PLANT RISK IMPACT EVALUATION OF CERTAIN ELECTRICAL EQUIPMENT

Prepared By:
Nucon Inc.

Bengt O.Y. Lydell
Thomas A. Morgan
Eugene A. Hughes

Prepared For:
Southern California Edison Company

July 1984

1. INTRODUCTION

1.1 Background and Purpose

This report presents the results of an analysis of the plant risk impact of certain electrical equipment that will not be environmentally qualified in accordance with the 10CFR50.49 deadline of March 31, 1985 for San Onofre Nuclear Generating Station Unit 1. The analysis follows the general approach presented in Reference 1-1. Lack of a plant-specific reliability analysis or probabilistic risk assessment (PRA) study required that generic component failure data be used when quantifying the plant risk impact of each component. The scope of this analysis is limited to point estimate quantification (i.e., mean values).

1.2 Establishment of a Risk Impact Index

A component's contribution to plant risk is normally determined by quantifying a so-called "importance measure". However, determination of such a measure requires detailed information on failure and repair characteristics, coupled with logical structures such as plant-specific event trees and fault trees. The alternative is the performance of bounding type analyses that focus on plant engineering knowledge rather than on a comprehensive theoretical model of plant risk.

The proper framework for performing a plant risk impact evaluation when a comprehensive plant specific PRA is not available is found in results of the published studies. Review of these studies helps in defining a plant risk profile consensus which makes it possible to determine

whether a certain component failure, or an unavailable safety function, contributes to plant risk. Table 1 summarizes core melt frequencies and major radioactive release frequencies developed in some of the publicly available PRA documents. A summary of some initiating event frequencies is found in Table 2.

An additional reference for evaluating plant risk impact is found in the Nuclear Regulatory Commission trial safety goal, where the quantitative design objective for plant damage frequency is defined as follows:

> "the likelihood of a nuclear reactor accident that results in a large scale core melt should normally be less than 1 in 10,000 per year of reactor operation."

Based on generic component failure data and simple functional fault trees, each component evaluated in this study is examined to establish its potential impact on plant risk. Table 3 gives the criteria used in summarizing the results of the analysis.

A HIGH risk impact index corresponds to a case in which the failure of the component under consideration is the main contributor to a dominant fault tree top event or a dominant event sequence. For a MEDIUM risk impact, the failure of the component in question must contribute to but not dominate an important top event or event sequence. A LOW risk impact index is used to characterize a component that does not have an impact on plant risk.

The threshold values used to determine the respective risk impact indices are taken from the publicly available PRA

studies for PWR plants. The risk impact of a component is evaluated relative to its contribution to the overall core melt frequency. Results from the published PRA studies show this frequency to be in the range from 4.0×10^{-6} to 4.0×10^{-4} per reactor year (mean values). Components that have an impact on a core melt frequency are typically found among the active components in safety systems required for shutting down the reactor, cooling the core, and cooling the containment building; i. e., components identifiable in emergency procedures and are required to actuate either manually or automatically.

There are, however, components that do not directly affect the core melt frequency but still affect the overall plant risk. An example of such a component is an isolation valve that is part of the containment isolation system. Complete failure of the containment penetration isolation results in an open release path for radioactive products with potential onsite and offsite consequences. To evaluate such cases it is necessary to determine the kind of release caused by an open penetration and whether the release has an effect on any of the event trees used to generate the accident sequences. In WASH-1400 (Reference 1-2) containment leakage was defined as that leakage which provides a flow path to the atmosphere equivalent to a 4" or greater diameter hole. Values used to establish a risk impact index for a containment isolation valve are based on the quantification of release categories and the containment failure modes found in available PRA studies.

1.3 Equipment

A total of 15 components are considered in this analysis (see Table 4). The components are part of the safety injection system, containment spray system, containment isolation system and the component cooling water system. Many of the components are normally not included in the systems analyses of a PRA project. The simplification procedures that are employed by a PRA study team include the setting of boundary conditions and simplification of hardware configurations, and this often implies that components such as flow transmitters and temperature sensors are deleted from the modeling efforts.

1.4 Assumptions

The analyses described in Section 2 assume that the effects from passive failures are negligible unless otherwise stated. Failure of such components as welds, gaskets (for failure mechanisms other than due to adverse environmental conditions), pipe caps and flanges has typically a lower frequency than active components.

Furthermore, it is assumed that the failure data used in this report embraces the operating conditions at San Onofre Unit 1. Applicable failure data are presented in Table 5 and include the most recently available generic failure rates applicable to PWRs. In the case of data for temperature sensors, a Swedish source (Reference 1-3) has been used. This source includes a comprehensive analysis of operating experience for instrumentation in BWRs which is equally applicable to U.S. PWR plants.

1.5 References

1-1. Atefi, B., and D. Gallagher, "Risk Based Categorization of San Onofre SEP Issues," SAI-83-131-WA, Science Applications, Inc. October, 1983.

1-2. U.S. Nuclear Regulatory Commission, "Reactor Safety Study: An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants," WASH-1400 (NUREG-75/014), October, 1975.

1-3. Nuclear Safety Board of the Swedish Utilities (RKS), "Reliability Data for Components in Swedish Boiling Water Reactors", RKS 82-07, November, 1982.

2.0 EQUIPMENT EVALUATIONS

2.1 Flow Transmitters (FT-912, FT-913, FT-914)

2.1.1 Equipment Description

There is one flow transmitter in each of the three safety injection lines; the transmitters are designated as FT-912, 913 and 914. Each flow transmitter sends an input signal to a flow indicator in the control room and also to the Technical Support Center (TSC) computer via a current-voltage converter. The flow transmitter manufacturer is Foxboro and the model/type is designated as 630-2AS.

2.1.2 Safety Function

The transmitters provide surveillance of safety injection flow until it is terminated and recirculation is initiated. The purpose of the transmitters is to help the operators verify the existence of safety injection flow. If the transmitters fail, the operators can still determine if safety injection flow exists by monitoring the RWST level; there is a single pneumatic RWST level indication system and one level switch which only initiates an alarm once the RWST level has dropped to 21%. A loss of the flow transmitters will not impact the operation of the safety injection system.

2.1.3 Failure Mode Analysis

With loss of one or more flow transmitters, the operators will be able to verify safety injection into the RCS by observing the level reduction in the RWST. Complete loss of all flow indication, RWST level indication, and the RWST low level alarm can affect the timely initiation of switchover to recirculation.

2.1.4 Quantitative Assessment

A functional fault tree for the complete loss of all flow indication and RWST level indication is shown in Figure 2.1-1. Evaluation of the probability for common cause failure of the three flow transmitters is performed using the MGL-method (Reference 2.1-1) which is an extension of the beta-factor method. The effects of radiation on the transmitters during the first hours of an accident should have a negligible impact on their reliabilty. The probability of failure due to high radiation during the first few hours of an accident is assumed to be 0.10.

Loss of RWST level indication is characterized by a failure probability of 2.2×10^{-2} (Reference 2.1-2).

2.1.5 Risk Impact Conclusions

The main contributor to the loss of all flow and level indication is the RWST level indication. A complete failure of flow transmitters is dominated by a common cause event. Failure of the transmitters has negligible impact on the top event. The plant risk impact is concluded to be LOW.

2.1.6 References

2.1-1. Pickard, Lowe and Garrick, Inc., "Seabrook Station Probabilistic Safety Assessment", PLG-0300, December 1983 (available from National Technical Information Service).

2.1-2. Atefi, B., and D. Gallagher, "Risk Based Categorization of San Onofre SEP Issues", SAI-83-131-WA, Science Applications, Inc., October 1983.

2.2 Containment Spray Valves (CV-82, CV-114)

2.2.1 Equipment Description

Valves CV-82 and CV-114 are pneumatic operated butterfly valves (ASCO Type WPLB 8300859) isolating two containment spray lines inside containment. CV-82 is opened by a solenoid valve (SV-128) on a train B containment spray actuation signal. CV-114 is opened by solenoid valve SV-118 on a train A containment spray actuation signal.

2.2.2 Safety Function

CV-82 and CV-114 are normally closed isolation valves and are opened automatically on high containment pressure (10 psig) coincident with safety injection by deenergizing the solenoid valves to the vent position. Once actuated, the control valves need not be reactuated during the entire course of the accident due to their fail-safe design. Both solenoid valves need to be operable several seconds subsequent to a LOCA or main steam line break.

2.2.3 Failure Mode Analysis

There are two redundant containment spray headers; one header is controlled by the two valves CV-82 and CV-114, the other header by a valve that is operated from the control room. The second header is part of the fire protection system and not part of the main line safety systems. Complete failure of containment spray requires both headers to be inoperable and the ultimate consequence is failure of the containment structure. The spray headers with valves and pumps are assumed equal in this assessment. A functional fault tree for this event is shown inFigure 2.2-1.

2.2.4 Quantitative Assessment

The effect of environmentally induced failure is assessed by assigning a probability of 0.9 that a spray valve fails due to high humidity following post accident conditions. Similarly, the failure probability in the short-term following an accident due to high radiation is assumed to be 0.1 for each valve. Common cause failures of pumps and valves are assessed using the beta-factor model with a generic beta-factor of 1.25×10^{-1} (Reference 2.2-1). Data for the spray header nozzles are from the Zion Probabilistic Safety Study (Reference 2.2-2); the probability of a plugged spray header is 2.40×10^{-4}. The valve and pump data come from the Seabrook PRA (Reference 2.2-1) which represents a recent generic data bank for PWR equipment.

2.2.5 Risk Impact Conclusions

The quantitative evaluation shows the failure of containment spray system to inject to be equal to 4.72 X 10-3 without environmentally qualified valves. This failure probability does not change significantly even if the spray valves withstand the post accident conditions. On a subsystem level (the two redundant spray valves), the reliability improvement of environmentally qualified valves over non-qualified valves is estimated to be 7%. This improvement does not propagate to the top event probability, which is dominated by the failure of the RWST suction valve to open. The risk impact of spray valves CV-82 and CV-114 is therefore considered to be LOW.

2.2.6 References

2.2-1 Pickard, Lowe and Garrick, Inc. "Seabrook Station Probabilistic Safety Assessment," PLG-0300, December 1983 (available from the National Technical Information Service).

2.2-2 Pickard, Lowe and Garrick, Inc., Westinghouse Electric Corporation, and Fauske & Associates, Inc., "Zion Probabilistic Safety Study", prepared for Commonwealth Edison Company, September 1981.

2.3 Containment Sump Pump Discharge Isolation Valve (CV-102)

2.3.1 Equipment Description

Control valve CV-102 isolates the discharge of the sphere sump pumps inside the containment. A solenoid valve designated as SV-108 controls CV-102, a pneumatic diaphragm actuated 3-way control valve. In series with CV-102, is a similar control valve located outside containment designated as CV-103 with solenoid valve SV-109. The containment penetration is a 1 1/2 inch diameter pipe.

2.3.2 Safety Function

Under normal operating conditions CV-102 and CV-103 are open to allow primary coolant that has leaked into the containment sump to be discharged into the radioactive waste disposal system. On high containment pressure (above 1.4 psig), high radiation, safety injection or remote manual operation, the solenoid valves for CV-102 and CV-103 are deenergized to the vent position, thereby securing instrument air from the pressure regulator (air set) to the valve actuator. This results in the spring return of CV-102 and CV-103 to the closed position which secures any discharge of primary coolant from the containment sump pumps to the radioactive waste disposal systems as a containment isolation function following a LOCA or main steam line break (MSLB).

Once the valves have actuated, they do not require reactuation during the entire course of the accident. These valves do, however, need to retain their structural

integrity for the course of the accident to ensure that they remain in the closed position, securing any discharge of primary coolant from the containment sphere, thereby isolating containment. Loss of power or instrument air does not jeopardize the closed position of CV-102 and CV-103, since actuator spring return force keeps the valves in the closed position.

2.3.3 Failure Effects

Failure of this containment isolation function requires that both isolation valves fail to close. Valve CV-103 is located outside containment and in case this valve fails to close, plant personnel can be dispatched to close it manually. In addition, plant personnel could deenergize the containment sump pumps in order to reduce the outflow of radioactive fluids if CV-102 and CV-103 were unable to be isolated. The failure logic is presented in Figure 2.3-1

2.3.4 Quantitative Assessment

The effect of environmentally-induced failure is assessed by assigning a probability of 0.9 that control valve CV-102 fails due to high humidity following post accident conditions. Similarly, the failure probability due to high radiation given a severe accident is assumed to be 0.1. It is furthermore assumed that no common cause effects due to the post accident conditions affect the two isolation valves. Termination of the sump discharge pump operation is conservatively assessed by assuming manual intervention only characterized by a human error rate of 3×10^{-3} (Reference 2.3-1). Valve failure data comes from Table 5.

2.3.5 Risk Impact Conclusions

Failure of the isolation function is dominated by a common cause failure of valves CV-102 and CV-103, and the failure to terminate the pump operation. Installation of an environmentally qualified (more reliable during severe post-accident conditions) valve does not affect the top event probability. The frequency of major release due to an open path via the sump discharge line is significantly lower than those estimated from published PRA studies as shown in Table 1. The risk impact of isolation valve CV-102 is therefore concluded to be LOW.

2.3.6 Reference

2.3-1. Swain, A.D., and H.E. Guttman, "Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications", NUREG/CR-1278, August 1983.

2.4 RCS Drain Tank Discharge Isolation Valve (CV-104)

2.4.1 Equipment Description

Control valve CV-104 isolates the discharge of the RCS drain tank pumps inside the containment. A solenoid valve designated as SV-110 controls CV-104, a pneumatic diaphragm actuated 3-way control valve. In series with CV-104 is a similar control valve located outside containment designated as CV-105 with solenoid valve SV-111. The containment penetration is a 2 inch diameter pipe.

2.4.2 Safety Function

Under normal operating conditions CV-104 and CV-105 are open to allow primary coolant in the RCS drain tank to be discharged into the radioactive waste disposal system. On high containment pressure (above 1.4 psig), high radiation, safety injection or remote manual operation, the solenoid valves for CV-104 and CV-105 are deenergized to the vent position, thereby securing instrument air from the pressure regulator (air set) to the valve actuator. This results in the spring return of CV-104 and CV-105 to the closed position which secures any discharge of primary coolant from the drain tank pumps to the radioactive waste disposal systems as a containment isolation function following a LOCA or MSLB.

Once the valves have actuated, they do not require reactuation during the entire course of the accident. These valves do, however, need to retain their structural integrity for the course of the accident to ensure that they remain in the closed position securing any discharge

of primary coolant from the containment sphere, thereby isolating containment. Loss of power or instrument air does not jeopardize the closed position of CV-104 and CV-105, since actuator spring return force keeps the valves in the closed position.

2.4.3 Failure Effects

Failure of this containment isolation function requires that both isolation valves fail to close. Valve CV-105 is located outside containment and in case this valve fails to close, plant personnel can be dispatched to close it manually. In addition, plant personnel could deenergize the RCS drain tank pumps in order to reduce the outflow of radioactive fluids if CV-104 and CV-105 cannot be isolated. The failure logic is presented in Figure 2.4-1

2.4.4 Quantitative Assessment

The effect of environmentally-induced failure is assessed by assigning a probability of 0.9 that control valve CV-104 fails due to high humidity following post accident conditions. Similarly, the failure probability due to high radiation during the first hours of an accident is assumed to be 0.1. It is furthermore assumed that no common cause effects due the post accident conditions affect the two isolation valves. Termination of the drain tank pump operation is conservatively assessed by assuming manual intervention only characterized by a human error rate of 3 X 10^{-3} (Reference 2.4-1). Valve failure data comes from Table 5.

2.4.5 Risk Impact Conclusions

Failure of the isolation function is dominated by a common cause failure of valves CV-104 and CV-105, and the failure to terminate the pump operation. Installation of an environmentally qualified (more reliable during severe post-accident conditions) valve does not affect the top event probability. The frequency of major release due to an open path via the drain tank discharge line is significantly smaller than those estimated from published PRA studies as shown in Table 1. The risk impact of isolation valve CV-104 is therefore concluded to be LOW.

2.4.6 Reference

2.4-1. Swain, A.D., and H.E. Guttman, "Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications", NUREG/CR-1278, August 1983.

2.5 RCS Drain Tank Vent Isolation Valve (CV-106)

2.5.1 Equipment Description

Control valve CV-106 isolates the RCS drain tank vent inside the containment. A solenoid valve designated as SV-112 controls CV-106, a pneumatic diaphragm actuated 3-way control valve. In series with CV-106, but outside containment, there is a similar control valve designated as CV-107 with solenoid valve SV-113. The containment penetration is a 2 inch diameter pipe.

2.5.2 Safety Function

Under normal operating conditions CV-106 and CV-107 are open to allow flashing primary coolant in the RCS drain tank to be discharged into the gaseous radioactive waste disposal system. On high containment pressure (above 1.4 psig), high radiation,safety injection or remote manual operation, the solenoid valves for CV-106 and CV-107 are deenergized to the vent position, thereby securing instrument air from the pressure regulator (air set) to the valve actuator. This results in the spring return of CV-106 and CV-107 to the closed position which secures any discharge of primary coolant from the drain tank vent to the radioactive waste disposal systems as a containment isolation function following a LOCA or MSLB.

Once the valves have actuated, they do not require reactuation during the entire course of the accident. These valves do, however, need to retain their structural integrity for the course of the accident to ensure that

they remain in the closed position securing any discharge of primary coolant from the containment sphere, thereby isolating containment. Loss of power or instrument air does not jeopardize the closed position of CV-106 and CV-107, since actuator spring return force keeps the valves in the closed position.

2.5.3 Failure Effects

Failure of this containment isolation function requires that both isolation valves fail to close. Valve CV-107 is located outside containment and in case this valve fails to close, plant personnel can be dispatched to close it manually. The failure logic is presented in Figure 2.5-1

2.5.4 Quantitative Assessment

The effect of environmentally-induced failure is assessed by assigning a probability of 0.9 that control valve CV-106 fails due to high humidity following post accident conditions. Similarly, the failure probability due to high radiation during the first hours of an accident is assumed to be 0.1. It is furthermore assumed that no common cause effects due to post accident conditions affect the two isolation valves. Valve failure data comes from Table 5.

2.5.5 Risk Impact Conclusions

Failure of the isolation function is dominated by a common cause failure of valves CV-106 and CV-107. Installation of an environmentally qualified (more reliable during severe post-accident conditions) valve does not affect the top event probability. The frequency of major release due to an open path vis the RCSdrain tank vent line is significantly smaller than those estimated from published PRA studies as shown in Table 1. The risk impact of isolation valve CV-106 is therefore concluded to be LOW.

2.6 Service Water Supply Isolation Valve (CV-115)

2.6.1 Equipment Description

Valve CV-115 isolates the service water supply to the containment. A solenoid valve designated as SV-126 controls CV-115, a pneumatic diaphragm actuated 3-way control valve. The isolation valve is located outside the containment. A manually operated valve, normally open, is also located upstream of CV-115. In addition, a third valve similar to CV-115 is located inside the containment in series with CV-115. The containment penetration is a 3/4 inch diameter pipe.

2.6.2 Safety Function

Under normal operating conditions CV-115 and its series valves are open to allow a service water supply to the containment. On high containment pressure (above 1.4 psig), high radiation, safety injection or remote control, the solenoid valves for CV-115 and its redundant valve inside containment are deenergized to the vent position, thereby securing instrument air from the pressure regulator (air set) to the valve actuator. This results in the spring return of the control valves to the closed position as a containment isolation function following a LOCA or secondary line break.

Once the control valves have actuated, they do not require reactuation during the entire course of the accident. These valves do, however, need to retain their structural integrity for the course of the accident. Loss of power or instrument air does not jeopardize the closed position of CV-115 and its redundant control valve, since actuator

spring return force keeps the valves in the closed position.

2.6.3 Failure Effects

Loss of the containment isolation function requires that both control valves fail to close on demand. Given an isolation failure, there then remains the option to isolate the penetration via the manual valve. This assumes that this valve is accessible after a LOCA or secondary line break; i.e., the radiation levels are low enough to permit operator access.

2.6.4 Quantitative Assessment

A simple functional fault tree for the containment isolation function is shown in Figure 2.6-1 together with applicable failure data. The failure to open the manual valve, given it is accessible, is characterized by a human error rate of 3×10^{-3} (mean value, taken from NUREG/CR-1278, Reference 2.6-1). The common cause failure likelihood of the two control valves is assessed using a simple beta-factor model with a generic beta-factor of 1.25×10^{-1} (Reference 2.6-2). This information together with the appropriate failure data in Table 5 makes it possible to quantify a point estimate for the probability of loss of the containment isolation in the service water supply line.

The effects of environmental-induced failure due to extreme post accident conditions is assessed by conservatively assigning a probability of 0.1 that valve CV-115 fails due to high absorbed radiation dose during the short time frame that the valve is

required to operate following an accident. Since this valve is located outside containment, it would not be exposed to adverse temperature or humidity conditions.

2.6.5 Risk Impact Conclusions

A failure of containment isolation is dominated by the failure to close the manual valve and common cause failure of the two control valves. Installation of an environmentally qualified (more reliable during severe post accident conditions) valve CV-115 does not affect the top event probability. The risk impact of isolation valve CV-115 is concluded to be LOW.

2.6.6 References

2.6-1 Swain, A.D., and H.E. Guttman, "Handbook of Human Reliability analysis with Emphasis on Nuclear Power Plantr Applications", NUREG/CR-1278, August 1983.

2.6-2 Pickard, Lowe and Garrick, Inc., "Seabrook Station Probabilistic Safety Assessment", PLG-0300. December 1983 (available from National Technical Information Service).

2.7 Sphere Purge Valves (POV-9, POV-10)

2.7.1 Equipment Description

Sphere purge valves POV-9 and POV-10 are installed outside containment. The valves are 24" pneumatic operated butterfly valves with solenoid valve operators designated as SV-29 and SV-28. The containment penetration is a 24 inch diameter pipe.

2.7.2 Safety Function

According to the operating instruction SOI-5-11 (Reference 2.7-1) the containment is not to be purged while in Modes 1-4; i.e, purging is only allowed with the plant in cold shutdown. Furthermore, surveillance instruction SOI-12.3-6 (Reference 2.7-2) includes the required purge valve alignments; these valves are in the locked closed position during power operation and the instruction includes a check-off provision for both POV-9 and POV-10. In addition, the manually operated butterfly valves in series with POV-9 and POV-10 are locked closed in accordance with SOI-5-11 requirements. On high containment pressure (above 1.4 psig), high radiation, safety injection indication, or remote manual operation the solenoid valves for POV-9 and POV-10 are energized to the open position, thereby directing instrument air from the pressure regulator (air set) to the piston actuator. This results in the movement of POV-9 and POV-10 to the closed position which secures the containment purge line following a LOCA or MSLB. Subsequent failure of the solenoid valve does not affect the closed position of either control valve.

2.7.3 Failure Effects

Once these valves have actuated they do not require reactuation during the entire course of the accident. The valves do, however, need to retain their structural integrity for the course of the accident to ensure that they remain in the closed position. Containment purging is governed by plant procedures to minimize instances of having a degraded containment integrity during power operation. The normally locked closed POV-9 eliminates loss of the purge line isolation function.

2.7.4 Quantitative Assessment

A fault tree analysis, see Figures 2.7-1, is performed under the pessimistic assumption of having left POV-9 or POV-10 in the open position upon resuming power operation (this is in violation of procedures). The top event is open release path via the purge line and is conditional on the occurrence of a large LOCA. The normally locked closed manual butterfly valves in series with POV-9 and POV-10 are assumed to be inadvertently left in the open position.

2.7.5 Risk Impact Conclusions

Given that POV-9 or POV-10 is left open, then the event of having an open release path through either the supply or exhaust line after the occurrence of a large LOCA is very unlikely. The Oconee RSSMAP study (Reference 2.7-3) discussed the failure to isolate purge lines and concluded that this event is a small contributor to the overall containment leakage probability. The risk impact of this component is therefore concluded to be LOW.

2.7.6 References

2.7-1. San Onofre Nuclear Generating Station Unit 1, "Operating Instruction SOI-5-11", May 1982.

2.7-2. San Onofre Nuclear Generating Station Unit 1, "Surveillance Instruction SOI-12.3-6", December 1981.

2.7-3. Sandia National Laboratories,"Reactor Safety Study Methodology Applications Program: Oconee 3 PWR Plant", NUREG/CR-1659, 1981.

2.8 Instrument Air Exhaust Vent Header Control Valve (CV-40)

2.8.1 Equipment Description

The instrument air exhaust vent header control valve CV-40 (ASCO Type 8345 C11) is installed inside the containment. It is a pneumatic diaphragm actuated 3-way control valve with an identical valve in series outside the containment with the designation CV-10. Both the control valves are operated by solenoid valves designated as SV-19 and SV-28 respectively. The containment penetration is a 6 inch diameter pipe.

2.8.2 Safety Function

Under normal operating conditions, CV-40 is open to allow instrument air exhaust to be discharged into the ventilation system and out the plant stack. On high containment pressure (above 1.4 psig), high radiation,safety injection, or remote manual operation, the solenoid valves for CV-40 and CV-10 are deenergized to the vent position thereby securing instrument air from the pressure regulators to the valve actuators. This results in the spring return of CV-40 and CV-10 to the vent port position which secures instrument air exhaust from leaving containment as a containment isolation function following a LOCA or MSLB.

Once the valves have actuated they do not require reactuation during the entire course of the accident. They do, however, need to retain their structural integrity for the course of the accident to ensure that

they remain in the vent port position maintaining containment isolation. Loss of power or instrument air does not jeopardize the vent port position.

2.8.3 Failure Mode Analysis

Loss of containment isolation requires both valves to fail on demand. This can occur either in the event of coincident independent valve failures or in the event of a common cause failure involving both valves. A functional fault tree, including quantitative estimates, for the containment isolation function is shown in Figure 2.8-1. The possibility of manually closing valve CV-10 is considered in the fault tree.

2.8.4 Quantitative Assessment

The effectof equipment failure due to extreme post accident conditions is assessed by assigning a probability of 0.9 that valve CV-40 fails due to high humidity following post accident conditions. Similarly, the failure probability in the short term following an accident due to higher radiation is assumed to be 0.1. The common cause failure probability is quantified using a generic beta-factor of 1.25×10^{-1}. Any common cause effects from an extreme environmental condition affecting both CV-40 and CV-10 are not considered.

2.8.5 Risk Impact Conclusions

Loss of the instrument air vent header exhaust isolation is dominated by failure to manually close CV-10 and common cause failure of CV-40 and CV-10. Installation of an environmentally qualified (more reliable during severe post accident conditions) valve does not affect the top event probability. The risk impact of isolation valve CV-40 is concluded to be LOW.

2.9 Sphere Pressure Equalization Control Valve (CV-116)

2.9.1 Equipment Description

Control valve CV-116 is a pneumatic diaphragm actuated butterfly valve (Fisher type 9110 Design RRL-2 with type 656-30 Actuator) installed in the sphere pressure equalizing line to the plant ventilation stack. On high containment pressure (above 1.4 psig) it is isolated by solenoid valve SV-127. The control valve is located inside containment and has a similar valve CV-10 in series outside the containment. The containment penetration is a 6 inch diameter pipe.

2.9.2 Safety Function

Under normal operating conditions, valve CV-116 is blocked open to allow pressure inside the containment sphere to equalize with the pressure outside containment. Valve CV-116 is actuated remote-manually from the control room between sphere pressure of +0.4 psig and -1.7 psig to reestablish equalization with outside ambient pressure. On high sphere pressure (above 1.1 psig), high radiation, safety injection or remote manual operation, the solenoid valve for CV-116 is deenergized to the vent position, thereby securing instrument air from the pressure regulator (air set) to the valve actuator. This results in the spring return of CV-116 to the closed position which secures exhaust of containment atmosphere from the sphere as a containment isolation function following a LOCA or main steam line break.

Once CV-116 has actuated it does not require reactuation during the entire course of the accident. CV-116 does,

however, need to retain its structural integrity for the course of the accident to ensure that it remains in the closed position, securing exhaust of containment atmosphere from the sphere and thereby isolating containment. Loss of power or instrument air does not jeopardize the closed position of CV-116 since actuator spring force keeps CV-116 in the closed position.

2.9.3 Failure Mode Analysis

Loss of the containment isolation function requires that both valve CV-116 and CV-10 fail on demand. This can occur either in the event of coincident independent failures or in the event of a common cause failure involving both valves. The functional fault tree for this system is virtually identical to that of CV-40, presented in Figure 2.8-1. The possibility of manually closing valve CV-10 is considered in the fault tree.

2.9.4 Risk Impact Conclusions

The functional fault tree shows containment leakage through the sphere pressure equalizing line to be dominated by a human error to manually close valve CV-10 and common cause failure of CV-116 and CV-10. Installation of an environmentally qualified (more reliable during severe post-accident conditions) valve does not affect the top event probability. The risk impact of isolation valve CV-116 is concluded to be LOW.

2.10 Excess Letdown Heat Exchanger Isolation Valve (CV-287)

2.10.1 Equipment Description

Valve CV-287 (manufactured by ASCO) isolates the excess letdown heat exchanger line. Its solenoid valve is operated manually from a remote control station. The valve is located inside the containment. There is one manual isolation valve located upstream from the control valve. On the downstream side of the excess letdown heat exchanger, still inside containment, there is a second control valve designated as CV-288 that is controlled by a remote manual switch as well. The letdown flow goes to the reactor coolant system drain tank. Control valve CV-104, previously discussed, isolates the drain tank discharge inside containment and this particular valve is actuated automatically by high containment pressure.

2.10.2 Safety Function

Valve CV-287 is normally closed and its safety position is closed. If the valve is not closed, the operator will close the valve early in an accident situation. Given a failure of this valve to close on demand, the operator has valve CV-288 available for isolating the letdown flow. Failure of both these valves requires that the drain tank discharge and vent lines be isolated.

2.10.3 Failure Mode Analysis

The top event under consideration is failure to isolate the reactor coolant system (RCS) letdown flow to the RCS drain tank (See Figure 2.10-1). This event is made conditional on CV-287 being in the open position. An open flow path is only possible if the manual isolation valve is left open, and the two control valves fail on demand.

2.10.4 Quantitative Assessment

The effects of equipment failure due to extreme post accident conditions is assessed by assigning a probability of 0.9 that valve CV-287 fails due to high humidity following post accident conditions. Similarly, the failure probability in the short term following an accident due to high radiation is assumed to be 0.1.

2.10.5 Risk Impact Conclusions

Loss of the isolation function is a very unlikely event. It should also be noted that should isolation not occur, the net result would be a relatively small RCS leak into containment. This leakage is insignificant, however, when compared with the leak rate resulting from the LOCA initiator. The risk impact of control valve CV-287 is therefore concluded to be LOW.

2.11 Component Cooling Water System Temperature Sensor (TE-606)

2.11.1 Equipment Description

Temperature sensor TE-606 (Foxboro, Type DB-13V-26W) is part of the component cooling water system (CCWS) and monitors the component cooling water temperature. The instrument is located outside the containment, downstream of the component cooling heat exchangers on the main supply line to various components. It sends a signal to a temperature indicator in the control room as well as a temperature recorder with a high temperature alarm.

2.11.2 Safety Function

The temperature sensor is part of the equipment supporting plant operations. It is not required for the operation of the CCWS.

2.11.3 Failure Mode Analysis

If the temperature sensor fails, then the component cooling water temperature can be read at the discharge of the component cooling water pumps. Also, there is a local temperature indicator at the discharge side of the CCW heat exchanger.

There is a surge tank for the CCWS to accomodate changes in operating volume due to changes in operating temperature. Surge tank levels are indicated and alarmed in the control room. In case all temperature monitoring capability is lost, then the surge tank level indication provides a redundant means of alarming serious

malfunctions.

In a PRA context the CCWS is evaluated for its ability to perform its heat removal duties during the recirculation phase of all LOCAs and all transient events. The function of the system is to remove residual and sensible heat from residual heat removal (RHR) heat exchangers, the recirculatn heat exchanger, RHR pumps and charging pumps. Results from PRA studies show that the dominant contributors to failure of the CCWS to supply a sufficient amount of cooled water given an initiating event (LOCA or transient) during the first 24 hours are:

- For No Loss of Offsite Power Cases:
  - -Random failure in the heat exchanger trains.
  - -Failure of the CCW pump trains to supply water due to random hardware failures.

- For Transient Loss of Offsite Power Cases:
  - -Random failure in the heat exchanger trains.
  - -Failure of the CCW pump trains to supply water due to random hardware failures, primarily pump failure to start on demand.

The temperature sensor is not required for the operation of the CCWS and effects from instrumentation on the system operation are typically not included in plant specific analyses. Different indicators and alarms on the safeguards panel in the control room will direct the operators to any malfunctions before primary system degradation.

2.11.4 Quantitative Assessment

The analysis of the effect of a failed temperature sensor is made conditional on a large LOCA and the complete loss of component cooling. Figure 2.11-1 is a functional fault tree for the primary system degradation given a LOCA. The tree includes the failure of all CCW temperature monitoring, loss of surge tank level control and loss of the radiation alarm system.

2.12.5 Risk Impact Conclusions

Loss of the temperature monitoring function coincident with a series of other failure events has only a small impact on the top event under consideration. Installation of an environmentally qualified temperature monitoring system does not affect the top event probability. This risk impact of temperature sensor TE-606 is considered LOW.

3. Discussion of Results

3.1 Important Contributors to Plant Risk

The published PRA studies have identified dominant accident scenarios as part of the effort to quantify the frequency of severe core damage. All studies that have been performed to date have not identified the same dominant contributors, but there are, despite this fact, some noteworthy commonalities:

1. Most PRAs have identified loss of offsite power initiated scenarios as important contributors to core damage frequency. In WASH-1400, loss of offsite power contributed 5% to the total core melt frequency for Surry.

2. Some PRAs that considered external events have identified dominant scenarios initiated by these events.

3. Small leak loss of coolant accidents have also been identified as important scenarios in many PRAs.

The components analyzed in the previous section do not appear in any of the risk significant scenarios that are identified in the published PRA studies. All the 15 components can be characterized as belonging to the outliers in the San Onofre Unit 1 plant risk topography, both from a short and long term risk perspective.

3.2 Summary of the Assessed Plant Risk Impact

Common to all the 15 components is the fact that none of them have any direct influence on the operation of the front line safety systems. Furthermore, they all have low risk impact indices and in order to see any notable effect on the San Onofre Unit 1 risk profile, a series of rare events need to occur in conjunction with failure of the function of which the respective component is a part. Any notable positive effects from improving the components resistance against extreme environmental conditions have not been identified in the bounding-type assessments of plant risk impact.

TABLE 1 RESULTS OF SOME PROBABILISTIC RISK ASSESSMENTS

PLANT	PRA [a]	F, CORE MELT [b]	F, MAJOR RELEASE [b]
Arkansas Nuclear One - 1	IREP	5×10^{-5}	2×10^{-5}
Biblis B	German RSS	4×10^{-5}	1×10^{-6}
Browns Ferry	IREP	2×10^{-4}	4×10^{-5}
Crystal River	IREP	4×10^{-4}	2×10^{-4}
Grand Gulf	RSSMAP	4×10^{-5}	4×10^{-5}
Indian Point 2	PLG	4×10^{-4}	3×10^{-4}
Indian Point 3	PLG	9×10^{-5}	3×10^{-5}
Limerick	SAI	2×10^{-5}	3×10^{-6}
Millstone	IREP	3×10^{-4}	1×10^{-4}
Oconee	RSSMAP	8×10^{-5}	4×10^{-5}
Peach Bottom	WASH-1400	3×10^{-5}	7×10^{-6}
Sequoyah	RSSMAP	6×10^{-5}	4×10^{-5}
Surry	WASH-1400	6×10^{-5}	1×10^{-5}
Zion	PLG	4×10^{-5}	4×10^{-6}
Ringhals 2	NUS	4×10^{-6}	--

Notes:

a. This column refers to the Nuclear Regulatory Commission (NRC) sponsored program or the study team of utility sponsored PRAs respectively;
   - IREP - Interim Reliability Evaluation Program (NRC)
   - RSSMAP - Reactor Safety Study Methodology Applications Program (NRC)
   - SAI - Science Applications, Inc. (contractor)
   - PLG - Pickard, Lowe and Garrick, Inc. (contractor)
   - NUS - Nuclear Utility Services Corporation (contractor)

b. All numbers are median values of yearly occurrence frequency

TABLE 2. A SELECTION OF INITIATING EVENT FREQUENCIES IN DIFFERENT PRAs

Initiating Event	Zion	Indian Point 2	Indian Point 3	ANO-1	Surry	Crystal River	Sequoyah
Large LOCA	9.4-4	1.95-3	2.16-3	7.5-4	1.0-4	1.0-4	4.7-5
Medium LOCA	9.4-4	1.95-3	2.16-3	1.6-4	3.0-4	1.0-4	9.8-4
Interfacing System LOCA	1.05-7	4.58-7	4.64-7	Є	4.0-6	Є	4.6-6
Small LOCA	3.54-2	1.85-2	2.01-2	2.0-1	1.0-3	1.0-4	1.8-3
Very Small LOCA						1.3-3	
Vessell Rupture					1.0-7		
SGTR	2.44-2	2.74-2	3.37-2			Є	
Steam Line Break (inside/ outside)	9.04-4	1.95-3	2.16-3				
Turbine Trip	3.69	7.32	2.72			1.92	
LOOP	5.76-2	1.82-1	2.66-1	3.2-1	2.0-1		2.0-1
Reactor Trip	3.77	6.84	2.86				
Loss of Main Feedwater	5.17	6.7	3.8	1.0	3.0		3.0
Loss of Service Water	9.4-4	1.95-3	2.16-3	2.6-3			
Loss of Component Cooling Water		1.95-3	2.16-3				

Notes: All initiating event frequencies: (frequencies per year) are mean values.
Exponential notation is indicated in abbreviated form; i.e., 9.4-4 = 9.4×10^{-4}
Negligible frequency is characterized by an Є

Table 3. Classification of Risk Impact Indices

Classification	Criterion
HIGH	Failure of a component is main contributor to a dominant fault tree top event or a dominant accident sequence event.
MEDIUM	Failure of a component contributes but does not dominate an important top event or a dominant accident sequence event.
LOW	Failure of a component does not have an impact on dominant fault tree top event or dominant accident sequence event.

TABLE 4. COMPONENTS REQUIRING EXTENSION OF 10CFR50.49 DEADLINE

COMPONENT	SYSTEM	REQUIRED SAFETY FUNCTION	WORST CASE RISK IMPACT
Flow Transmitter FT912, 913, 914	Safety Injection System (SIS)	Surveillance of safety injection flow on a loss of coolant inventory event.	Given failure of all transmitters with a coincident failure of the RWST level indication system the operators may either terminate safety injection or fail to initiate timely switchover to recirculation. Ultimate consequence could be core damage.
Control Valve CV-82, 114	Containment Spray System	Open containment spray path on high containment pressure	Complete failure of containment spray may ultimately lead to failure of containment structure with release of radioactive products
Control Valve CV-102, 104, 106, 115, POV-9, 10, CV-40, 116, 287	Containment Isolation System	Close on high containment pressure	Complete isolation failure results in a release path to the environment.
Temperature Sensor TE 606	Component Cooling Water System (CCWS)	Surveilance of component cooling water temperature	Complete failure of temperature surveillance can lead to damage of component cooling water pumps.

TABLE 5. GENERIC FAILURE DATA FOR THE EQUIPMENT REQUIRING EXTENSION OF THE 10CFR50.49 DEADLINE

COMPONENT	LOCATION[2]	POTENTIAL IMPACT OF ENVIRONMENT ON COMPONENT RELIABILITY	FAILURE MODE	FAILURE RATE[3] (MEAN)	SOURCE[4]
Flow Transmitter FT 912, 913, 914	0	Susceptibility to long-term effects from accumulation of high radiation dose. Pipe break outside containment causes saturated steam condition	Fail during operation	6.25-6/h	(1)
Temp Sensor TE 606	0	During long term recirculation, the sensor is susceptible to long term effects of high radiation dose. Normally located in an ambient environment	Fail during operation	5.30-6/h	(2)
Solenoid Valve SV-118, SV-128	I	Steam in containment following pipe break may short the solenoid. These particular solenoid valves are required to be operable several seconds subsequent to a LOCA or MSB	Fail to operate on demand	2.43-3/d	(1)
SV-108, SV-110 SV-112	I	Same as for SV-118, SV-128 Required to be operable several seconds subsequent to a LOCA or MSB	"	"	"
SV-126	0	Susceptible to long term effects from accumulation of high radiation dose.	"	"	"
SV-29, SV-30	0	Same as above. Required to be operable several seconds subsequent to a LOCA or MSB	"	"	"
SV-19, SV-127	I	Steam in containment following pipe break may short the solenoid. Required to be operable several seconds subsequent to a LOCA or MSB	"	"	"

TABLE 5. (CONTINUED)

COMPONENT	LOCATION[2]	POTENTIAL IMPACT OF ENVIRONMENT ON COMPONENT RELIABILITY	FAILURE MODE	FAILURE RATE[3] (MEAN)	SOURCE[4]
Control Valve			Fail to operate on demand	1.52-3/d	(1)
			Fail to transfer to failed position	2.66-4/d	(1)
CV-82 (SV-128)[1] CV-114 (SV-118) CV-102 (SV-108) CV-104 (SV-110) CV-106 (SV-112)	I	Steam in containment following pipe break may short the solenoid. These particular solenoid valves are required to be operable several seconds subsequent to a LOCA or MSLB	"	"	"
CV-115 (SV-126)	0	Susceptible to long term effects from accumulation of high radiation dose	"	"	"
POV-9 (SV-29) POV-10 (SV-30)	0				
CV-40 (SV-19) CV-116 (SV-127)	I	Same as for CV-82	"	"	"
CV-287 (SV??)	I	Same as for CV-82	"	"	"

Notes:

1. The respective solenoid valves are given in the parentheses.
2. Inside containment (I), outside containment (O).
3. The failure rates are either per demand or per hour. Failures per demand are indicated as /d and failures per hour are indicated as /h.
4. 1) Pickard, Lowe and Garrick, Inc., "Seabrook Station Probabilistic Safety Assessment", PLG-0300, December 1983. This report is available from the National Technical information Service (NTIS). The component failure rates in PLG-0300 are based on operating experience at various PWRs and data found in industry compendia such as WASH-1400 and IEEE-500.
   2) Nuclear Safety Board of the Swedish Utilities (RKS), "Reliability Data for Components in Swedish Boiling Water Reactors", RKS 82-07, November 1982. This report includes a comprehensive evaluation of operating experience for instrumentation.

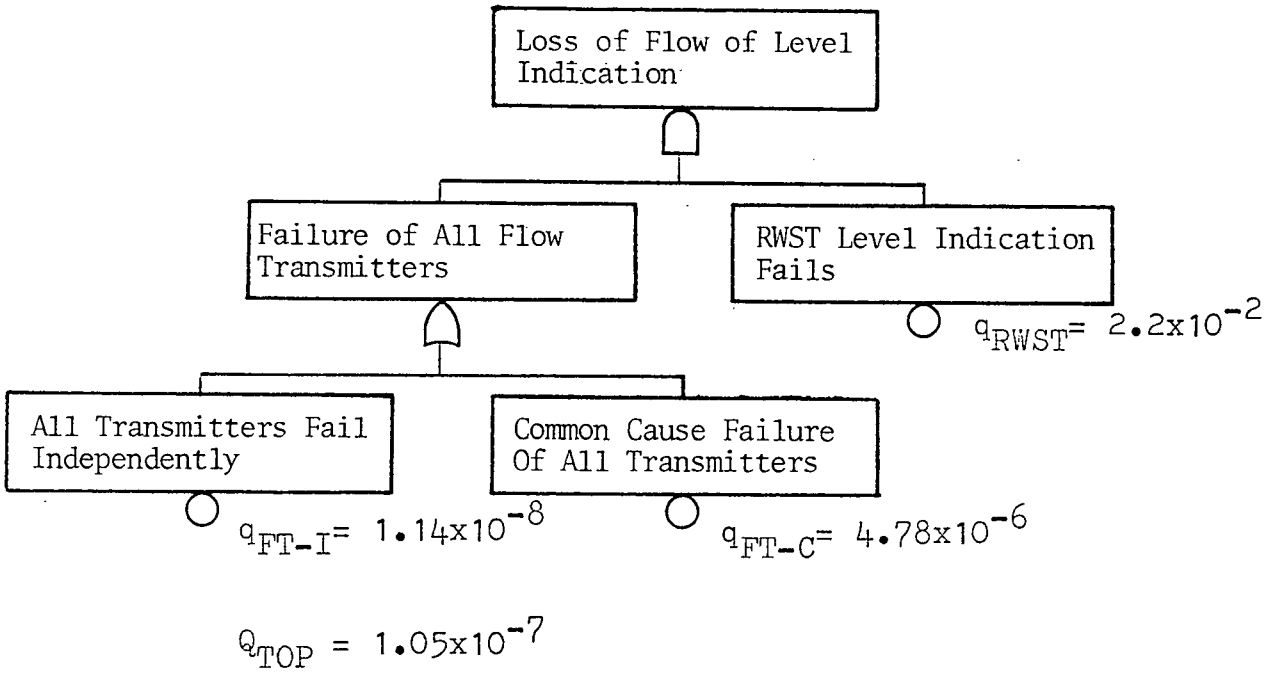


Figure 2.1-1

Fault Tree for Loss of Safety Injection Flow and RWST Level Indication

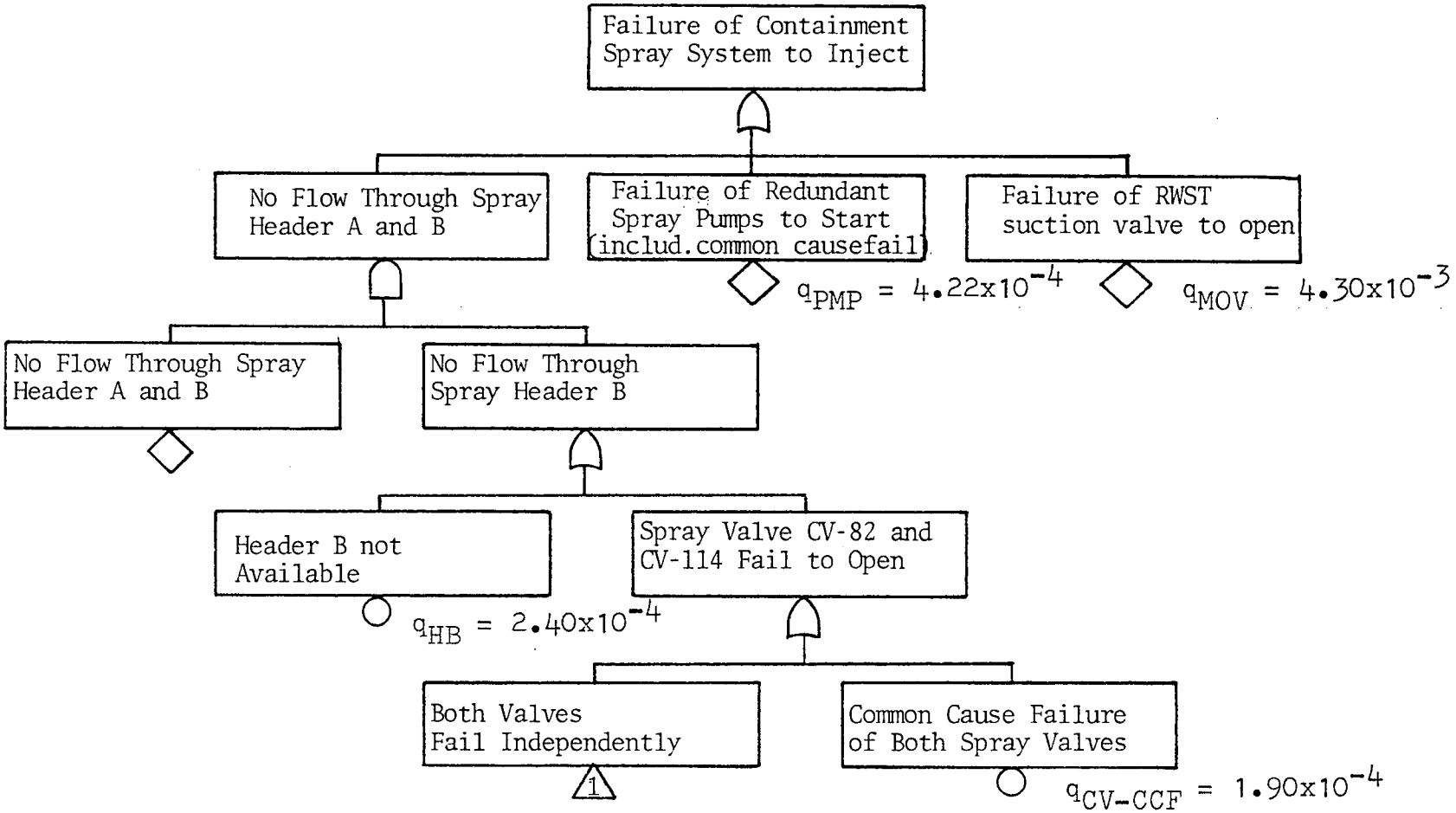
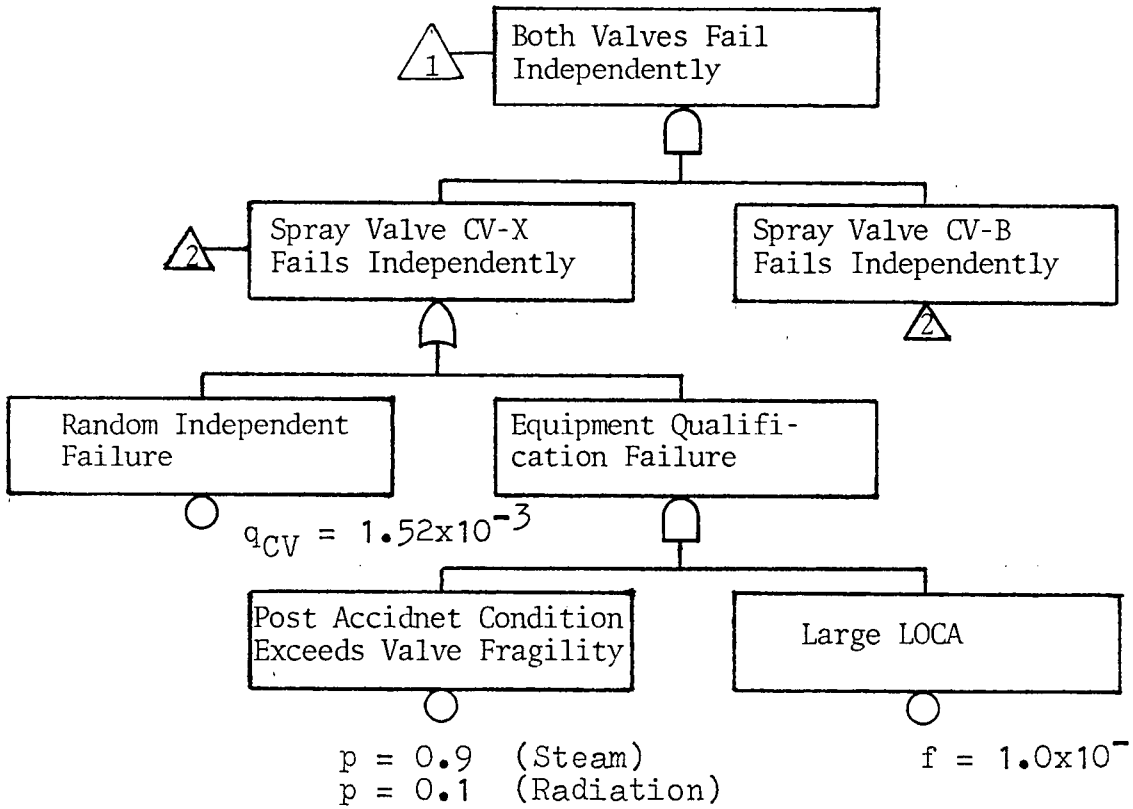


Figure 2.2-1

Fault Tree for Failure of Containment Spray System to Inject (Sheet 1 of 2).



$Q_{TOP} = 4.72 \times 10^{-3}$ (without environmentally qualified valves)

Figure 2.2-1

Fault Tree for Failure of Containment Spray System to Inject (Sheet 2 of 2).

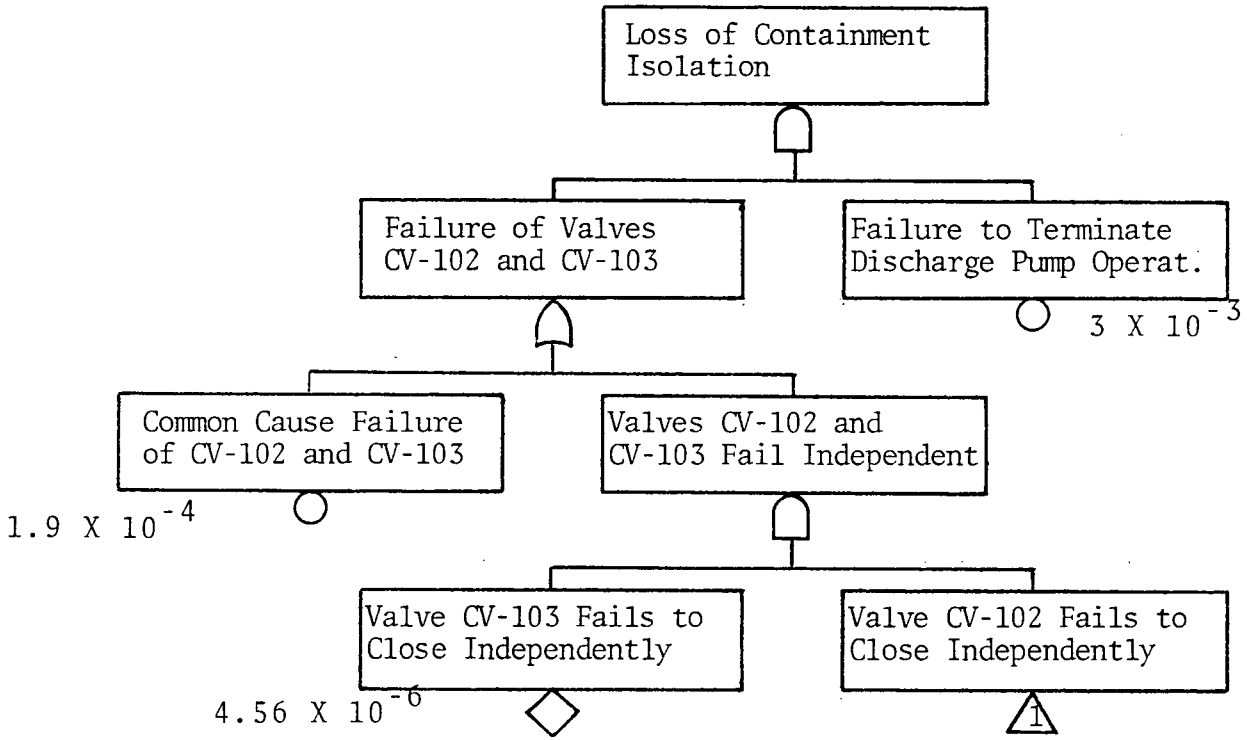
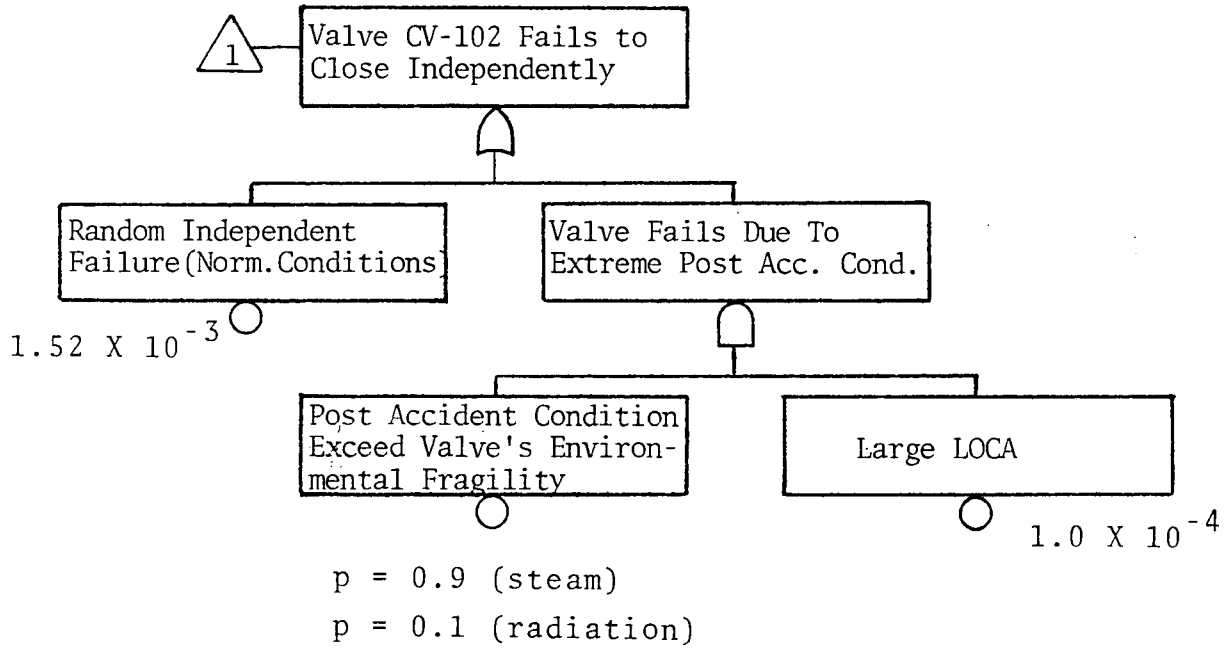


Figure 2.3-1

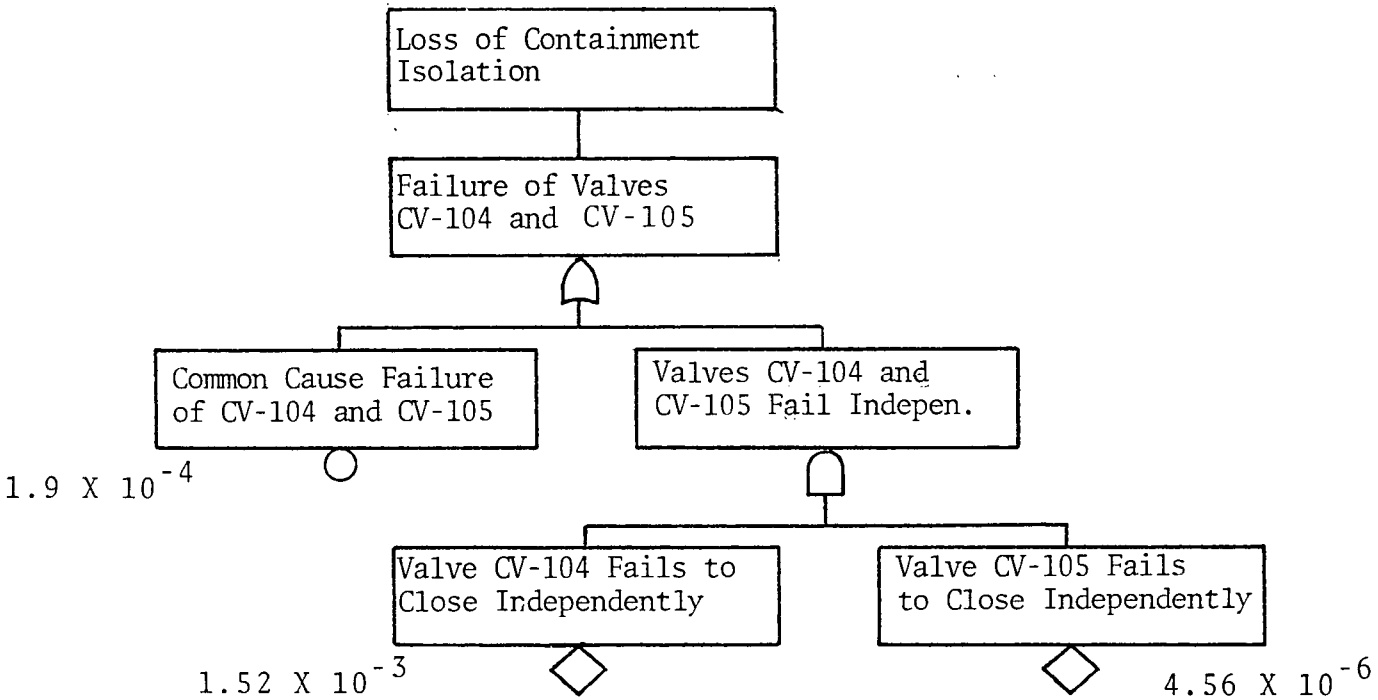
Fault Tree for Failure of the Containment Sump Discharge Line Isolation (Sheet 1 of 2).



$Q_{top} = 5.70 \times 10^{-7}$

Figure 2.3-1

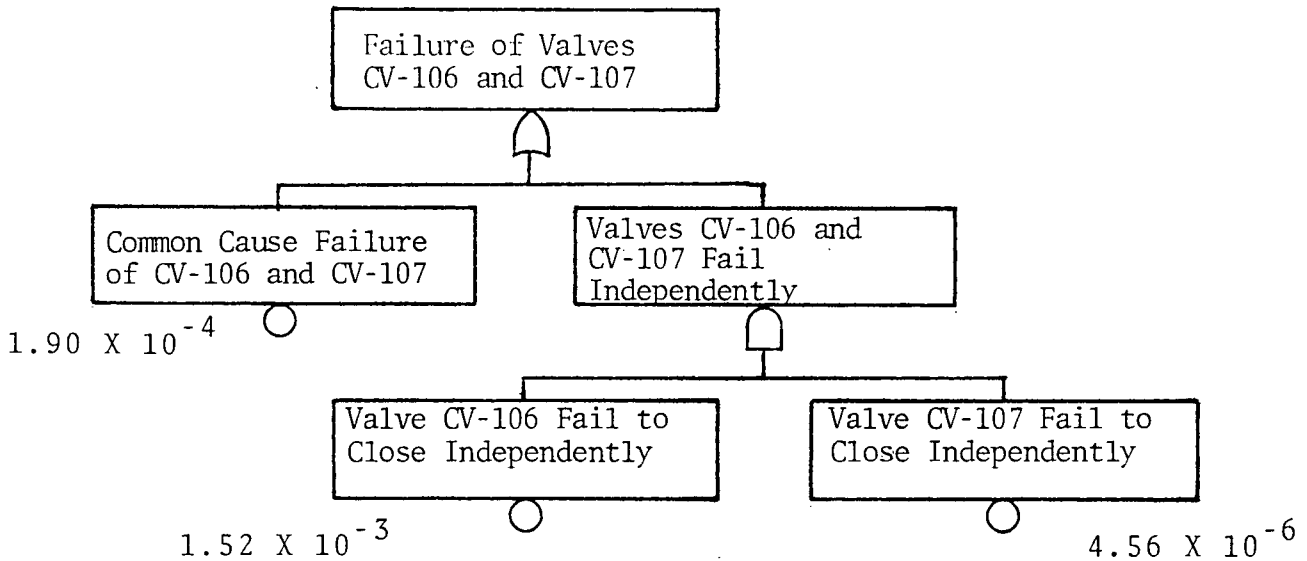
Fault Tree for Failure of the Containment Sump Discharge Line Isolation (Sheet 2 of 2).



$Q_{top} = 1.90 \times 10^{-4}$

Figure 2.4-1

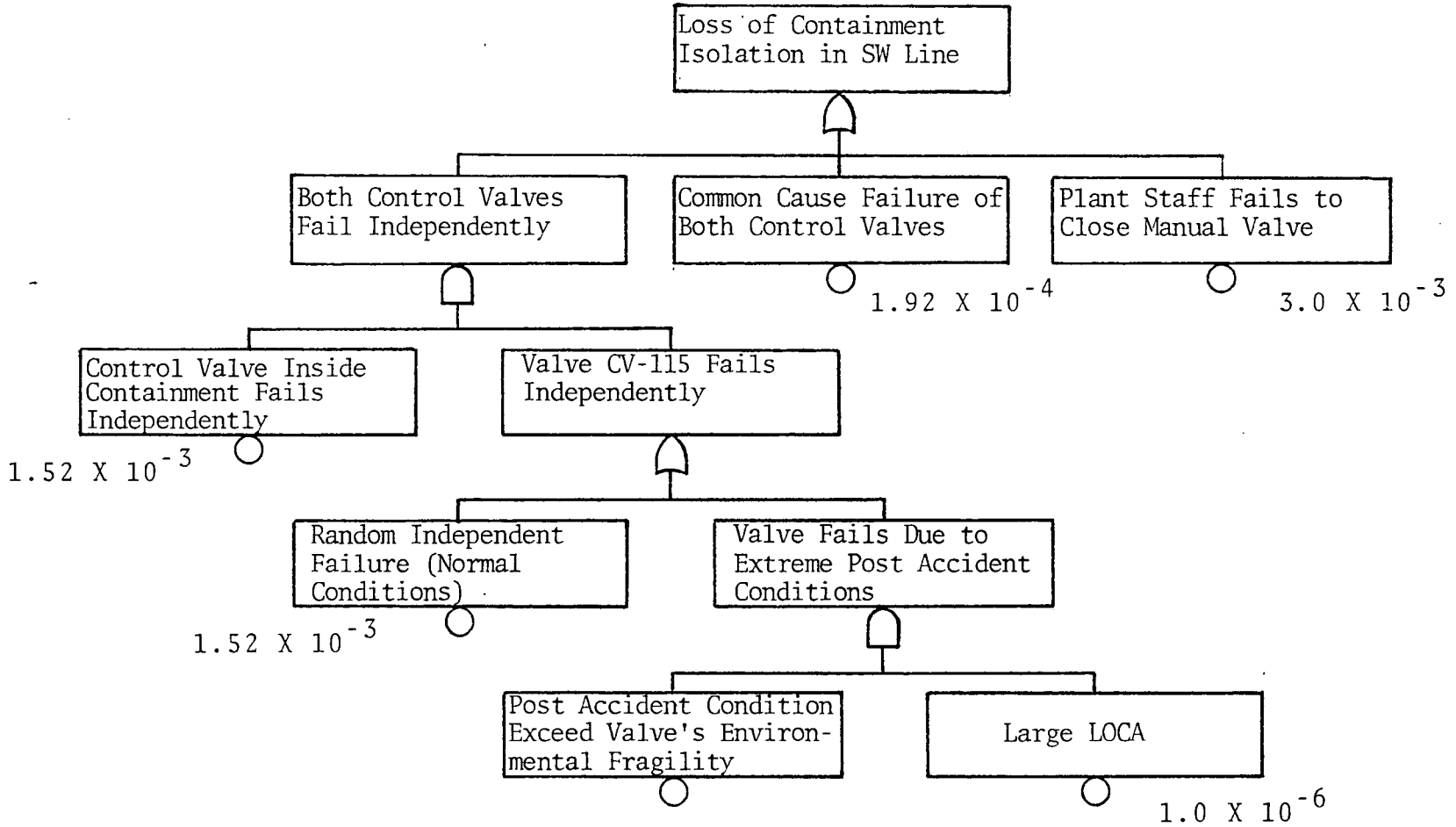
Fault Tree for Failure of the Drain Tank Vent Line Isolation



$Q_{top} = 1.90 \times 10^{-4}$

Figure 2.5-1

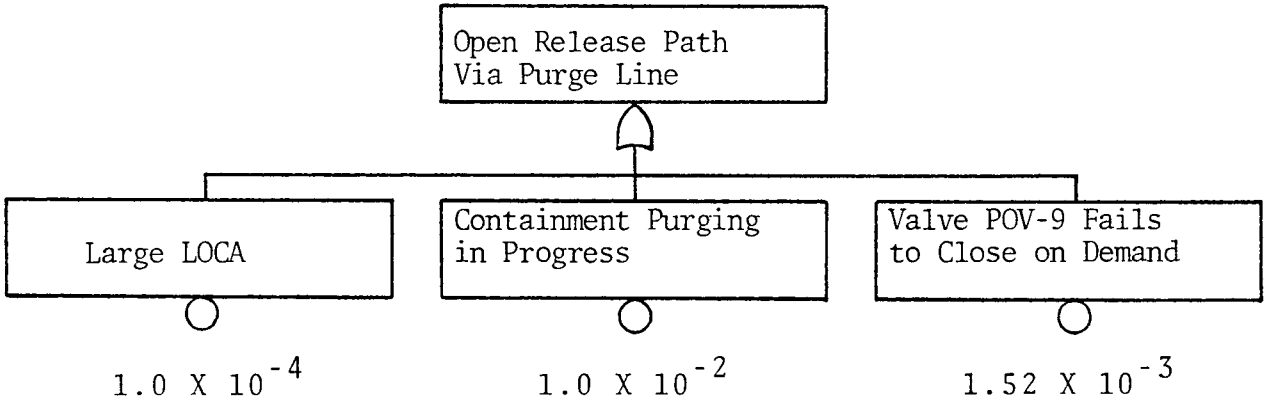
Fault Tree for Failure of the Drain Tank Vent Line Isolation



$Q_{top} = 3.19 \times 10^{-3}$

Figure 2.6-1

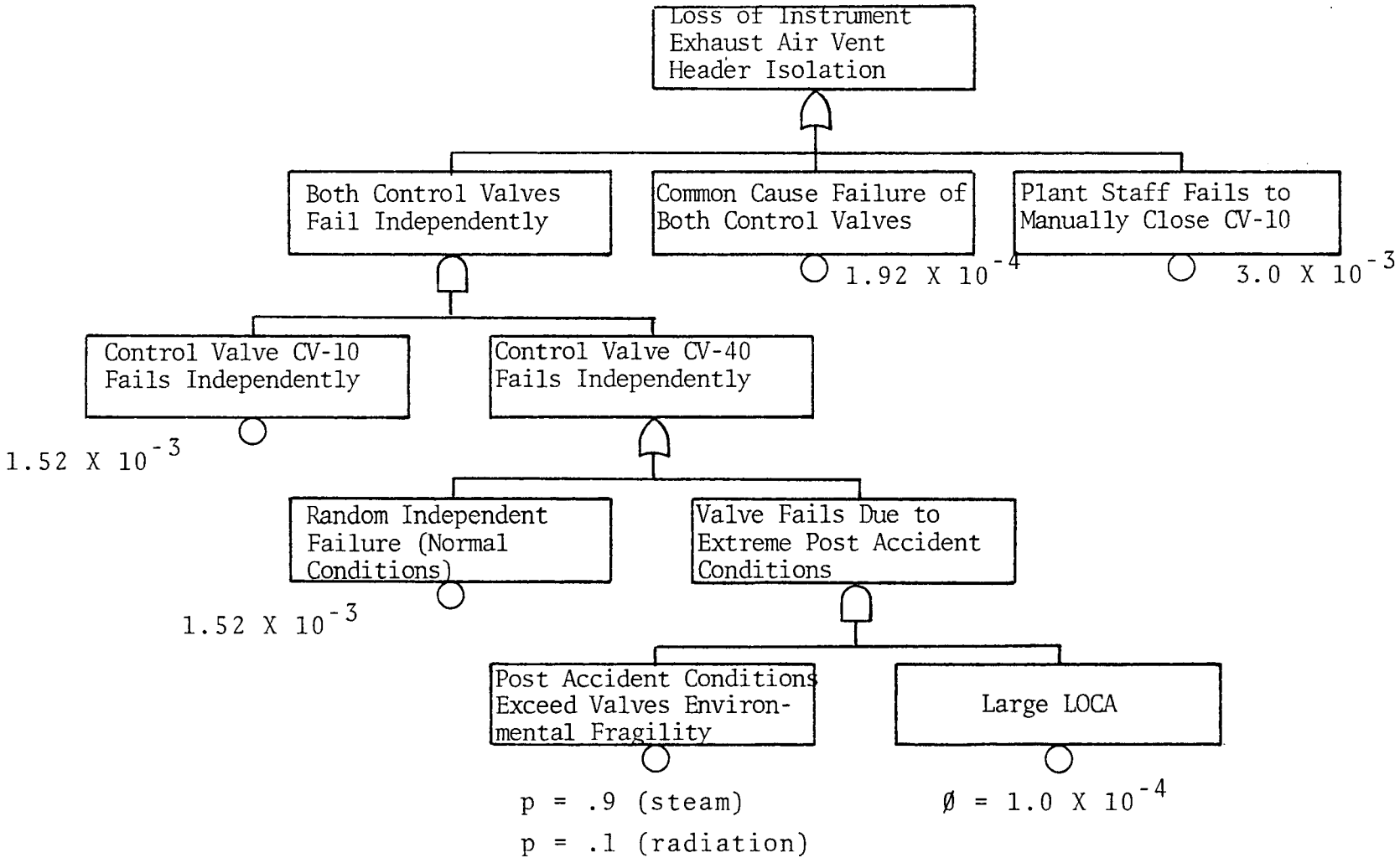
Fault Tree for Failure of the Service Water Supply Line Isolation.



$Q_{Release} = 1.52 \times 10^{-9}$

Figure 2.7-1

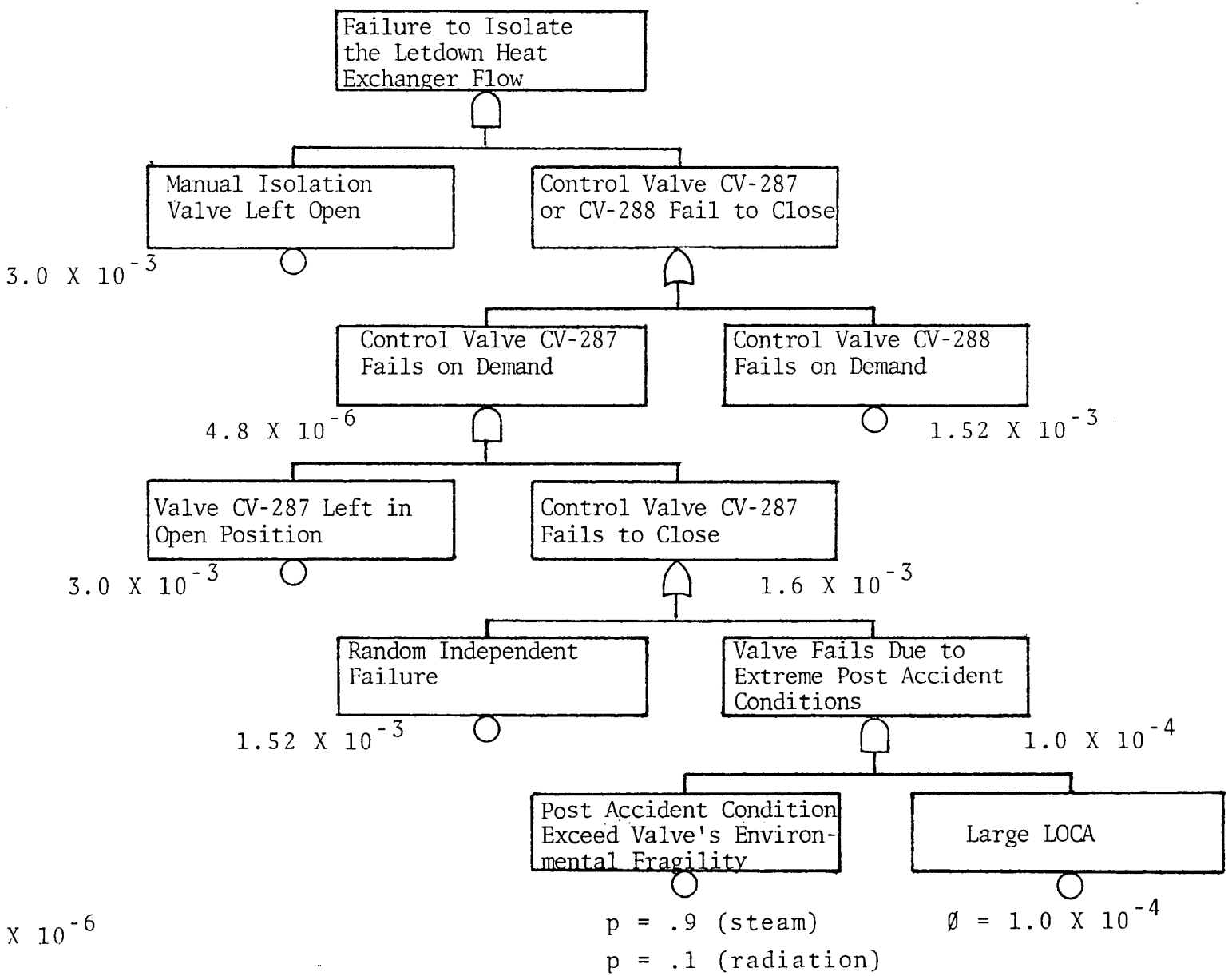
Fault Tree for Failure of the Containment Purge Supply (or Exhaust) Line Isolation.



$Q_{top} = 3.19 \times 10^{-3}$

Figure 2.8-1

Fault Tree for Failure of the Instrument Exhaust Air Vent Header Isolation.



$Q_{top} = 4.5 \times 10^{-6}$

Figure 2.10-1

Fault Tree for Failure of the Letdown Heat Exchanger Flow Line Isolation.

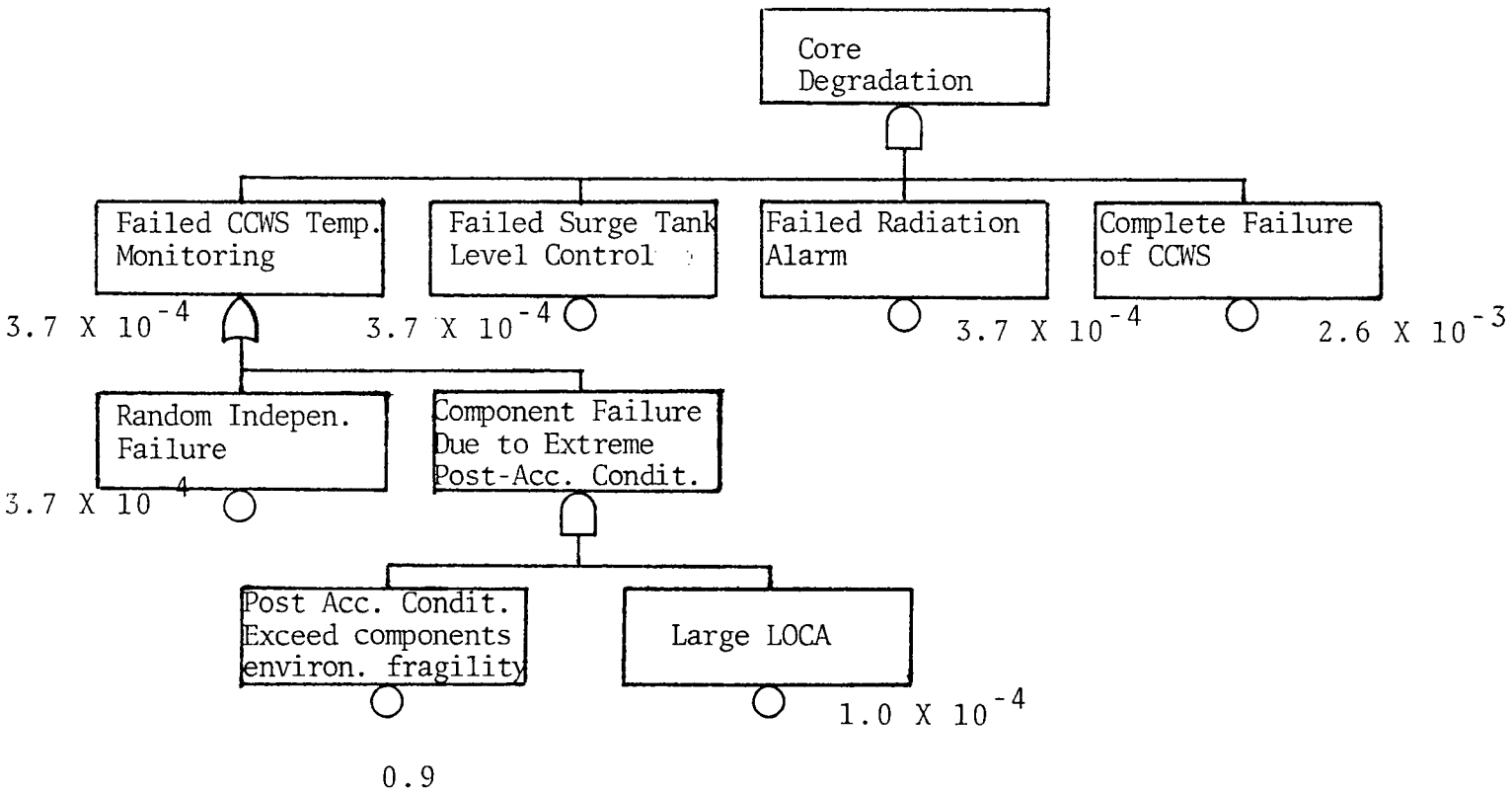


Figure 2.11-1

Functional Fault Tree for Loss of all CC Temperature Indication.