequency of this event approaches that of a LOCA. However, the consequences of such a liquid challenge postulating that both the valve and discharge pipe fail are certainly bounded by the LOCA design basis analysis. Further, as explained previously, this frequency is based on a conservative estimate of the minimum operator response time. A more detailed transient analysis is necessary to determine a more realistic time for operator action.

2.4 Cold Overpressurization

2.4.1 Salem Pressurizer Overpressure Protection System

A cold overpressurization event represents the greatest potential for subcooled safety valve discharge. If the reactor is in cold shutdown-water solid condition then subcooled liquid is present throughout the primary loop and any safety valve discharge will be at maximum mass flow rates. Thus, cold overpressurization presents the greatest problems with respect to waterhammer instability and safety valve discharge piping loads. To mitigate any such potential problems, Salem administrative procedures require that the pressurizer not be water solid unless the reactor coolant system (RCS) is going to be drained, or maintenance requirements necessitate the water solid condition. Therefore, the RCS is water solid only for the time necessary to complete system cooldown. Since such intervals are of short duration, the potential for cold overpressurization with a water solid system is minimal.

In addition to maintenance of a pressurizer bubble at cold shutdown, Salem Units 1 & 2 have a pressurizer overpressure protection system (POPS) which is designed to prevent subcooled liquid challenges to the safety valves from either mass or heat input events at cold shutdown. Unit 1 POPS utilizes a 375 psi setpoint for the PORVs whenever the reactor coolant system temperature is less than 312°F. To supplement the PORVs relief capability, the Unit 1 residual heat removal (RHR) system suction relief valve (RH3) also has a 375 psi relief setting. The capacity of this valve is 840 gpm. Unit 2 POPS consists of two electrically operated solenoid valves in parallel with the PORVs. These valves also open whenever the RCS pressure is greater than 375 psi and have a relief capacity similar to that of the PORVs. (While it is not considered a part of the POPS Unit 2 also has a RHR suction relief valve which has a 450 psi relief setting.)

Salem Operating Procedures require that the operators activate the POPS whenever the RCS temperature is less than 312°F. For each unit there are two independent POPS channels. If the operators fail to activate the POPS an alarm is activated when the RCS temperature falls below 312°F. Arming the POPS opens the PORV stop valves. The main design criteria for the POPS are:

1. Conformance to IEEE-279 and the single failure criterion.
2. Conformance to Seismic I requirements.
3. No operator action until ten minutes after the initiation of a pressure transient.
4. Testability.

In going to cold shutdown, when the RCS temperature reaches 350°F several system changes are completed. First, the electrical supplies to both safety injection pumps and one centrifugal charging pumps are de-energized, the circuit breakers re racked out, and the DC control power is turned off. Also, when the temperature is less than 350°F and the RCS pressure is less than 375 psi the residual heat removal (RHR) system is placed in operation. Thus, upon RHR initiation one centrifugal charging pump and the positive displacement pump are available. The POPS is not armed until the RCS temperature reaches 312°F. There is at least 30 minutes during which a system component failure or a inadvertent operator action could initiate a overpressurization event and the POPS would not be available. However, during this interval the RHR suction relief valve and the PORVs are available for overpressure protection. After the RHR is successfully placed in operation and the system is cooled to 312°F, the entire POPS system will be available.

To analyze the cold overpressurization event two RCS scenarios have been studied:

1) Cold Overpressurization Prior to Arming POPS

   RCS Temperature greater than 312°F
   RCS Pressure less than 375°F; and

2) Cold Overpressurization at Cold Shutdown (POPS Armed)

   RCS Temperature less than 200°F
   RCS Pressure in range of 100-200 psi.

The question may logically be asked as to why the range of RCS temperatures between 312°F and 200°F is not considered. Over this range two changes of interest occur: 1) the reactor coolant pumps (RCP) are taken out of operation, and 2) the power to the remaining centrifugal charging pump is removed. The inadvertent operation of a RCP may produce a heat input event. But this event is not being analyzed because the mass input event is more likely to occur and less easily mitigated. Consequently the heat input event will not be considered further. However, inadvertent operation of the centrifugal charging pump could initiate a rapid overpressurization event. Since the Salem operators receive training on the procedure for approaching cold shutdown and they perform the actual operation at least yearly, the probability that they would inadvertently start the centrifugal charging pump is considered to be small in comparison to the probability of other initiating events. Also, for each of the two cases that will be considered no credit is taken for operator action to mitigate the event. Hence, the outcome is dependent upon a differentiation of which mechanism initiated the event. Therefore, the two ranges of operation adequately represent the potential configurations for a cold overpressurization event.

2.4.2 Cold Overpressurization Prior to Arming POPS

System Configuration Prior to POPS Initiation

For this analysis the PORV availability will be the same as the "at power" situation discussed in Section 3. The RHR is assumed to be placed in operation, i.e., the RHR suction isolation valves (RH1 and RH2) are open and the RHR suction relief valve is available. (See Figure 2.4.)

Initiators

Any incident which causes an enhanced mass input to the primary coolant system can cause an overpressurization event. Historically, the potential initiators can be broken into two general categories:

1) Inadvertent Pump Actuation; and
2) Letdown - Charging Mismatch

As discussed previously, the inadvertent actuation of the centrifugal charging pump, or the failure to remove power from the safety injection pumps and then the activation of one of these pumps, is considered to be a very improbable event.

The inadvertent activation of a pump would require a sequence of actions similar to that described in Section 3 for the inadvertent operator closure of a motor operated valve. However, the value obtained there of 3×10^{-5} events per cold shutdown is conservative for inadvertent pump operation because the alarms and sensors activated by such operation should result in a prompt recovery. Therefore, a reasonable estimate of inadvertent pump operation would be less than 3×10^{-6}. In comparison to the other initiators that will be discussed, this probability is not significant.

As the RHR system is brought on-line the letdown path from the RHR system to the Chemical and Volume Control System (CVCS) is established. A failure to establish this path could result in charging - letdown mismatch. This path will not be established if both manuals valves 11RH17 and 12RH17 are not opened, or if valve CV8 fails upon demand. The failure to open RH17 would, at a minimum, require a failure to carry out a specific oral instruction to change a valve (1×10^{-3}) and improper use of the valve check-off list (.5). Thus, the probability that 11RH17 (12RH17) is not opened is less than 5×10^{-4}. The probability of air-operated valve CV8 failing to operate on demand is 2×10^{-3}. As discussed in the next section the inadvertent closure of CV18 or the failing plugged of CV18, or certain motor operated valves in the RHR can also cause a mismatch. However, since the time-frame for this scenario is small (less than 8 hours) these failures are not significant in comparison to the failures described here. Therefore, the initiator for this scenario will be taken as 3×10^{-3} events per reactor year.

<u>Event Tree for Cold Overpressurization Prior to Arming POPS</u>

Since this event is assumed to occur after the RHR suction isolation valves are opened, the RHR suction relief valve (with a setpoint of 375 psi for Unit 1 and 450 psi for Unit 2) can provide RCS pressure relief. Its 840 gpm relief capacity is sufficient to relieve the output from either or both the Positive Displacement Charging Pump (PDCP) and the centrifugal charging pumps. If it is available, there is no liquid challenge to the safety valves. If the RHR suction relief valve is not available (see Section 3.6), one PORV has sufficient capacity to prevent a safety valve liquid challenge. For this scenario the applicable PORV control logic and availability probability is the "at power" case developed in Section 3. Using these probabilities, the probability of a cold overpressurization event prior to arming POPS is 2.0E-9 events per reactor year. (See Figure 2.3.)

2.4.3 Cold Overpressurization at Cold Shutdown

<u>System Configuration at Cold Shutdown</u>

For the cold shutdown scenario the residual heat removal system is successfully operating with letdown from the RHR system to the Chemical and Volume Control System (CVCS). The charging flow is provided by the positive displacement

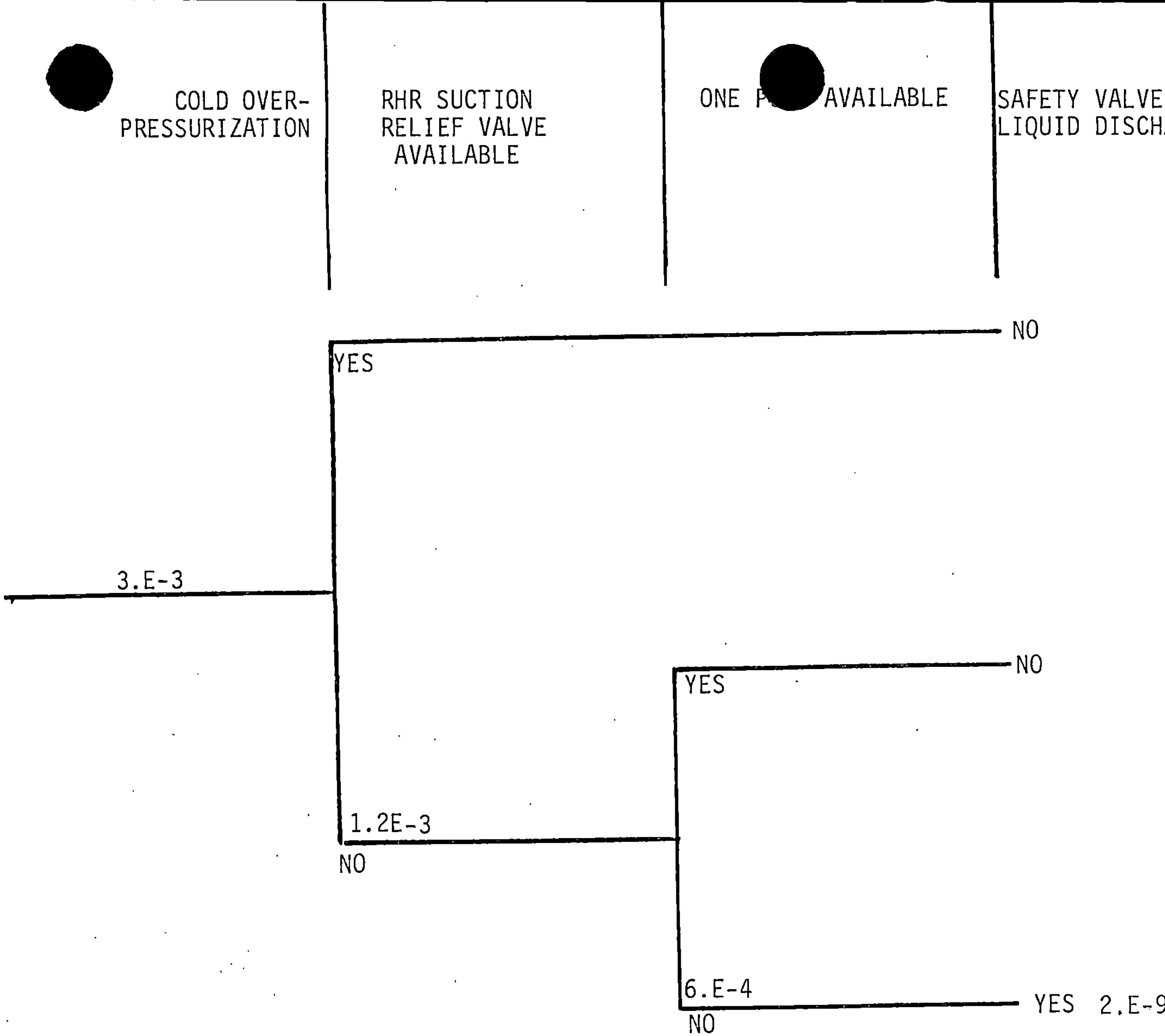


FIGURE 2.3

COLD OVERPRESSURIZATION PRIOR TO ARMING POPS EVENT TREE rging pump (PDCP) in the CVCS. The PDCP and the letdown pressure control valve 18) are in manual operation. Also, the letdown path from the reactor coolant cold leg is typically open. Figure 2.4 shows a simplified piping diagram for the RHR and CVCS at cold shutdown. For this scenario, only one loop of the RHR is in operation. The other loop is isolated. This is a conservative assumption since if conditions permit, one RHR pump may be stopped, but the loop is not isolated.

Initiators

At cold shutdown the PDCP is used to provide charging flow. Typically this pump must supply about 75 gpm to the primary coolant system. For this analysis, the charging pump will be assumed to be at full flow (98 gpm). Thus, inadvertent control of the PDCP or the charging flow control valve (CV71) will not increase the charging flow, and so these actions are not considered as event initiators. This is a conservative assumption since it implies that the probability of an operator error in manipulating these components is 1.0. Inadvertent operation of centrifugal charging pumps or the safety injection pumps could also initiate s event. However, in comparison to other potential initiators, the probability of such an occurrence is judged to be extremely small since it would require several administrative and operator errors.

The initiators of concern are those which can isolate the letdown. Since only one loop of the RHR is in operation, failure of either manual valve RH17 or the motor operated valves RH1, RH2, or RH4 would isolate the letdown flow. In the CVCS system, failure of the air operated valves, CV8 or CV18, can also isolate the letdown. The letdown line from the RCS cold leg to the CVCS could provide an alternate path if CV8 or any valve in the RHR system failed. However, since the letdown orifices have a very high resistance to flow, this path provides little flow relief at low pressures. Thus, no credit is taken for this path. Again this is a conservative assumption, since after a postulated valve failure, as the RCS pressure increases the flow through this path will also increase. The net effect would be to either mitigate the event prior to liquid challenge to the safety valves, or to increase the time available for operator action.

determine the frequency of this event failure of the four valves, RH4, RH17, CV8, and CV18, was considered as one initiator (Case 1), and the failure of the

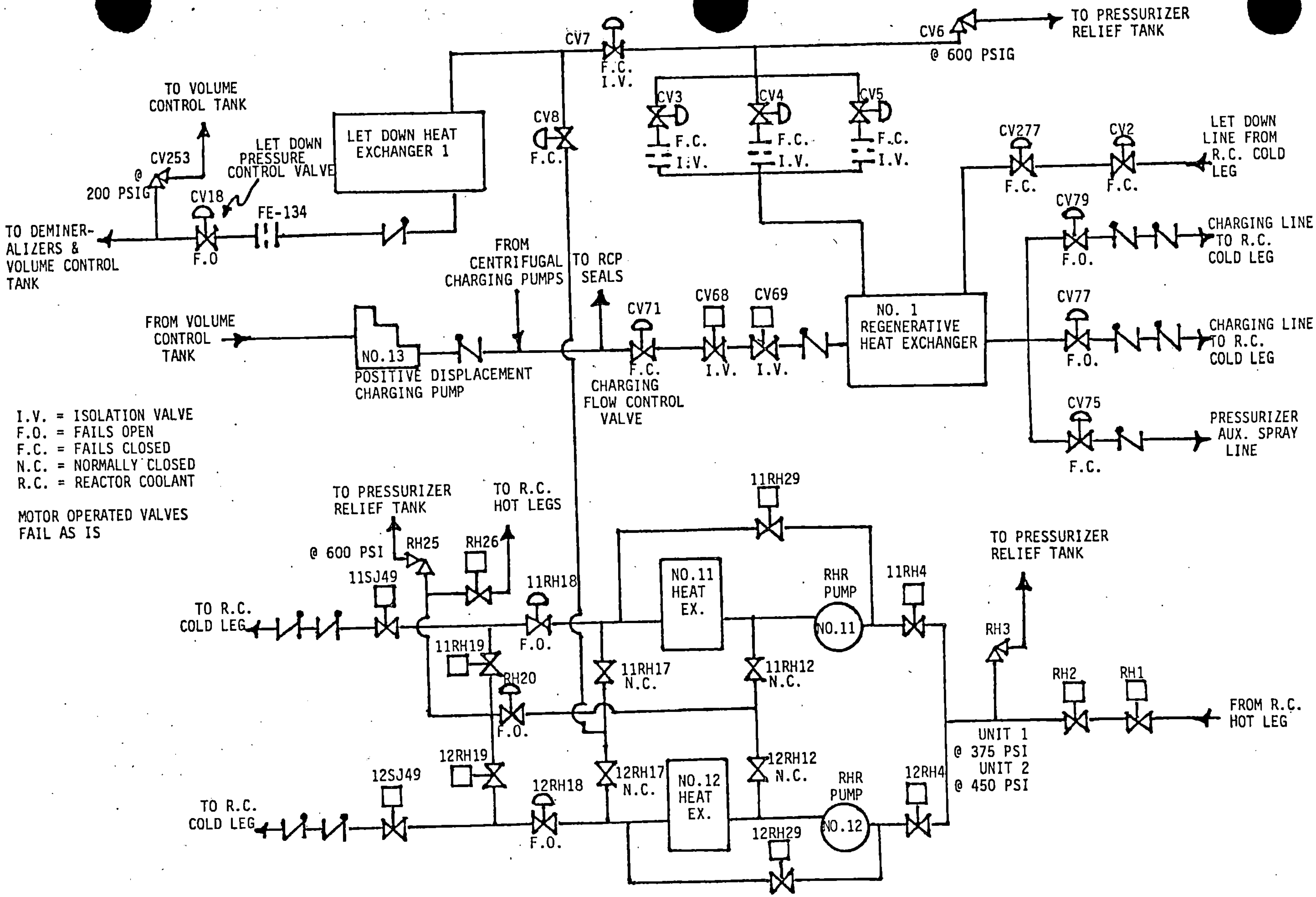


FIGURE 2.4

PIPING DIAGRAM FOR RHR & CVCS AT COLD SHUTDOWN tion isolation valves, RH1 and RH2, as a second initiator (Case 2). The systems available for mitigation of a cold overpressurization event are different for these initiators. Hence, it is easiest to analyze the two cases separately.

Specific Failure Modes for Case 1

For the air operated valves, CV8 and CV18, two failure modes were considered: an inadvertent closure by an operator and a mechanical failure to remain open. For the motor operated valve RH4, the previous two failure modes were considered in addition to the probability that the close pushbutton shorted. The probability of inadvertent closure of an MOV or AOV is developed in Section 3, and is 3×10^{-5}.

Based upon data from Reference 11, the probability that a MOV fails to remain open is 6.6×10^{-5} and an AOV is 1.1×10^{-4}. For the manual valve only the probability of an inadvertent closure is considered since Reference 11 indicates that there have been no reported incidents of manual valves failing-closed due to mechanical failures. From data in Reference 8, the probability of an inadvertent operator closure of RH17 is 5.8×10^{-5}. Using this data for Case 1 the probability of a letdown isolation initiating a cold overpressurization event is 9.0×10^{-4} per reactor year.

Case 1 Event Tree for Cold Overpressurization at Cold Shutdown

No credit is taken for operator action in this scenario. If the pressurizer is water solid when letdown isolation occurs, operator action is required in less than ten minutes. However, if the pressurizer level is at 70%, then there is at least 40 minutes for operator action. Salem Administrative Procedures require maintaining a pressurizer bubble unless the RCS is to be drained or maintenance work requires the system to be totally depressurized, and so the RCS is water solid for only a small fraction of time each year. Therefore, the assumption of no operator action is conservative.

After the initiation of this event, four events are considered in its mitigation. They are:

1. POPS activated.
2. One POPS relief valve functions.
3. RHR suction relief valve functions.
4. One PORV functions.

As depicted in Figure 2.5, there are a total of eight possible sequences; five of which do not result in a liquid challenge to the safety valves. However, since there are some common mode failures which must be considered, as well as differences in Units 1 and 2, the three sequences which result in liquid challenges will be discussed in detail.

If the POPS is armed, then only one relief valve must function to prevent a liquid challenge. The probability of one POPS relief valve not being available is developed in Section 3.2. If both POPS valves fail then the RHR suction relief in either Unit can also prevent the liquid challenge. The probability of the RHR suction relief valve not mitigating the event is developed in Section 3.6.

If a RHR suction relief valve failure follows the failure of both POPS valves, then Unit 1 will experience a subcooled liquid challenge to the safety valves. There is one exception to this, if the Unit 1 PORVs did not lift at the 375 psi setpoint because of a failure in the low pressure channel instrumentation, then the PORVs could still function at the high setpoint. For all other cases of PORV failure at the low pressure setpoint, the PORVs for Unit 1 would also be expected to fail at the higher setpoint. Since the probability of a pressure channel failure is small, it is conservatively assumed for Unit 1 that if the PORVs fail to lift at the low setpoint then they also will fail at the higher setpoint.

For Unit 2, the POPS relief valves are in parallel with the PORVs and if both the POPS valves and the RHR suction relief valve fail, then the PORVs can still relieve the pressure transient at their "at power" setpoint. However, for this sequence, common mode failures which impact both the POPS relief valves and the PORVs must be considered. There are three such common mode failures; 1) if the POPS fail to lift because of a large calibration error, the PORVs are assumed to have the same large calibration error and hence, also fail to lift. (See Section [illegible] for a discussion of the probability of a large calibration error.); 2) if the PORV block valve fails closed, this precludes the related POPS relief valve from

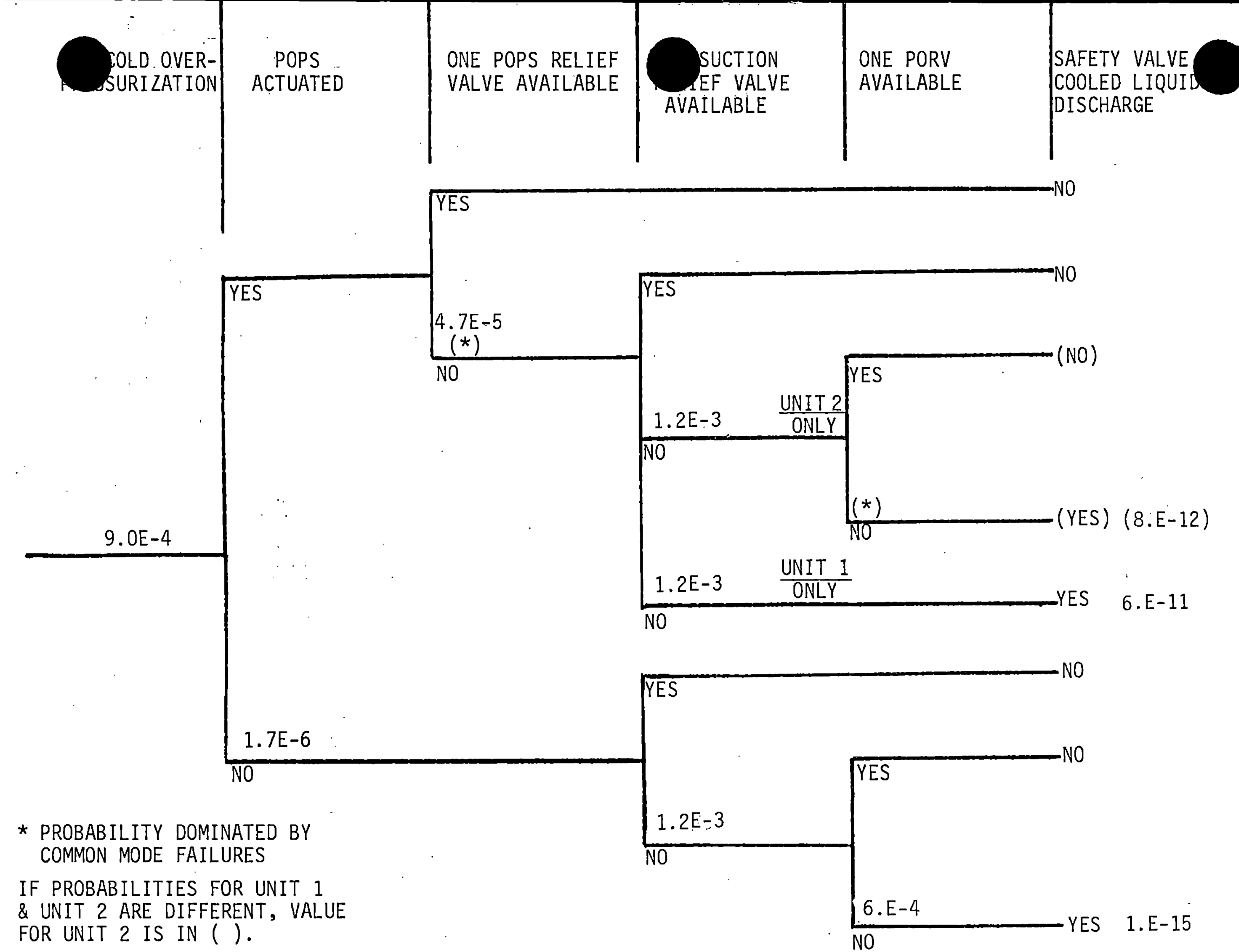


FIGURE 2.5

CASE 1 - COLD OVERPRESSURIZATION AT COLD SHUTDOWN EVENT TREE mitigating the event; and 3) if the circuit breaker in the logic circuit fails, the valves controlled by that channel would not be operable.

In evaluating the probabilities for Case 1 of liquid discharge for Units 1 & 2 following the arming of the POPS, the common mode failures have been taken into consideration. If the POPS is armed, for Case 1 the probability of liquid discharge is 6.0E-11 per reactor year for Unit 1 and 8.0E-12 per reactor year for Unit 2.

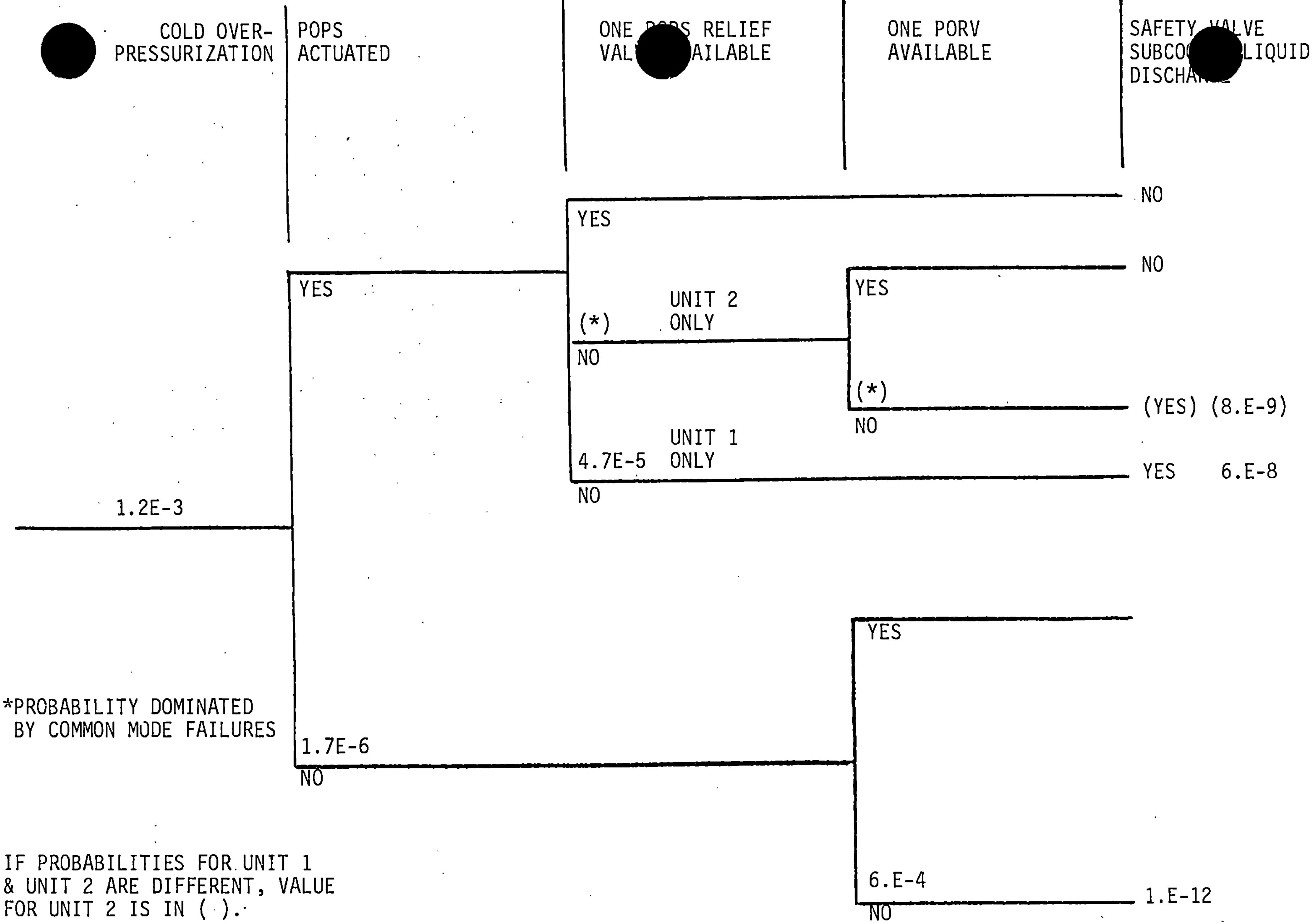
If the POPS is not armed then the POPS relief capability is not available. The probability of the POPS not being armed is developed in Section 3.5. For this sequence the RHR suction relief valve must still fail and the PORVs must fail at their "at power" settings before a liquid challenge to the safety valves can result. For both Units the probability of this sequence is so small that it does not contribute to the frequency of this event.

Specific Failure Modes for Case 2

The second possible initiator of a letdown - charging mismatch at cold shutdown is a failure of the RHR suction isolation valves to remain open. The failure modes considered for the RHR suction isolation valves are depicted in Figure 3.11. They are: logic circuit failure; close pushbutton failure; spurious RCS high pressure interlock signal; inadvertent operator closure; and valve fails plugged. The estimated failure probability for these isolation valves is 1.2E-3 per reactor year.

Case 2 Event Tree for Cold Overpressurization at Cold Shutdown

For this case no credit is taken for operator action to terminate the overpressurization event. As discussed for Case 1, this is judged to be a conservative assumption. Since the RHR system is isolated by the initiation of this event, the RHR suction relief valve is not available. With this exception Case 2 is identical to Case 1. The event tree for Case 2 is shown in Figure 2.6. Since the sequences here are similar to those for Case 1 each will not be discussed again.



*PROBABILITY DOMINATED
BY COMMON MODE FAILURES

IF PROBABILITIES FOR UNIT 1
& UNIT 2 ARE DIFFERENT, VALUE
FOR UNIT 2 IS IN ( ).

FIGURE 2.6

CASE 2 - COLD OVERPRESSURIZATION AT COLD SHUTDOWN EVENT TREE

For Case 2 if the POPS is armed the probability of liquid challenge is 6.0E-8 per reactor year for Unit 1 and 8.0E-9 per reactor year for Unit 2. If the POPS is not armed the PORVs must fail at their "at power" settings before a liquid challenge to the safety valves can occur. For both units the probability of this sequence is 1.0E-12.

Cold Overpressurization Event Summary

For the cold overpressurization event two different scenarios have been evaluated and one of the scenarios has been divided into two specific cases to demonstrate the difference in systems available for event mitigation. For this event no credit is taken for operator action. This is conservative since the pressurizer typically is not water solid and hence the operators have sufficient time to diagnose the event and take corrective action. A cold overpressurization will present a liquid challenge to the safety valves with the following frequencies:

Condition	Unit 1 (events/reactor yr.)	Unit 2 (events/reactor yr.)
a) Prior to Arming POPS	2.0E-9	2.0E-9
b) At Cold Shutdown		
Case 1	6.0E-11	8.0E-12
Case 2	6.0E-8	8.0E-9
COLD OVERPRESSURIZATION TOTAL	6.2E-8	1.0E-8

The multiple systems available to prevent liquid challenges to the safety valves following initiation of a cold overpressurization event makes the likelihood of such challenges extremely small. In fact, external events may cause common mode failures which result in cold overpressurization liquid challenges with frequencies comparable to, or greater than those calculated here. Analysis of such events is beyond the scope of the present effort. However, since the frequencies are expected to be very small in comparison to the frequency of a small break LOCA further analysis is not warranted at this time.

FAULT TREE ANALYSIS

The analysis of the event trees described in the previous section shows that several systems or operator actions are capable of eliminating the possible liquid challenges to the safety valves in Salem Units 1 & 2. Fault tree analysis techniques were used to quantify the unavailability* of these systems for both units. The fault tree analyses are presented in detail for Unit 1, and for Unit 2 only the system differences and modifications are discussed.

3.1 Fault Tree Analysis of PORVs for Salem Unit 1

Two pressurizer power operated relief valves exist in Unit 1 of the Salem plant. Figure 3.1 shows a sketch of one of those PORVs with its actuation air supply. Each PORV is actuated on a pressurizer pressure protection signal through its actuation circuit shown in Figure 3.2. The positions of two control switches dictate which pressure signal is required for valve actuation; the PORV control de selector switch and the Pressurizer Overpressurization Protection System PS) control mode push button-key lock selector switch. The PORV selector switch is used when the reactor is at power to place the PORVs in either the "AUTO" (open setpoint at 2335 psig) or "MANUAL" mode of operation. The POPS selector switch is used at cold shutdown to arm the POPS which automatically controls PORV operation, and can be in either the "ON"(open setpoint at 375 psi), "OFF", or "TEST" position. As directed by operating procedures, the operator adjusts the positions of these switches according to the reactor mode of operation. Thus, the unavailability of the PORVs is dependent upon the mode of operation of the reactor. The following sections discuss the fault-tree analysis for the reactor "At Power" and in "Cold Shutdown" modes of operation.

3.1.1 Reactor At Power

When the reactor is at power, operational procedure dictates that the POPS be "OFF". The PORV control mode selector switch is required to be on "AUTO" but there exists a probability that the operator may fail to place the PORV control

*hroughout this report unavailability and estimated failure probability are defined to be equivalent.

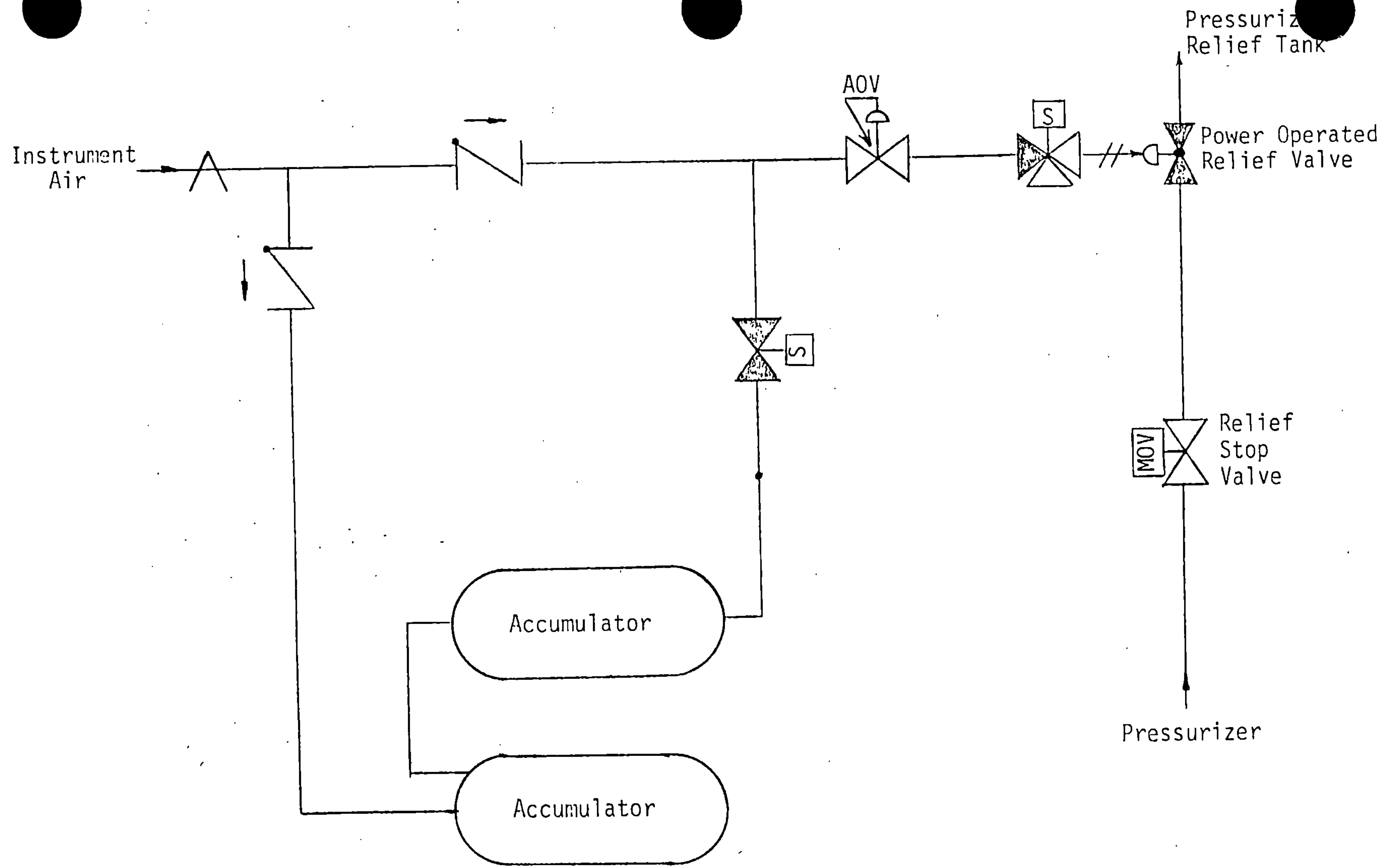


FIGURE 3.1

POWER OPERATED RELIEF VALVE SCHEMATIC WITH
ACTUATION AIR SUPPLY - SALEM UNIT 1

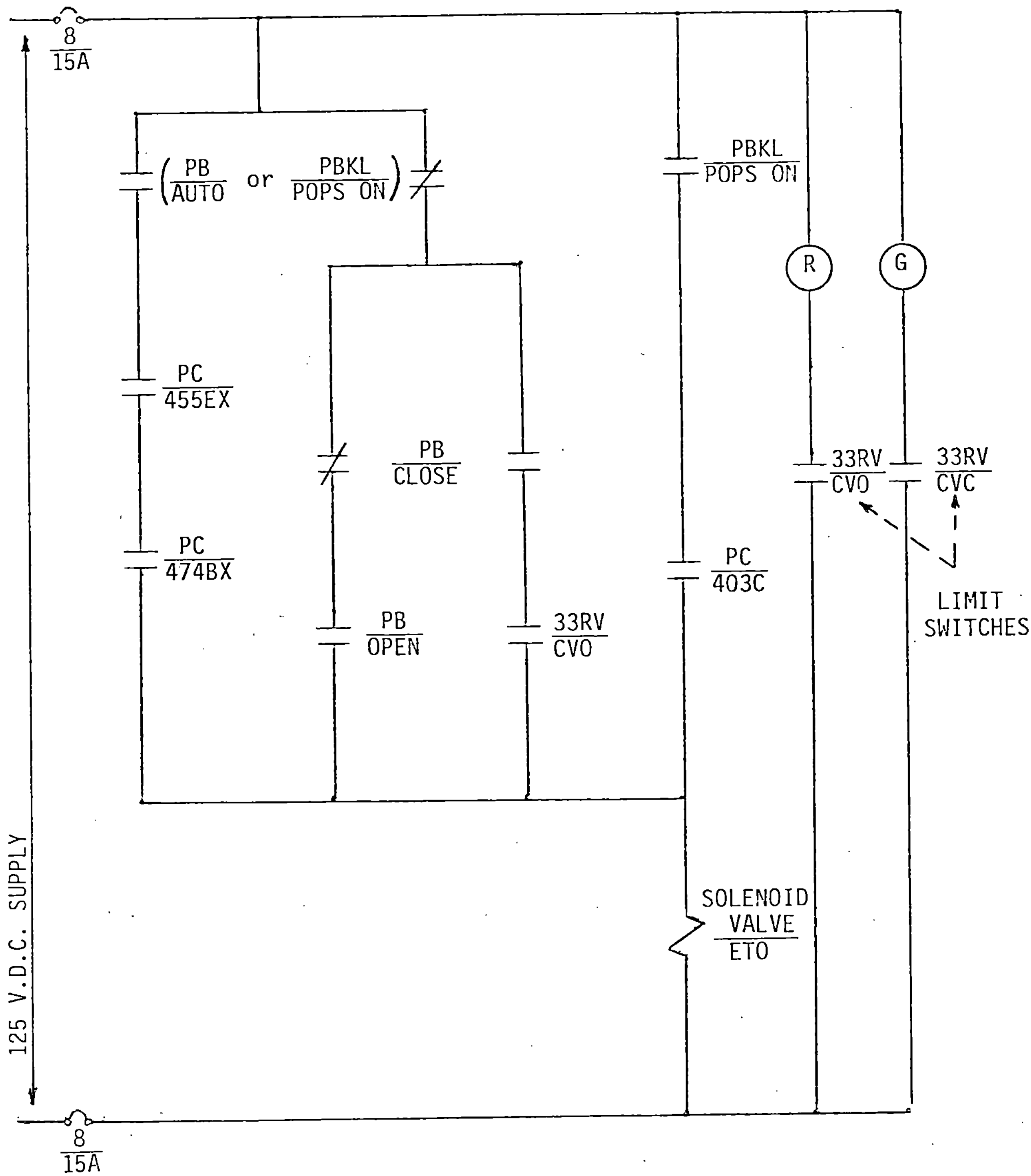


FIGURE 3.2

TYPICAL POWER OPERATED RELIEF VALVE
ACTUATION CIRCUIT - SALEM UNIT 1

mode selector switch in the "AUTO" position. Also, the pressurizer master controller must be in "AUTO". If the operators fail to perform both of this operations, then no credit is given for operator action and the PORVs are assumed to be unavailable.

The Salem procedure for going from cold shutdown to hot standby requires the operator to use the Valve Alignment Check-Off Sheet. This sheet instructs the operator to place the PORVs in the "AUTO" mode and then check-off the valve mode selection. To estimate the failure to accomplish this task, we follow Fig. 21-3 in NUREG-1278.[10] Figure 3.3 describes the probability tree for this failure. The total probability of failure to place the PORVs in the "AUTO" mode is estimated to be 6.5E-5/act. This probability is also used for the failure of the operators to place the pressurizer master controller in the "AUTO" mode.

A fault tree for failure of both PORVs to open when the reactor is at power was constructed and quantified. The fault tree is shown in Fig. 3.4. This figure gives details for only one of the PORVs as both PORV unavailability trees are identical. The failure data used for this analysis is listed in Table 3.1. Not listed in Table 3.1 is the failure rate for the plant control air supply. A generic study[16] of compressed air and backup in nuclear power plants has established a value of 8.E-4 failures per demand for the control air system. However, the Salem FSAR describes the total loss of plant control air to all systems and equipment as an event of such low probbility that it will not occur. This is justified because each unit has a separate control air supply system with an emergency control air system that is designated Class I (seismic). Furthermore, each units emergency air system can supply control air to both units. Although the detailed analysis of the control air systems required to confirm the non-credibility of this event is beyond the scope of this work, the system redundencies present in the Salem units indicate that a control air failure rate of 8.0E-6/demand is a more reasonable estimate. It is important to note, however, that this change in the probability of a control air system failure on PORV unavailability, is insignificant (<0.1%) for both units. An evaluation of this tree shows an overall estimate of the failure probability (for both PORVs) equal to 6.0E-4/demand.

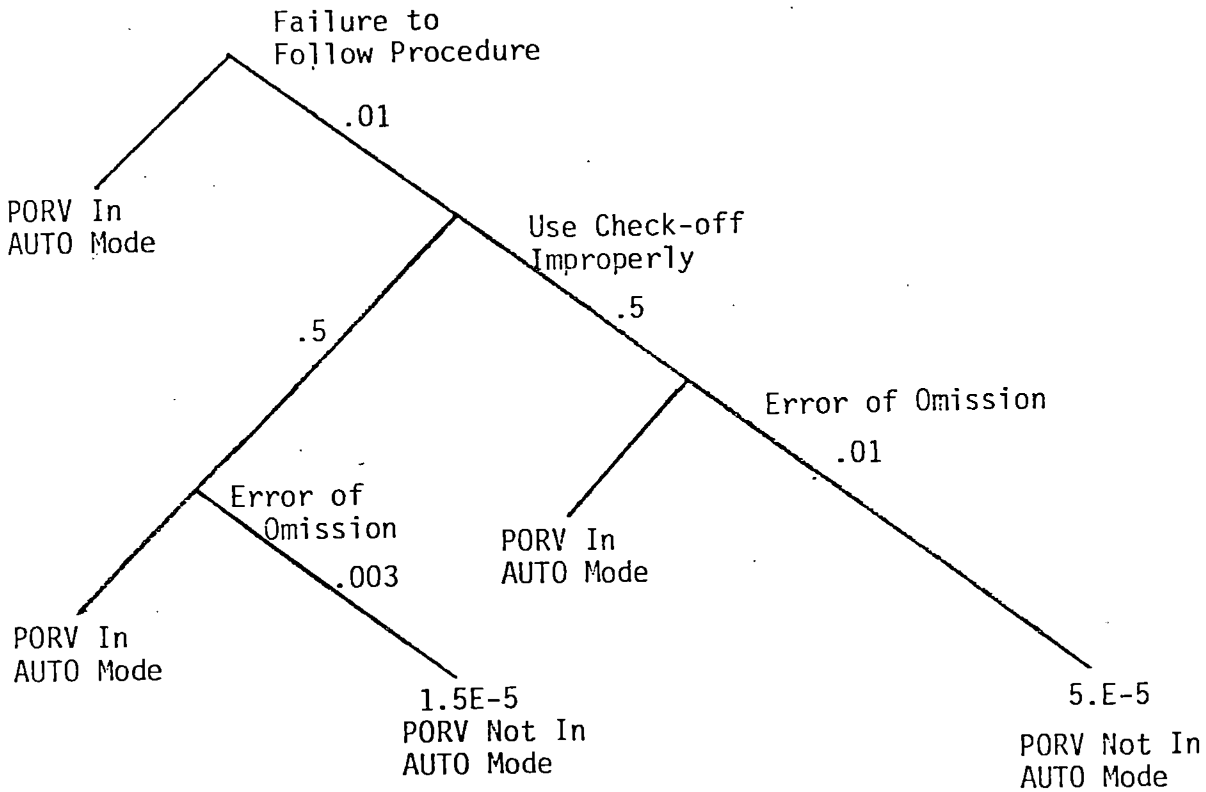


FIGURE 3.3

PROBABILITY TREE DIAGRAM FOR PORV CONTROL
SWITCH SELECTION TASK

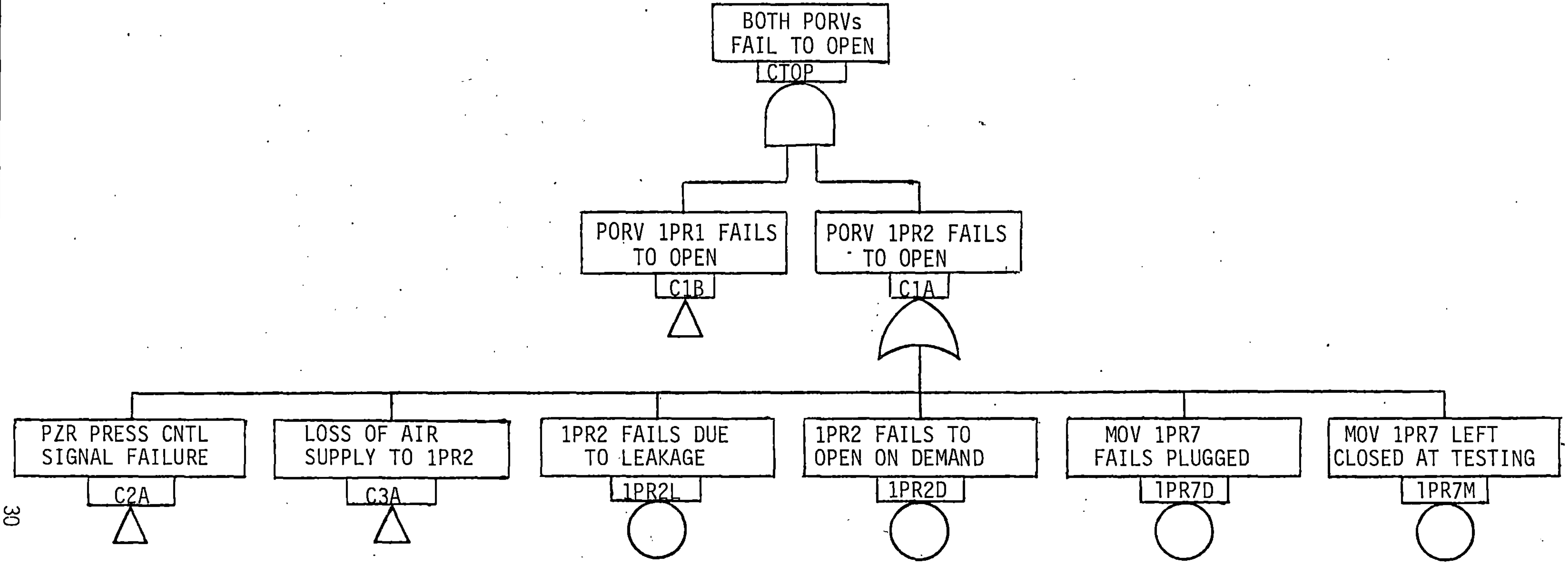


FIGURE 3.4

REACTOR AT POWER - FAULT TREE FOR UNAVAILABILITY OF BOTH PORVs

SALEM UNIT 1

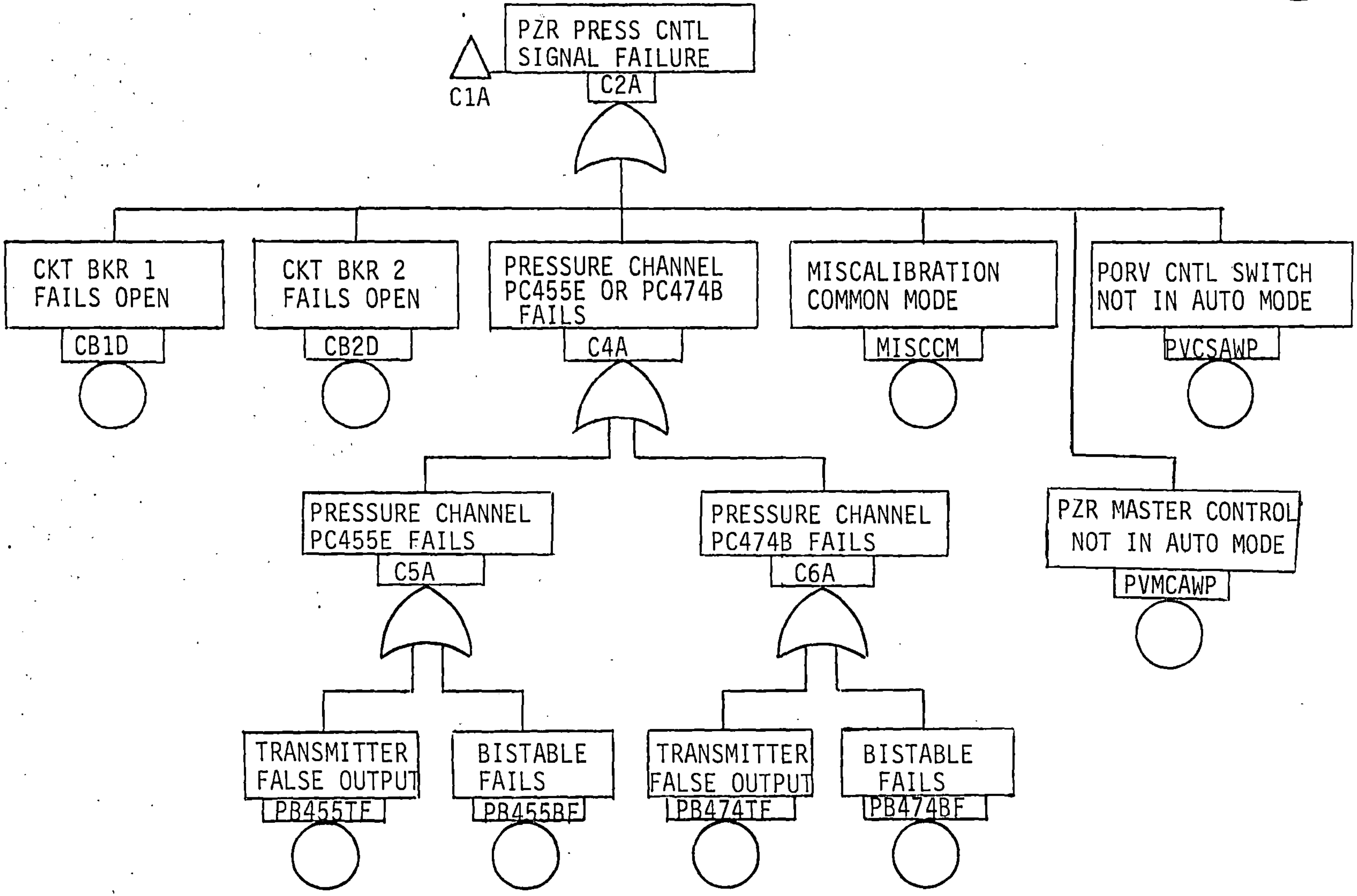


FIGURE 3.4 (continued)

REACTOR AT POWER - FAULT TREE FOR UNAVAILABILITY OF BOTH PORVs
SALEM UNIT 1

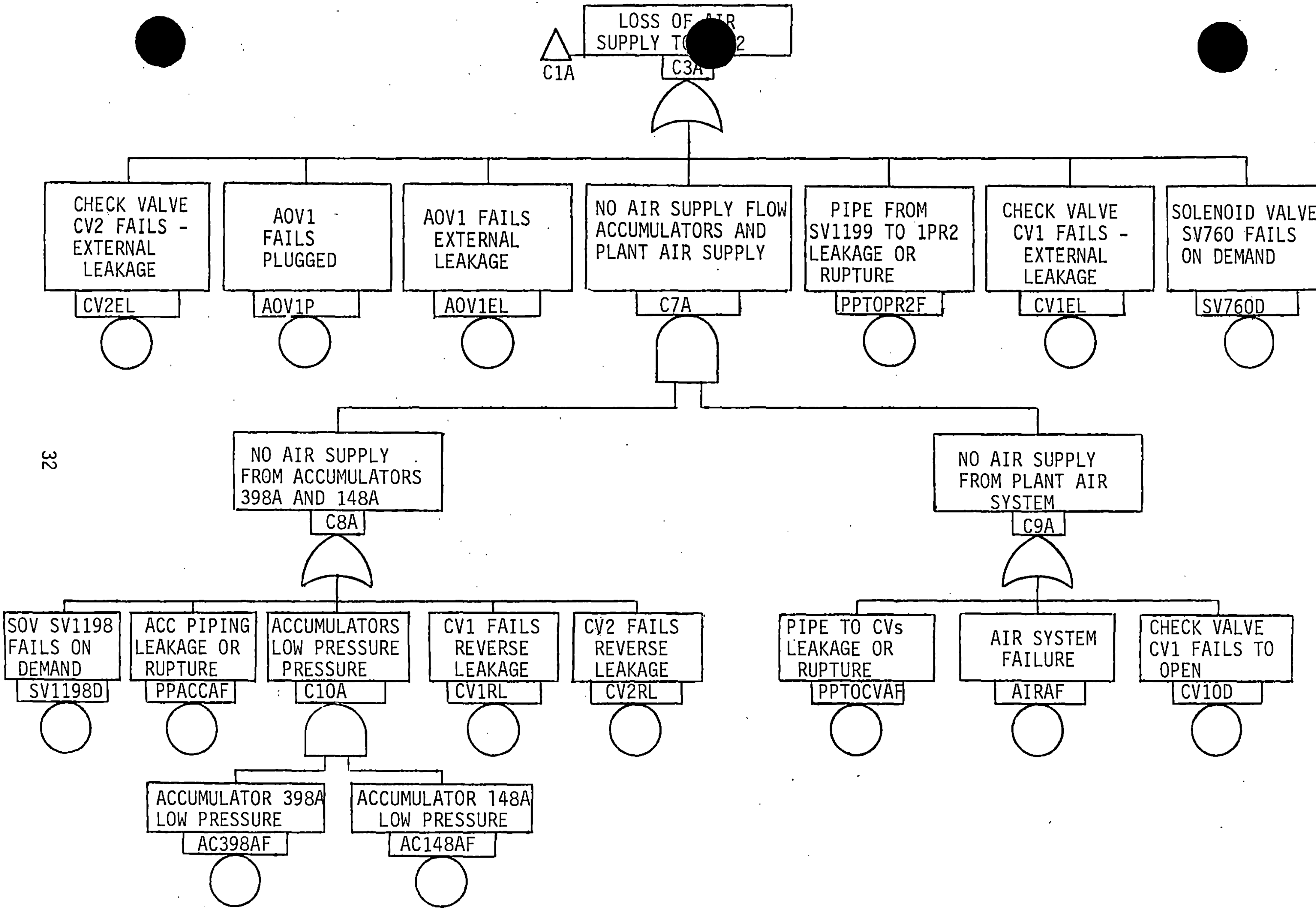


FIGURE 3.4 (continued)

REACTOR AT POWER - FAULT TREE FOR UNAVAILABILITY OF BOTH PORVs
SALEM UNIT 1

TABLE 3.1 FAILURE DATA FOR FAULT TREE ANALYSIS

COMPONENT	FAILURE MODE	FAILURE RATE (1/hr)	EXPOSURE TIME (hr)	UNAVAILABILITY	REF
Air Operated Valve	Failure to Open on Demand			2.0E-3/d	LER
Air Operated Valve	Leakage	2.0E-7	4380[a]	8.8E-4	LER
Air Operated Valve	Plugged	1.0E-7	4380[a]	4.4E-4	LER
Motor Operated Valve	Plugged	6.0E-8	4380[a]	2.6E-4	LER
Check Valve	External Leakage	5.0E-8	4380[a]	2.2E-4	LER
Check Valve	Reverse Leakage	7.0E-7	4380[a]	3.1E-3	LER
Check Valve	Fails to Open on Demand			1.0E-4/d	LER
Solenoid Operated Valve	Fails on Demand			1.3E-3/d	WASH-1400
Pipe (ϕ< 3in.)	Leakage or Rupture	9.0E-9/hr/section	4380[a]	4.0E-5/section	WASH-1400
Accumulator	Low Pressure in Accumulator			1.0E-6	Zion PSS
Bistable (Includes Bistable & Logic Relays)	Fails on Demand			6.7E-6/d	Zion PSS
Transmitter (Includes Sensor & Transmitter)	Fails to Provide Proper Output	1.66E-6	4[b]	6.6E-6	Zion PSS
Circuit Breaker	Premature Transfer	1.3E-6	365[c]	4.8E-4	WASH-1400

[a]Assumes test every year

[b]Assumes mean time to detection for these transmitters is every shift (Zion PSS)

[c]Assumes test every month

The main contributor to the unavailability of both PORVs is a common mode miscalibration of two or more comparators. This failure accounts for more than 90% of the total unavailability, and it is discussed in the next section.

3.1.2 Miscalibration

The probability of miscalibrating two or more comparators which actuate the signal to open the PORVs is determined using techniques described in NUREG/CR-1278. The evaluation is done in detail by considering both small and large miscalibrations. A large change is defined as one that is so extreme so as to be not normally expected, while a small change is one that can be expected to occur occasionally because of variations in equipment or other conditions.

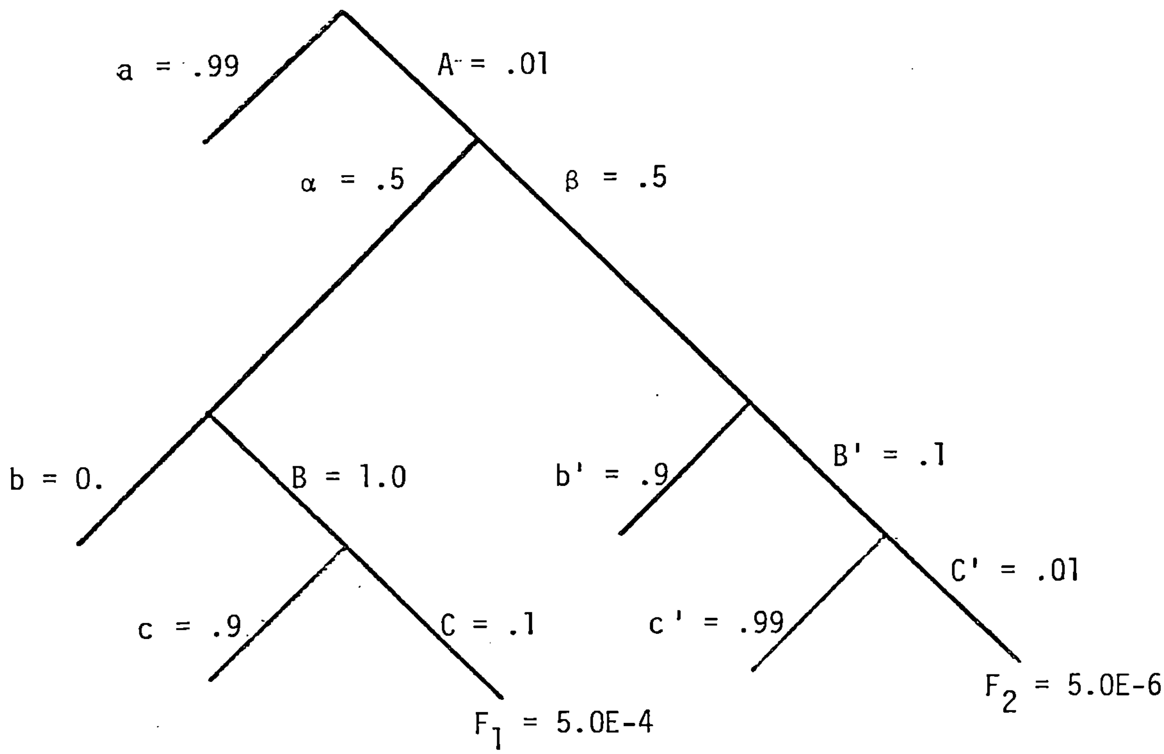
To check the calibration the technician must first set up the test equipment. An error in this initial setup is the initiating event for miscalibration. Figure 3.5 presents the Probability Tree Diagram for this calibration task. It is necessary to point out here that the checking of the calibration of all pressure channel comparators is done by the same technician once per refueling shutdown.

Figure 3.5 illustrates that the probability of a large miscalibration of two or more comparators (F_2) is equal to 5.0E-6/act, the probability of a small miscalibration of two or more comparators (F_1) is 5.0E-4/act, and the probability of a small or large miscalibration ($F_1 + F_2$) is equal to 5.05E-4/act.

The following comments are necessary for a better understanding of the Probability Tree Diagram in Fig. 3.5:

1. The complete notation for the conditional probabilities events is not employed but should be understood, e.g., α is written instead of $\alpha|A$.

2. As suggested by NUREG/CR-1278, it is estimated that a miscalibration would be equally likely to result in a large change or in a small change. This assumption is conservative since the total probability (i.e., the summation of the probabilities of a small and large miscalibration) is used in this analysis. A more realistic analysis would include only the large miscalibration, because the miscalibration error will cause a PORV failure (prior to an S/RV challenge at 2485 psig) only if the setpoint is calibrated to a value greater than 2485 psig. The differences between calibrations



A - FAILURE TO SET UP TEST EQUIPMENT CORRECTLY

α - Small Miscalibration of Test Equipment
B - For a Small Miscalibration,Failure to Detect Miscalibration for First Setpoint
C - For a Small Miscalibration,Failure to Detect Miscalibration for Second Setpoint
β - Large Miscalibration of Test Equipment
B'- For a Large Miscalibration,Failure to Detect Miscalibration for First Setpoint
C'- For a Large Miscalibration,Failure to Detect Miscalibration for Second Setpoint

Fig. 3.5

PROBABILITY TREE DIAGRAM FOR CALIBRATION TASK at 2485 and 2335 (the PORV setpoint) should certainly be considered a large error.

3. It is conservatively assumed that if the technician does not detect the instrument error by the time he calibrates the second setpoint, 100% of the time he will continue the erroneous calibration through the third and subsequent setpoints.

3.1.3 Reactor in Cold Shutdown Mode

There are several differences in PORV operations during at Power and Cold Shutdown modes of operations. Those differences which affect the PORV failure probabilities are discussed below:

i) Pressurizer Pressure Control Signal: In the cold shutdown mode, the POPS control switch is administratively keylocked "ON". This allows the PORVs to be opened via two actuation paths (refer to Fig. 3.2); due to a POPS signal at 375 psi or a high pressurizer pressure signal at 2335 psig. These pressure signals are generated by two independent channels. Since the probability of a pressure channel signal failure is a rather insignificant contributor to both PORVs being unavailable, it is conservatively assumed that if the PORVs fail to open at the POPS setpoint then they will be unavailable at higher pressures, i.e., both pressure channels fail. Consequently, the actuation circuit is treated has having only one pressure comparator, that of the POPS.

ii) PORV Failure Due to Leakage: Technical Specification 3.4.9.3[17] for cold shutdown requires that the PORVs be available for actuation or the RCS vented. Therefore, the closing and removing power from the pressurizer relief stop valves due to PORV leakage is not considered to be a credible event.

iii) Stop Valve Left Closed at Testing: When the POPS is armed the pressurizer relief stop valves are automatically opened. Thus, stop valve failure due to their being left closed at testing is also considered to not be a credible event.

iv) Miscalibration: With the reactor in Cold Shutdown the PORVs are set to open at 375 psi. Therefore, only a very large miscalibration will cause the actuation of the safety valves, whose setpoint is at 2485 psig, before the actuation of the PORVs. Based on this, and using the probability tree diagram in Fig. 3.5, the miscalibration error was taken to be 5.0E-6/act, corresponding to a large miscalibration only.

se modifications to the fault tree given in Fig. 3.3 are presented in Fig. 3.6. An evaluation of this tree shows an overall estimate of the failure probability

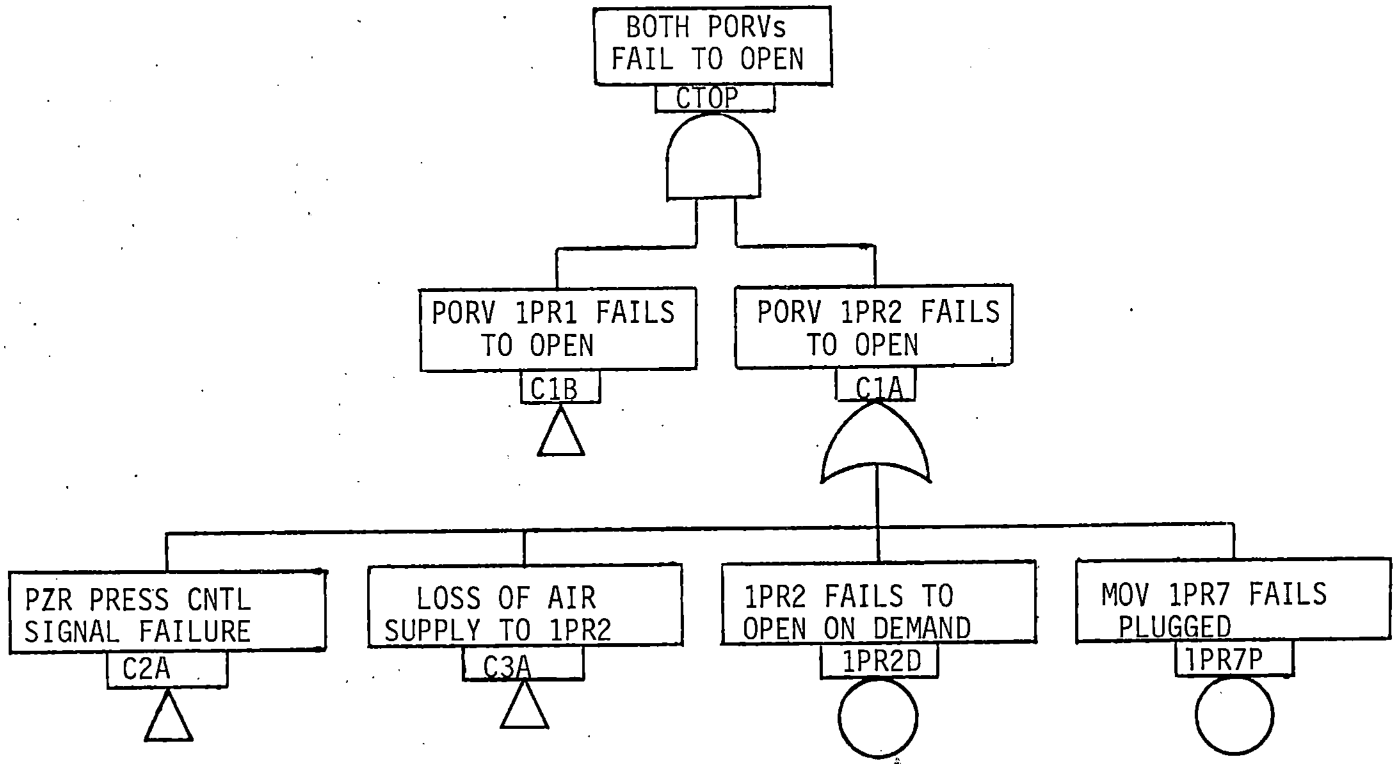


FIGURE 3.6

REACTOR AT COLD SHUTDOWN - FAULT TREE FOR
UNAVAILABILITY OF BOTH PORVs - SALEM UNIT 1

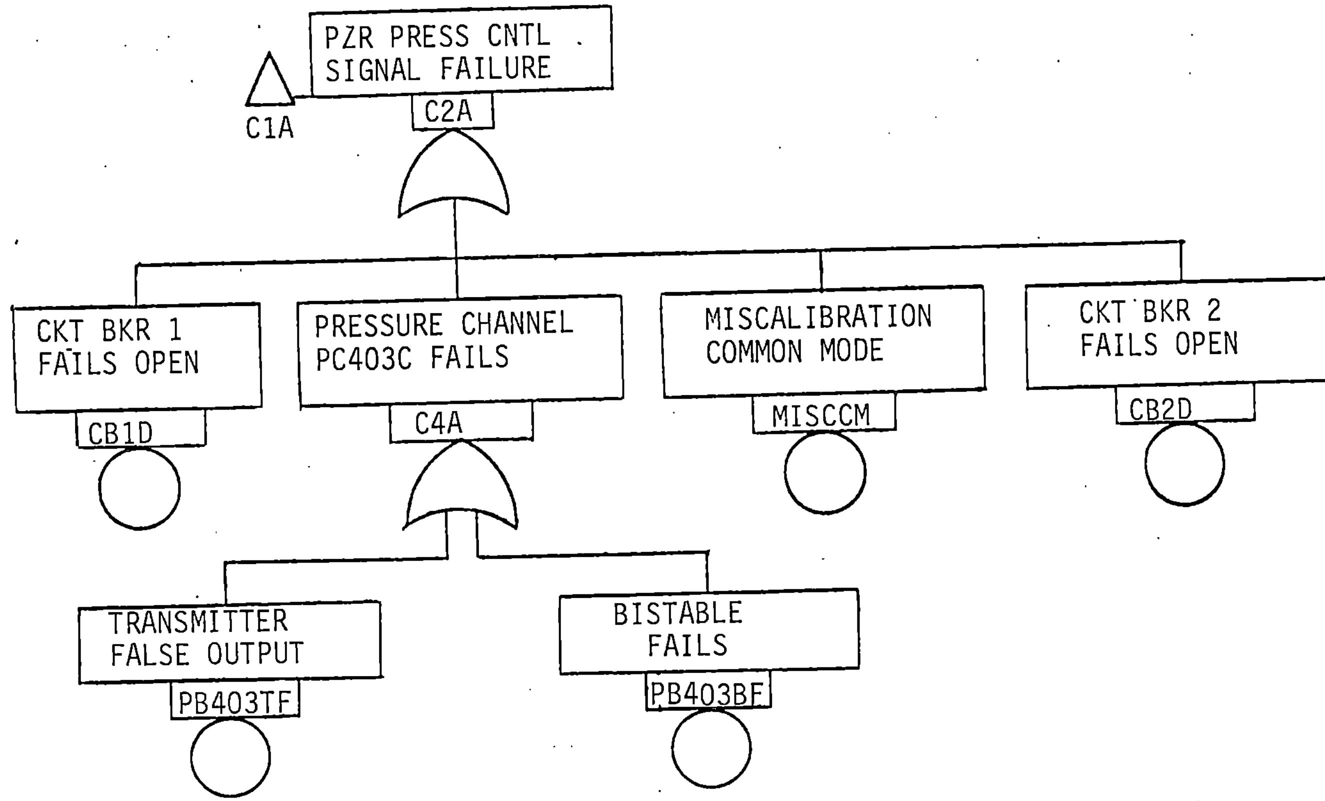


FIGURE 3.6 (continued)

REACTOR AT COLD SHUTDOWN - FAULT TREE FOR
UNAVAILABILITY OF BOTH PORVs - SALEM UNIT 1

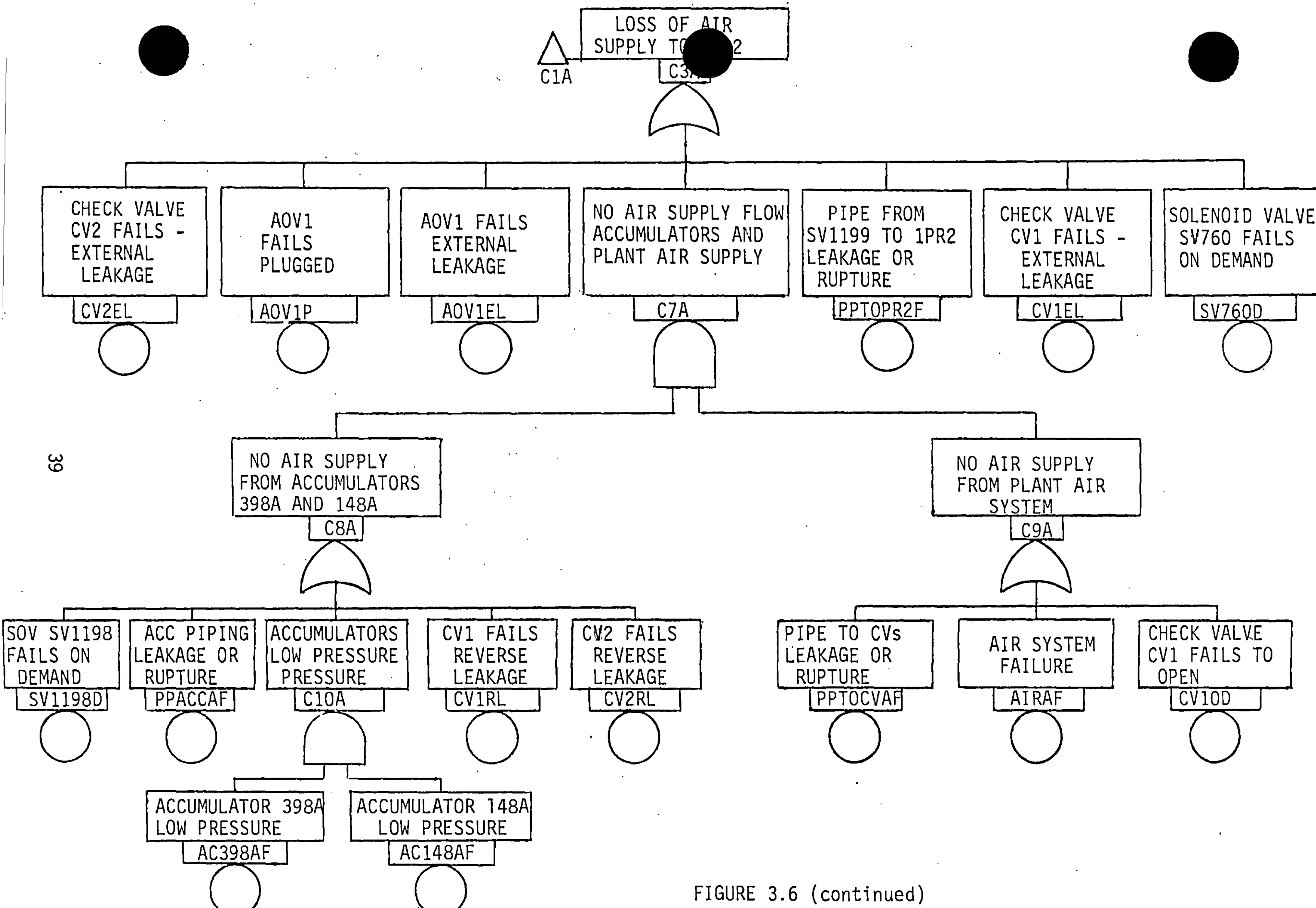


FIGURE 3.6 (continued)

REACTOR AT COLD SHUTDOWN - FAULT TREE FOR UNAVAILABILITY OF BOTH PORVs - SALEM UNIT 1 equal to 5.0E-5/demand for the cold shutdown mode. The main contributors are combinations of single failures in both valves.

3.2 Modifications to PORV Fault Trees for Salem Unit 2

The fault trees for failure of both PORVs to open when the reactor is at Power and on Cold Shutdown modes of operation for Salem Unit 2 are shown in Figures 3.7 and 3.8, respectively. The only differences between Unit 2 and Unit 1 are:

i) The Unit 2 air operated PORVs do not have auxiliary accumulators as a backup for the plant air supply system.

ii) At cold shutdown, the POPS actuates a separate set of electrically operated solenoid relief valves. Thus,should the POPS valves fail to open it is assumed that the PORVs are available for actuation at the higher setpoint pressure. The availability tree for the PORVs is nearly the same as if the reactor is at power, and it is discussed in Section 2.

The fault tree for PORV unavailability when the reactor is at power is identical to that for Unit 2 (Fig. 3.4) except for the "Loss of Air Supply to PORV" probability tree. Therefore, only this specific tree is presented in Fig. 3.7 for PORV unavailability for the reactor at power. The fault tree for POPS valve unavailability at cold shutdown is given in Fig. 3.8. An evaluation of these trees shows an overall estimate of failure probability equal to 6.0E-4/demand for the PORVs when the reactor is at power and 1.0E-5/demand for the POPS valves at cold shutdown.

3.3 Failure to Recover from Spurious Safety Injection

The failure to recover from a spurious safety injection appears in the event tree for Extended High Pressure Injection at Power (see Section 2.3 and Figure 2.2). As discussed in Section 2.3 this event is neither extremely rare nor difficult to control, and there are specific procedures[12] for recovery. Furthermore, since the operator has at least 20 minutes for recovery (as discussed in Section 2.3) this event is considered as only a moderately high stress level event.

According to NUREG/CR-1278, the basic human error probability for this event is 0.003 and a multiplier of 2 is recommended for a moderately high stress level.

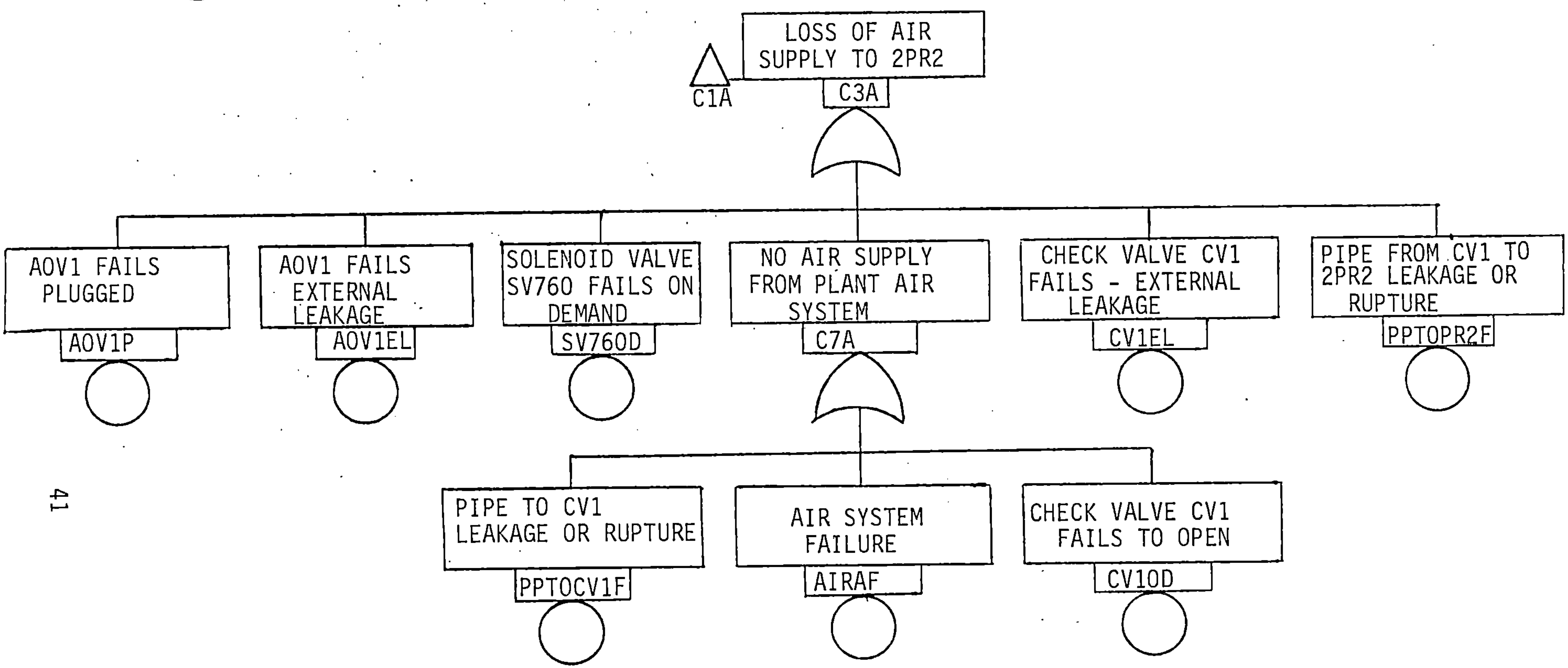


FIGURE 3.7

REACTOR AT POWER - FAULT TREE FOR UNAVAILABILITY OF BOTH PORVs - SALEM UNIT 2

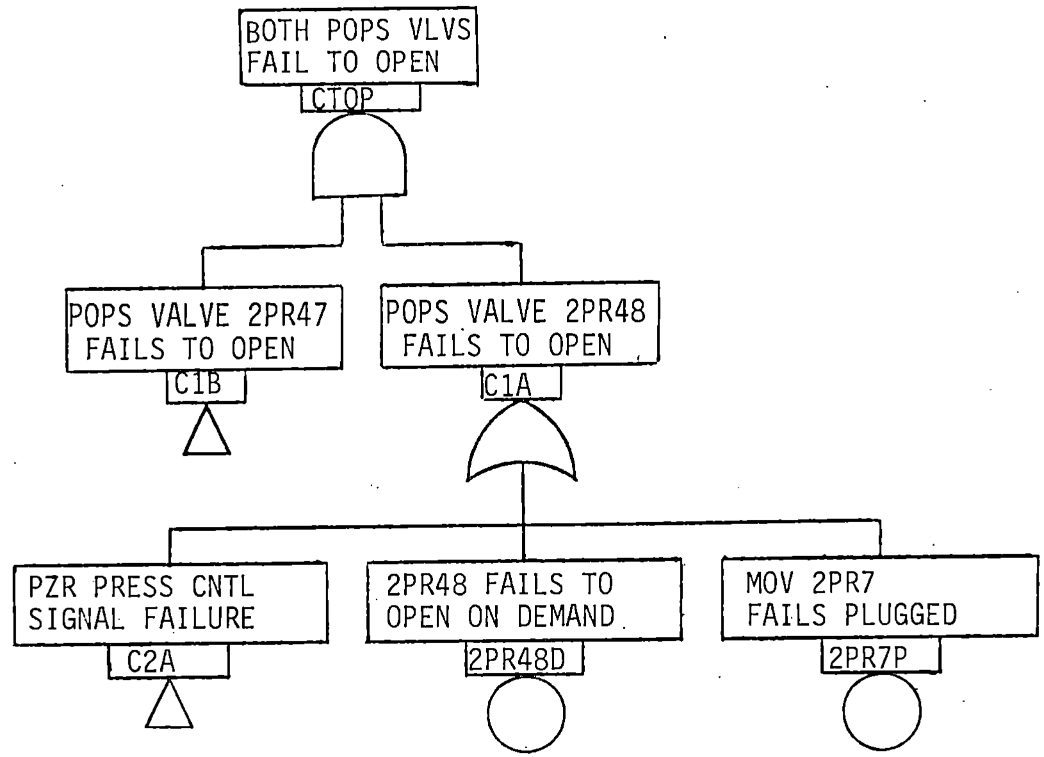


FIGURE 3.8

REACTOR AT COLD SHUTDOWN - FAULT TREE FOR UNAVAILABILITY OF BOTH POPS VALVES - SALEM UNIT 2

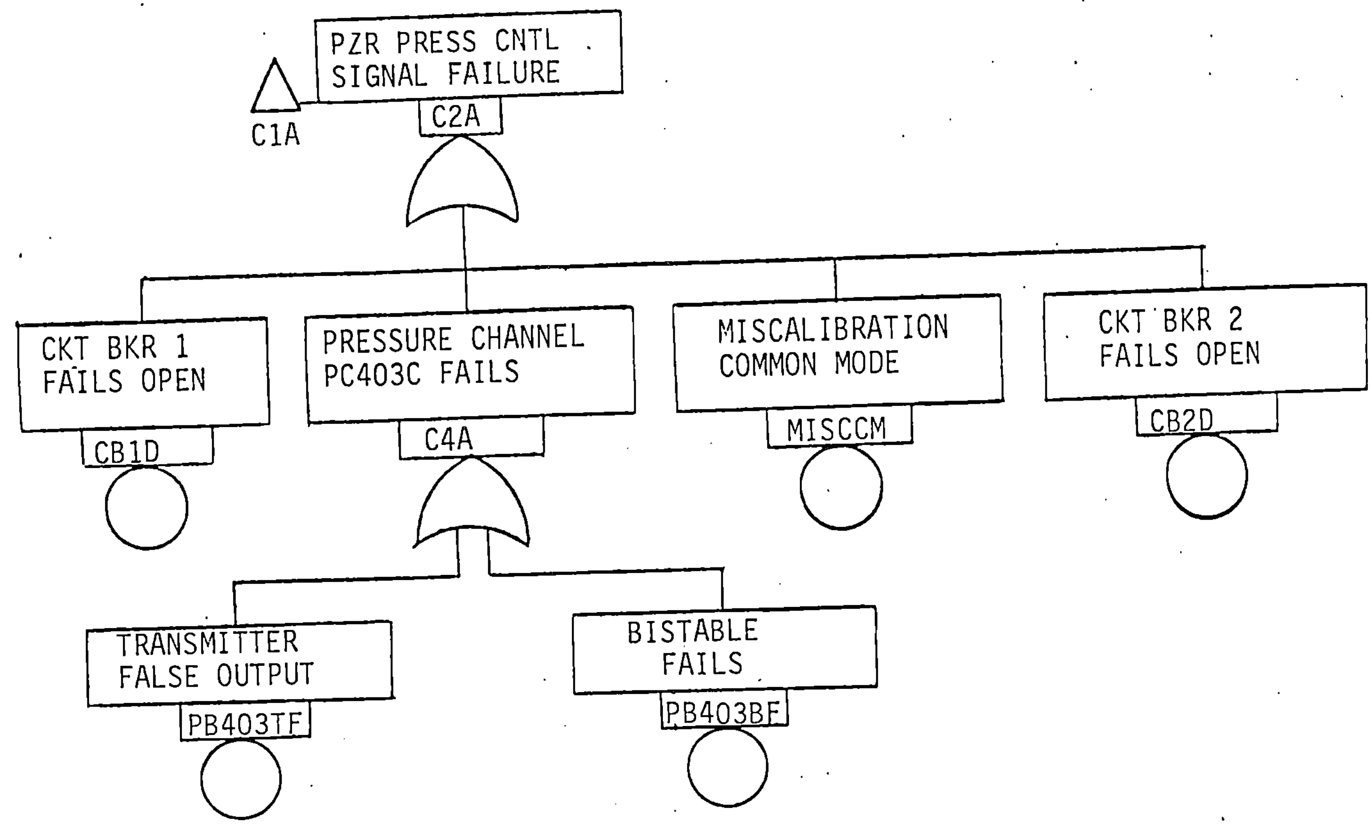


FIGURE 3.8 (continued)

REACTOR AT COLD SHUTDOWN - FAULT TREE FOR
UNAVAILABILITY OF BOTH POPS VALVES - SALEM UNIT 2

Three people would be in the control room.[18] Two are reactor operators (RO) and the third is the Shift Supervisor. To compute the human error probabilities, one uses the formulas recommended by NUREG/CR-1278 with the following dependencies among operators: high dependence between the two reactor operator and moderate dependence between the Shift Supervisor and the two operators. The error frequency of the three-person team for this task (Recovery from Spurious Safety Injection) would be:

$$6.0E\text{-}3 \times \frac{1 + 6.0E\text{-}3}{2} \times \frac{1 + 6 \times 6.0E\text{-}3}{7} = 4.5E\text{-}4$$

3.4 Inadvertent Operator Closure of an MOV or AOV

At cold shutdown for the scenario described in Section 2.4.3, the closure of motor operated valves (MOV) RH1, RH2, or RH4, and air operated valves (AOV) CV8 and CV18, may result in a liquid challenge to the pressurizer safety valves. The likelihood that an operator will inadvertently close one of these valves is estimated here.

Since the inadvertent closure of a MOV is not a common occurrence, a definitive scenario for such action is not known. Here two steps are deemed necessary for such an incident; 1) the operator fails to use the appropriate written procedure, and as a result, 2) changes the wrong MOV switch in a group of similar looking switches. This sequence is depicted in Figure 3.9. Using human factor probabilities from NUREG/CR-1278, the probability of this sequence is 3.0E-5. The probability of an inadvertent operator closure of an AOV is taken to be the same as that for an MOV.

This estimate of inadvertent operator action is believed to be conservative because the Salem operators are trained on valve changes and restorations. In addition to training on the correct use of written procedures and valve check-off lists, the operators are also trained to note valve deviations in a computer based system used to monitor valve deviations. This training, coupled with Salem Administrative Procedures, makes it unlikely that the operators will either fail to use the procedures or select an inappropriate switch.

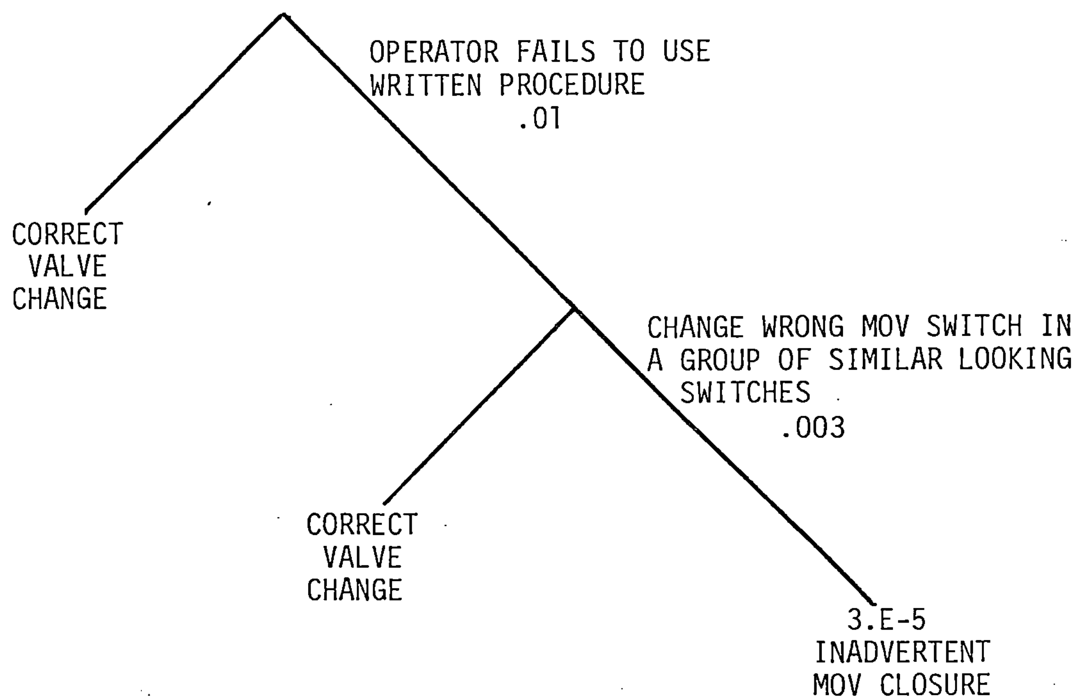


FIGURE 3.9

PROBABILITY TREE DIAGRAM FOR INADVERTENT OPERATOR CLOSURE OF AN MOV

The simple sequence used here also assumes no operator recovery. This requires that the operator ignores the position indication for the desired valve and any alarms that may be activated by the unappropriate valve closure (e.g., for this scenario any valve closure in the RHR suction line would activate the alarms associated with the RHR pump suction). Again this is judged to be highly unlikely, and hence, further supports the judgment that the calculated probability is conservative.

3.5 Operator Failure to Arm POPS

The pressurizer overpressure protection system (POPS) is required by Salem Operating Procedure to be armed when the RCS temperature reaches 312°F. Since there are two independent POPS channels, this requires turning a key and pressing the "on" button for each channel. Failure to perform this operation could result in liquid challenges to the safety valves as described in Section 2.4.3.

Typically, in each unit control room there are two reactor operators. The Shift Supervisor will be either in the control room, or in his office which is immediately adjacent to the control room. The two Salem units share a Senior Shift Supervisor. For this analysis no credit is taken for the presence of either the Shift Supervisor or the Senior Shift Supervisor in the control room.

In progressing from hot standby to cold shutdown, normally only one operator would be directly concerned with arming POPS. Thus, if the operator skips this step in the procedure, the POPS would not be armed. However, following this omission, when the RCS temperature reaches 312°F two annunciators would sound. If both operators fail to respond to the annunciators with appropriate action the POPS would remain unarmed. To estimate the probability of a failure to respond to the annunciators, it was assumed that there is a moderate dependence between the operators and that they monitor the control boards simultaneously only one-half of the time. If the operators silence the annunciator, but do not take corrective action, they may still note the unannunciated, lighted panel on subsequent scans and take corrective action. Here credit is taken for only one subsequent scan. This sequence of events along with the probability for each event is shown in Figure 3.10. Based upon this sequence, the probability that the POPS will not be armed is 2×10^{-6}.

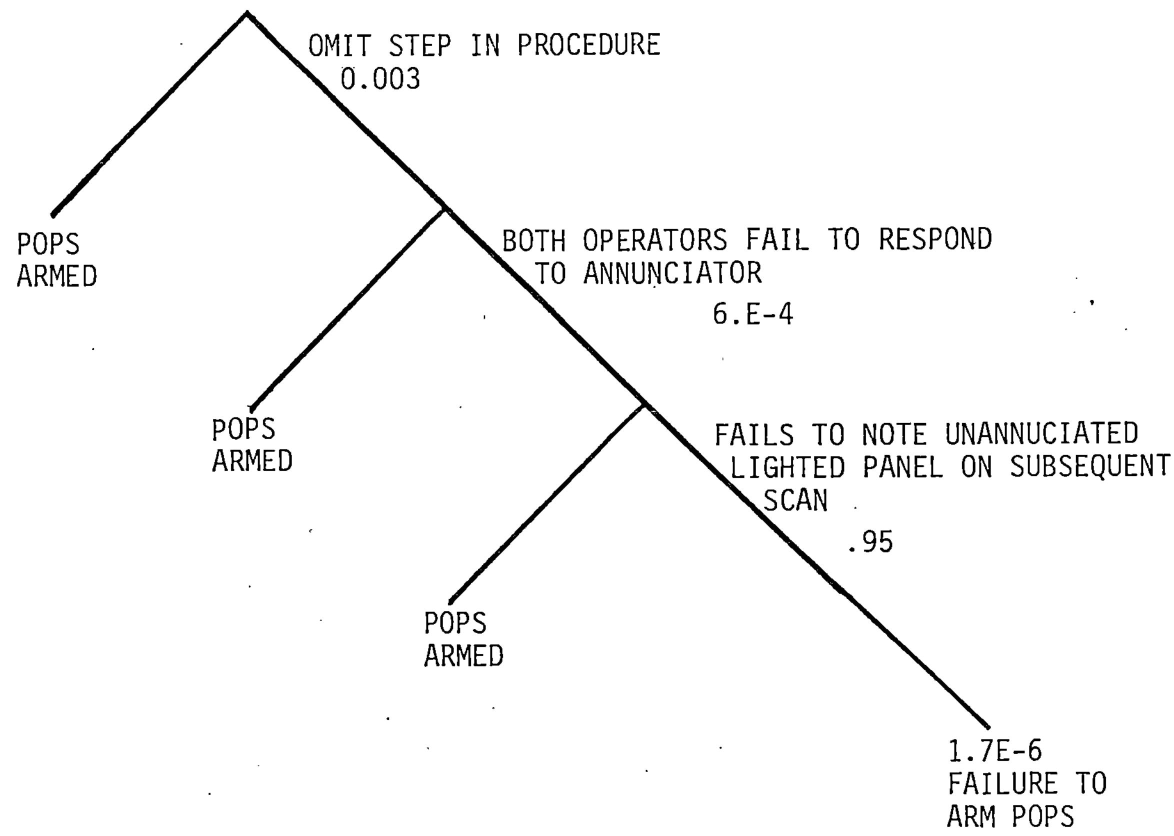


FIGURE 3.10

PROBABILITY TREE DIAGRAM FOR ARMING POPS

3.6 RHR Suction Relief Valve Unavailability

The residual heat removal (RHR) system suction relief valve, RH3, has sufficient capacity to relieve a charging-letdown mismatch. Thus, as indicated in Section 2.3.4, if this valve functions there will not be a liquid challenge to the safety valves. The fault tree shown in Figure 3.11 was used to determine the unavailability of the RHR suction relief valve.

If the suction relief valve fails on demand, or either motor operated RHR suction isolation valve fails closed, the mitigation capability of the relief valve is not available. Some of the failure modes for a RHR suction isolation valve are typical of a MOV (e.g., inadvertent operator closure, and a mechanical failure to remain open). However, since these valves are isolation valves for an engineered safety feature, there are additional failure modes that must be considered. The close pushbutton for the valve may fail shorted. Also, since these valves are designed to automatically close when the RCS pressure is 600 psi or greater, failures in the logic or pressure channel instrumentaion may cause an inadvertent closure. Based upon the failure modes described here, the probability that the RHR suction relief valve is not available for mitigation of a letdown-charging mismatch is 1.2E-3.

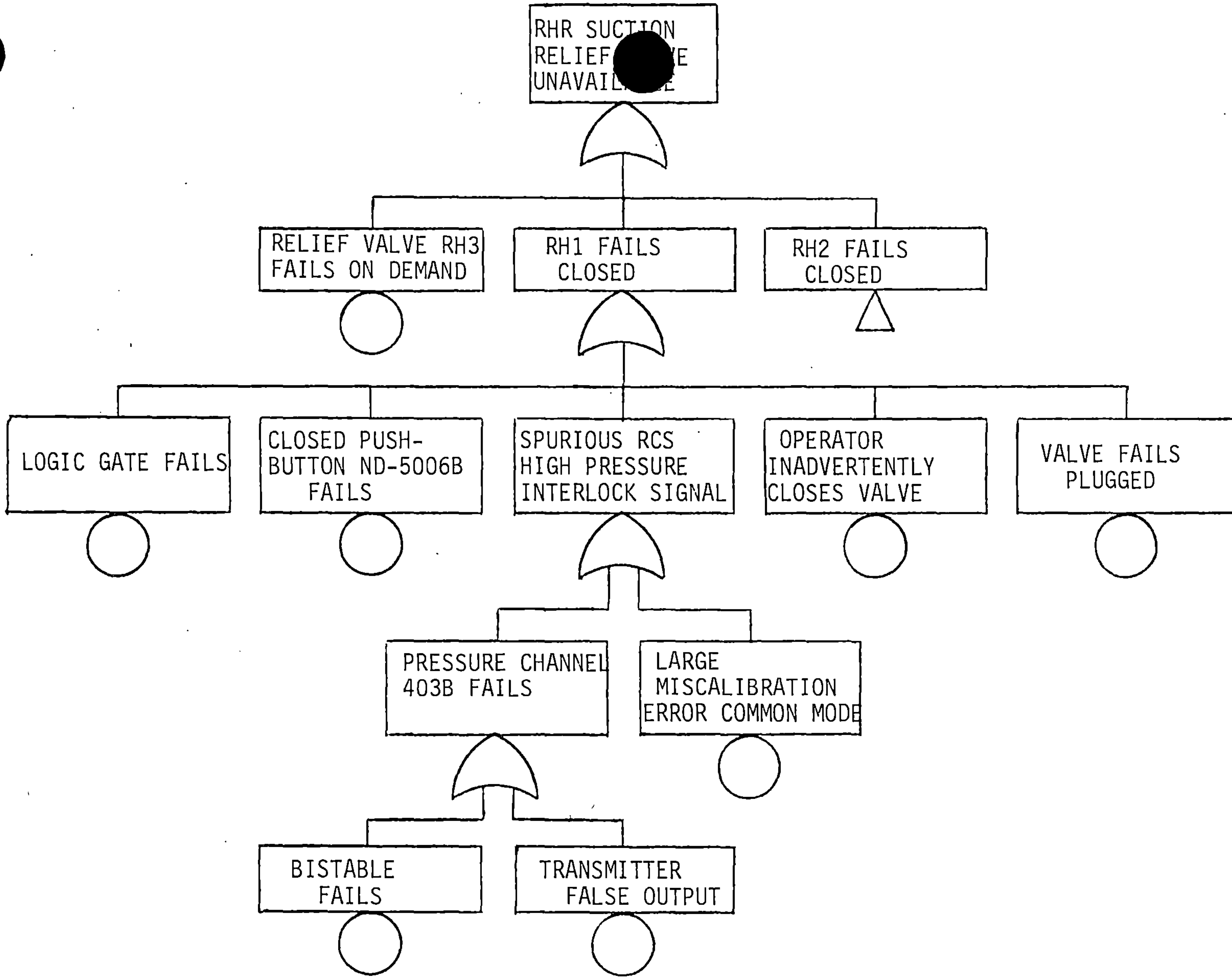


FIGURE 3.11

COLD OVERPRESSURIZATION - FAULT TREE FOR UNAVAILABILITY OF RHR SUCTION RELIEF VALVE

SUMMARY OF RESULTS

The mean estimate for the frequency of liquid discharge from the pressurizer safety valves is 1.0E-7 events/reactor year for Unit 1 and 5.0E-8 events/reactor year for Unit 2. Table 4.1 shows the contribution to this result from each of the three initiating events considered. This frequency is dominated by the occurrence of spurious safety injections at power for Unit 2 and is almost equally split between the spurious safety injection at power and cold overpressurization at cold shutdown for Unit 1. Unit 2 has an estimated lower frequency of liquid challenges because of the addition of the POPS solenoid valves in parallel to the PORVs. These valves reduce the estimated frequency of liquid challenges at cold shutdown.

The discharge of liquid from the Salem pressurizer safety valves has been shown to be a possible but extremely unlikely event. The estimated frequencies are based upon conservative data and assumptions and are sufficiently small that even order-of-magnitude errors would not affect the qualitative conclusions.

Zion Probabilistic Safety Study shows that for a generic PWR population the probability of a large or medium loss-of-coolant-accident (LOCA) is 1.01E-3 per reactor year and the probability of a small loss-of-coolant-accident is 2.69E-2 per reactor year. Thus, the scenarios of safety valve liquid discharge have been predicted to occur significantly less frequently than a large or medium loss-of-coolant-accident and the consequences of such liquid discharge are certainly much less severe. Further, the consequences of such liquid discharge are bounded by the Salem Design Basis Accident. Thus, safety valve liquid discharge appears to be an insignificant concern compared with LOCA or FSAR transients events and, hence, is certainly not a significant factor in either plant safety or risk to the public.

TABLE 4.1

SUMMARY OF RESULTS FOR FREQUENCY OF LIQUID
DISCHARGE FROM SALEM UNITS 1 & 2 SAFETY VALVES

Initiating Event	Calculated Frequency of Occurrence (Events/Reactor Year)		Type of Discharge
	Unit 1	Unit 2	
Spurious Safety Injection	4.0E-8	4.0E-8	Steam followed by saturated or slightly subcooled liquid; possible valve cycling
Main Feedwater Line Break	2.0E-9	2.0E-9	Steam followed by saturated liquid
d Overpressurization			
a) Prior to Arming POPS	2.0E-9	2.0E-9	Saturated steam followed by saturated or subcooled liquid
b) At Cold Shutdown	6.0E-8	8.0E-9	Far subcooled liquid
TOTAL	1.0E-7	5.0E-8	

REFERENCES

1. NUREG-0737, "Clarification of TMI Action Plan Requirements," Item II.d.1, November 1980.

2. W. R. Hocking, et al., "EPRI/CE PWR Safety Valve Test Program," EPRI Research Project V102-2, Final Report, July 1982.

3. D. F. Streinz, "EPRI/CE PWR Safety and Relief Valve Test Program, Upstream Pressure Oscillations," Combustion Engineering Letter PE-81-415, December 18, 1981.

4. B. R. Strong, et al., "Steam Hammer Design Loads for Safety/Relief Valve Discharge Piping," from Safety Relief Valves, ASME 1979.

5. B. S. Singer, and R. S. May, "Analysis of Safety/Relief Valve Chatter and Transient Problems," SAI Report to Commonwealth Edison, June 1982.

6. D. Harris, et al., "Probabilistic Evaluation of High Pressure Liquid Challenge of Safety/Relief Valve Piping," SAI Report SAI-245-81-PA submitted to BWR Owner's Group and General Electric Company, April 1981.

7. A. Meliksetian and A. M. Sulencar, "Valve Inlet Fluid Conditions for Pressurized Safety and Relief Valves in Westinghouse-Designed Plants," EPRI Research Project V102-19, January 29, 1982.

8. Zion Probabilistic Safety Study. Commonwealth Edison Company.

9. Reactor Safety Study: An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants, "NUREG-75/014, October 1975.

10. A. D. Swain and H. E. Guttman, "Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications," NUREG/CR-1278, October 1980.

11. W. H. Hubble and C. F. Miller, "Data Summaries of Licensee Event Reports of Valves at U.S. Commercial Nuclear Power Plants," NUREG/CR-1363, June 1980.

12. Salem Emergency Instructions:
    - I - 4.0 Safety Injection Initiation
    - I - 4.2 Recovery From Safety Injection

13. Salem Station, Units 1 & 2, Final Safety Analysis Report, Public Service Electric & Gas Company, July 1982.

14. Reactor Coolant System Description SD-R200, Salem Nuclear Generating Station Nos. 1 and 2 Units, Public Service Electric & Gas Company.

15. W. W. Clark, et al. "EPRI/Wyle Power Operated Relief Valve Phase III Test Report; Volume III," EPRI Research Project V102-11, Phase III Interim Report, March 1982.

16. W. Q. Hagen, "Compressed Air and Backup in Nuclear Power Plants," Report by ORNL on a contract for NRC, to be published.

REFERENCES (continued)

17. Salem Technical Specification 3.4.9.3.

18. Private Communication with Mr. J. Baily (PSE&G).