



LONG ISLAND LIGHTING COMPANY

SHOREHAM NUCLEAR POWER STATION

P.O. BOX 618, NORTH COUNTRY ROAD • WADING RIVER, N.Y. 11792

December 2, 1982

SNRC-805

Mr. Harold R. Denton, Director
Office of Nuclear Reactor Regulation
U.S. Nuclear Regulatory Commission
Washington, D. C. 20555

Evaluation on Internal Flooding
Shoreham Nuclear Power Station - Unit 1
Docket No. 50-322

Dear Mr. Denton:

The purpose of this letter is to respond to a NRC letter dated September 29, 1982 for a LILCO evaluation of concerns expressed by Future Resources Associates (FRA), regarding reactor building internal flooding sequences due to inadvertant valve operation during maintenance. The following enclosures (forty copies) are provided:

Enclosure 1 - Response to the FRA estimate of core vulnerable condition¹ due to postulated internal flooding sequences.

Enclosure 2 - A detailed re-analysis by our PRA consultant, Science Applications, Inc. (SAI), of postulated flooding sequences that lead to a core vulnerable condition. Flow rates, water sources, equipment vulnerability levels, and response times are addressed in an appendix to this report.

The basic conclusions of the re-analysis are:

1. The internal flooding initiator is a highly improbable event which requires gross violations of power plant administrative controls on maintenance not accounted for in the FRA analysis.

¹The term "core vulnerable" as utilized in the draft Shoreham PRA refers to a time-dependent loss of core cooling function. No credit is taken in this calculation for systems such as condensate transfer, ultimate cooling or fire pump which are also available to the operator. These systems were evaluated in the containment event tree portion of the Shoreham draft PRA in the calculation of core melt probability.

December 2, 1982
Mr. Denton
Page 2

2. Internal flooding sequences due to maintenance leading to core vulnerable states are not dominant accident sequences for Shoreham when compared with other accident sequences evaluated in the draft Shoreham PRA. A conservative estimate of the core vulnerable frequency contribution is 1.5×10^{-6} /year.
3. An as-built survey of electrical equipment was performed and confirms that the reactor building floor area is sufficiently large to accommodate very large quantities of water prior to inundating safety equipment.
4. Both non-safety and safety-grade level instrumentation alarms in the control room provide the reactor operator an early warning of potential flooding hazards.
5. The operator can isolate the flood source from the control room.
6. Given a flooding condition, safe shutdown can be achieved with the power conversion system per emergency procedures which is not degraded by the flooding condition due to its location. The condensate system provides a highly reliable source of water in all scenarios. In addition, the availability of feedwater pumps was treated conservatively in this analysis taking into account flooding scenarios which potentially lead to reactor isolation.

The above conclusions are consistent with those of the draft Shoreham PRA.

In response to your request for a LILCO position on design changes, the following information is provided:

The Shoreham PRA was performed as a continuing risk management tool for use by LILCO over the life of the plant. The Shoreham PRA addresses the sources of risk associated with postulated accident sequences in comparable detail to a "level 3" PRA. In addition, the Shoreham PRA includes a detailed state-of-the-art technology evaluation of both in-plant and ex-plant consequences associated with the identified low probability accident sequences.

In addition to the above scope of work, LILCO identified that a specific probabilistic analysis should be performed on the impact of the release of excessive water onto the elevation 8'0" floor of the reactor building.

The results of the updated probabilistic analysis of the internal flood sequences due to maintenance indicates that the calculated frequency of these postulated events taken together represent a

small fraction of the best estimate core vulnerable frequency. Based upon this finding, the sequences involving postulated large internal floods do not represent risk "outliers" at Shoreham. This small contribution should be evaluated along with the other identified contributors to risk to determine if there are any cost-effective methods to minimize the frequency of identified risk contributors. Plant or procedural changes should be assessed in the context of a cost/benefit evaluation recognizing that residual risks will persist despite the changes in a single group of sequences.

Based upon LILCO's cost/benefit considerations, coupled with the fact that the frequency of the postulated sequences is very low, there does not exist sufficient justification for plant modifications to further reduce the frequency of these postulated sequences. However, LILCO's review of the SAI re-analysis indicates that although the overall risk due to internal flooding events is very low, the opportunity does exist for prudent positive actions that provide additional cost-effective risk reduction in both the areas of prevention and mitigation of postulated flooding events. In this light, the following actions will be taken by LILCO:

1. Tagging procedures will be enhanced to provide additional appropriate cautionary information to maintenance personnel on specific boundary valves which have been shown to be important to flooding sequences, and
2. LILCO will continue efforts with the BWR Owners Group to arrive at a meaningful Secondary Containment Control Procedure which will provide additional specific guidance to the operator for dealing with postulated flooding events.

In the course of finalizing the preparation of this submittal, a letter from the NRC (A. Schwencer) to LILCO (M. S. Pollock), dated November 24, 1982, was received which requested additional information. LILCO has reviewed this letter and has concluded that the SAI re-analysis enclosed, in conjunction with additional information forwarded by letters SNRC-794, SNRC-792, and SNRC-783, is responsive to this request.

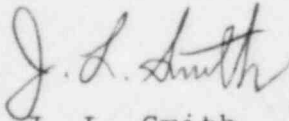
It should be noted that FRA did not, in its analysis, account for the fundamental fact that boundary valves of concern to flooding sequences are required both by LILCO procedure and standard power plant operating practice to be de-energized during maintenance acts. This omission in the FRA analysis in large part accounts for the discrepancy in the calculation. The enclosed SAI analysis resolves this discrepancy and others.

December 2, 1982
Mr. Denton
Page 4

This submittal concludes LILCO's review of the FRA concerns and should, in LILCO's judgement, close this issue on the Shoreham docket.

Should you have any questions, please contact this office.

Very truly yours,



J. L. Smith
Manager, Special Projects
Shoreham Nuclear Power Station

RJT:jm

c.c.: J. Higgins
All Parties

ENCLOSURE 1

RESPONSE TO FUTURE RESOURCES
 COMMENTS CONCERNING INTERNAL FLOODING
 DUE TO MAINTENANCE ACTS

In response to the Future Resources Analysis (FRA) comments concerning the internal flood analysis appearing in the Shoreham draft PRA, a complete reanalysis has been performed. This conservative analysis estimates that there are maintenance induced internal flooding sequences involving Elevation 8 of the reactor building having a core vulnerable frequency value of $1.5E-6$. This result indicates that these flooding scenarios have a small contribution to risk on the order of 3%. The following discussion compares the results of this reanalysis reconstructed to the form of the sequence mentioned in the FRA draft report.

The FRA report presents the following approximation for a maintenance-induced-flood core vulnerable accident.

expected no. of on-line maintenances per year	probability that the system is disassembled given mainten- ance	probability that the operator opens the isol- ation valve dur- ing maintenance	probability operator fails to reclose the isolation valve	probability that the operator erroneously isolates the power con- version sys- tem during flooding.
--	---	--	--	---

$$E[N_A(\text{one year})] \times P(B/A) \quad \times P(C/A) \quad \times P(D/A \cap B \cap C) \times P(E/A \cap B \cap C)$$

The following discussion compares the SAI reanalysis of this expression with the analysis appearing in the FRA submittal for a human error, during HPCI maintenance event.

$$\underline{E[N_A(\text{one year})] \times P(B/A)}$$

The FRA analysis for this combination of events was done by assuming the number of maintenance acts per year is 1.08, and the probability that a maintenance act will cause a system to be disassembled is 0.1. This yields a probability for the combination of the frequency of $E[N_A(\text{one year})] \times P(B/A)$ to be 0.108 per reactor year.

In a more detailed analysis, SAI has used the LER data base for turbine driven pumps used in BWRs, to determine the expected number of failures per year for the pump. While all the reported failures do not require the system to be opened for maintenance, use of this number will, to some extent, account for unreported maintenance acts that cause the system to be opened. This calculation is described in the revised Appendix A of the submittal, and estimate the value for $E[N_A(\text{one year})] \times P(E/A)$ of 0.079. Although this number is not significantly different from the FRA value, the estimate derived from the LER data base is judged to be more realistic.

P(C/A)

The FRA analysis uses the upper bound of $2.0E-2$ /maintenance outage as the value for P(C/A). This value was taken from Swain and Guttman as an upper bound due to an assumed 3.5 day maintenance outage. This value is for a simple valving error during a maintenance act.

SAI has performed a detailed human reliability analysis of the maintenance procedure requiring isolation of the pump, the associated valves and their controls. This analysis indicates that the maintenance procedures call for power to be removed from the valve operators. When power is removed remote operation of the valves is not possible. In addition, the location of the valves, close to the location where water would be released, makes it highly unlikely that local manual operation of the valves could take place without the operator noticing the water flow and reclosing the valve. Therefore, if power is removed from the isolation valves, it is highly unlikely that the system will become unisolated.

The probability of an inadvertent opening of an isolation valve is the product of two parts: 1) the probability that power is not removed from the valve and 2) the operator inadvertently operates the valve. The conservative estimate for the first event is 0.01, while the estimate used for the second event is 0.02. This yields a probability for P(C/A) of 2×10^{-4} (0.01×0.02).

P(D/A∩B∩C)

The FRA analysis used the curve estimating human performance after a large LOCA to estimate the probability. The estimate used for this event by FRA is 0.25 due to the assumed highly stressful conditions.

SAI has performed a detailed analysis of this event including a procedural and control room review. This analysis used new information concerning cognitive behavior, and simulator data to derive a time-dependent model of operator actions subsequent to a flood event. For the event analyzed here the estimated time available for operator action is 13-17 minutes, depending on the source of water. Using this, the estimated probability for event P(D/A∩B∩C) is 0.1 since it is likely that the flood would be the only "off normal" event going on in the control room for an operator error induced flood during major maintenance.

P(E/A∩B∩C)

The FRA analysis of this event concludes that due to the stressful situation a value of 0.25 or higher is appropriate. In the detailed analysis, SAI has evaluated all possible dependencies that would preclude the use of the PCS (feedwater and condensate) to become unavailable during a flood event occurring while the reactor is at power. The availability of feedwater pumps was found to be dependent on operator actions following a flood event. The condensate system was found to be

a highly reliable source of water in all sequences. The SAI analysis estimates the conditional probability that, given a flood, the probability of core vulnerable sequence is approximately 0.038.

Evaluation of the Resulting Expressions

Evaluation of the expression for flood frequency is shown below:

FRA analysis

$$0.108 \times 0.02 \times 0.25 \times 0.25 = 1.35 \times 10^{-4} / \text{reactor year}$$

SAI detailed reanalysis

$$0.079 \times 2 \times 10^{-4} \times 0.1 \times 0.038 = 6.6 \times 10^{-8} / \text{reactor year}$$

SAI believes that the detailed analysis performed shows that the core vulnerable frequency of flooding scenarios involving HPCI maintenance is conservative. A more realistic analysis estimates a frequency, 3 orders of magnitude lower than the FRA approximation found in their draft report.

SAI-336-82-PA

ENCLOSURE 2

Event Tree Evaluation of Sequences Following a Release of Excessive
Water In Elevation 8 of the Shoreham Reactor Building Due to
Postulated Errors During Maintenance.

November 1982

Prepared For:

Long Island Lighting Company

Prepared By:

Science Applications Inc.
5 Palo Alto Square, Suite 200
Palo Alto, California 94303

1. Event Tree Evaluation of Sequences Following a Release of Excessive Water in Elevation 8 of the Shoreham Reactor Building Due to Postulated Errors During Maintenance

The SNPS Reactor Building surrounds the Mark II containment structure. The majority of safety-related equipment is located throughout the Reactor Building, with the largest concentrations located on elevation 8, the lowest level. All of the ECCS pumps are located in the Shoreham Reactor Building at elevation 8 in a large cylindrical compartment. Such an arrangement provides the benefits of good maintenance access and the capability for natural circulation compartment ventilation; however, there is also a remote possibility of a common mode event disabling all the equipment in the elevation 8 compartment. Therefore, in addition to the initiators considered for a Level 3 PRA (1), the SNPS PRA also includes an evaluation of the potential for public risk due to possible common mode events such as a high water level in the elevation 8 compartment which may disable the ECCS equipment.

A typical scenario involving the release of water into the elevation 8 compartment consists of the following items:

- Leakage in the reactor building would drain to elevation 8' (lowest level) via openings and stairwells

- The reactor building sump indication would give early indication in the control room that water was collecting in the sump
- The ECCS Instrumentation would assist in determining leakage from any safety train for immediate operator isolation
- Redundant, safety related water level detectors located on elevation 8' would alarm in control room at approximately $\frac{1}{2}$ " flood level (approximately 2000 gallons)
- Pumpback system is operated to continuously control postulated leakage by returning leakage to the suppression pool
- The operator takes action to terminate the leak and safely shutdown the plant using normal makeup systems or available ECCS equipment.

Based upon the available indication to the operator, and the capability of the available sump and pump back systems, it is judged that small to medium leaks in the Reactor Building are adequately mitigated by the existing systems and produce a negligible contribution to potential core vulnerable states. However, large postulated leaks may compromise the availability of several systems, therefore this section presents an evaluation of the frequency of

core vulnerable conditions resulting from a large release of water within the Reactor Building.

In order to place these postulated flooding sequences in perspective it should be recognized that:

- The large release of water in elevation 8 is an unlikely event.
- Elevation 8 safety grade water level instrumentation alarms are located in the control room to alert the operator to the potential hazard.
- Safe shutdown can be performed with equipment which is not affected by the postulated flood.

This section provides the logic models used in the elevation of postulated accident scenarios associated with the release of excessive water into the elevation 8 compartment. Figure 1 is a flow chart of the steps and information flow developed for the evaluation of large releases of water in the Reactor Building. The discussion to follow includes:

- Initiating sources and the potential paths which would lead to sufficient water in the Reactor Building to disable the equipment in elevation 8

- Vulnerability of the equipment if a quantity of water collects in elevation 8 as a function of the height of the postulated flooding.
- Potential alternative sources of coolant makeup and containment heat removal if a disabling release of water into elevation 8 should occur
- Quantification of the event trees describing the frequency of unacceptable conditions for each unique water source and pathway to elevation 8 accounting for both automatic and operator action in response to the postulated flood.

Appendix A provides additional details on the elevation 8 evaluation.

1.1 Initiating Sources

The likelihood of an initiator can be derived by examining the potential water sources involved and the possible paths available to lead to the release of water into elevation 8. Table 1 lists the sources and quantity of water each contains. Of these sources only the CST, suppression pool, and the service water system can supply water for maintenance induced floods.

Table 1

SUMMARY OF POTENTIAL WATER SOURCES WHICH MAY
RELEASE EXCESSIVE WATER IN REACTOR BUILDING

SOURCE	QUANTITY (Gallons)
Suppression Pool	160,000*
Condensate Storage	550,000
Reactor Primary System**	a) 42,928 b) 152,928
Screenwell (Long Island Sound)	Unlimited

* Total water volume in the suppression pool at the high water level mark is 608,500 gallons.

**Figure "a" includes water from the bottom of the core to the normal water level in the RPV. Figure "b" includes "a" plus condenser hotwell water.

1.2 Vulnerability of Equipment

If large quantities of water are introduced into elevation 8, important equipment may become inoperable. Some of the principal equipment in the elevation 8 compartment includes the following:

- HPCI Pump and Electrical Panels
- RCIC Pump and Electrical Panels
- Core Spray Pumps and Electrical Panels

- LPCI Pumps and Electrical Panels
- RHR Heat Exchangers
- Recirc Pump MG-Set Fluid Coupler Cooling Water Pump Motor Control Centers

Each piece of equipment has different vulnerability aspects. Some equipment such as heat exchangers and tanks are not judged to be adversely affected under any water-related condition. However, most pumps, turbines, and electrical panels are assumed to be disabled if water comes in contact with any electrical feature on the equipment. No credit is assumed for low conductivity water sources such as CST in which electrical shorting is less likely to occur.

The combined capacity of the elevation 8 sump pumps is 640 gpm. The quantity of water and related flow rates given in Appendix A indicate that the sump pumps are not adequate to prevent excessive water collection in elevation 8 for certain unlikely sequences of events. The calculated height of water collection in elevation 8 is found to be higher than the above principal equipment in some scenarios; therefore, resulting in disabling the ECCS equipment cited above (see Table 2).

The following pumps or systems are available to provide coolant injection to the reactor vessel in the event that the ECCS equipment on elevation 8 are disabled:

Table 2

SUMMARY OF VITAL EQUIPMENT ASSOCIATED WITH SAFETY SYSTEMS
 LOCATED IN THE ELEVATION 8 COMPARTMENT AND THE POSTULATED
 HEIGHT AT WHICH VITAL EQUIPMENT COULD BE DI-SABLED

SYSTEM	ASSOCIATED VITAL EQUIPMENT	MINIMUM POSTULATED DISABLED HEIGHT (NOTE 2)	SYSTEM FAILURE MODE
HPCI	HPCI INST. (1E41*PS023A-D)	1' - 10"	HPCI ISOLATION
RCIC	RCIC INST. (1E51*PS026A, B)	2' - 0"	RCIC ISOLATION
LPCI	RHR INST. RACK A, B (1E11*PDS001A, B)	3' - 10"	RHR LOGIC DI-SABLED
CORE SPRAY	CORE SPRAY INST. RACK A, B (1E21*PDS033A, B)	3' - 10"	INJECTION VALVE CLOSURE
RECIRC PUMPS (MG-Set)	MOTOR CONTROL CENTERS (11D1, 12D1)	1' - 6"	COOLING WATER PUM TRIP FOR FLUID COUPLER (NOTE 1)
CONDENSATE	NONE	NONE	NONE

NOTE 1: Due to oil heatup, trip of recirculation pump MG-SET is calculated to occur in approximately 7.5 minutes following loss of MCC. Emergency procedures require initiation of Emergency Shutdown on loss of cooling water indication in control room.

NOTE 2: Based on physical survey of electric component position and postulated electrical shorting effects.

1. High pressure

- Feedwater
- Control Rod drive
- Stand by Liquid Control

2. Low Pressure

- Condensate
- Condensate Transfer Pumps*
- Service Water Pumps*
- Diesel Fire Pump*

*Treated in the Containment Event Trees

Each of these pumps are considered in the evaluation of the coolant injection function; however, some of the cited alternatives have a relatively small effect on the calculated reliability of coolant injection.

For postulated floods during normal or accident conditions, Shoreham has a redundant level alarm system, powered by emergency supplies, at elevation 8 in the reactor building secondary containment. The main purpose of this alarm system is to provide indication in the main

control room of any unacceptable water buildup at elevation 8. This alarm system is not the only means to provide a warning of a potential flood problem since alternate instrumentation and continuous running of the sump pumps (indicated by a light in the control room) would also provide indication of excessive leakage. The sump pumps and their associated alarm system are powered from normal power buses.

1.4 Quantification of Event Tree Sequences Following A Release of Excessive Water into the Reactor Building

This section provides the event trees used to quantify the frequency of events leading to core vulnerable states resulting from a release of water into elevation 8. The event trees portray the sequences of events following a major maintenance action on a safety system requiring system disassembly while the plant is at power.

Two sets of event trees are constructed to reflect the pathways to postulated core vulnerable conditions from each of the above. The two sets of event trees referred to here and the role that each of these two play in the assessment process is as follows:

- Initiator event trees: Using a major maintenance act as the starting point, subsequent operator actions are accounted for in the determination of the potential course of the accident.

These initiator event trees are used to sort out similar plant conditions, entry condition states (regardless of how the plant reached that state), so that these entry states can be used to enter the systemic event trees.

- Systemic event trees: Using the entry condition states and frequencies determined from the initiator event trees, the systemic event trees are then used to determine the likelihood of particular plant response paths for similar entry condition states. The quantification of successful core cooling and containment heat removal is performed for each initiator type using the same event tree structure repeated for each of the entry states.

In summary, the quantification of the postulated flooding sequences which could result in core vulnerable conditions takes place in two steps: (1) the initiator event trees are used to sort out operator action and plant state, and the results summarized by collecting similar plant conditions together for entry into the second groups of event trees; (2) the system event tree are then used to quantify the plant response for the predisposed entry states determined in the initiator event trees.

1.3.1 Initiator Event Trees

The initiator considered in the structuring of the event trees is a major maintenance act which requires exposing safety system to the Reactor Building atmosphere.

These initiator event trees are each addressed separately with a short discussion of the considerations used in quantifying the functional events in each event tree type. The initiator event trees are formulated to discretize the continuum of potential end states possible in postulated flooding events. These discrete states are then lumped together in manageable groupings based upon similar effects on plant systems. Following the discussion and quantification of individual initiator event trees, the results are summarized in a matrix format. The calculated frequencies from the initiator event trees are collected together into similar bins within the matrix which are then used as entry condition states for the systemic event trees.

It should be noted that within the initiator event trees are a number of automatic and manual actions. The characterization of operator response under the postulated flooding conditions is crucial to the quantification. As has been noted elsewhere in this PRA and in the open literature, the quantification of operator action is subject to relatively large uncertainties. The operator response model used to

quantify operator action following postulated internal flood sequences assumes that the Shoreham operators and shift supervisors are thoroughly trained in the procedure to be used in the event of a high water level alarm in the Reactor Building.

The end points of the initiator event trees are the entry condition states for the systemic event trees. The critical height used in this analysis is 3'-10", all ECCS systems are assumed to be disabled if the flood is not isolated before this height is reached. There are four principal entry condition states derived from the potential flood initiators; these are the following:

The four principal reactor plant states are determined by the source of water, either the CST (C), or other (O) (suppression pool, service water); and by the reactor status, either a manually initiated controlled shutdown (T), or an automatic trip from high power resulting in an MSIV closure (S). The four events are designated as follows:

T-C: A flood resulting in the loss of inventory from the CST, combined with a controlled shutdown (turbine trip) of the reactor according to emergency procedures.

T-O: A flood resulting from loss of inventory from other sources (suppression pool, service water), combined with a

controlled shutdown (turbine trip) of the reactor according to emergency procedures.

S-C: A flood resulting in the loss of inventory from the CST, combined with an MSIV closure that results in loss of feedwater.

S-O: A flood resulting from loss of inventory from other sources, combined with an MSIV closure that results in loss of feedwater.

The following discussion focuses on the description and quantification of the initiator event trees.

INITIATOR EVENT TREE: Major Maintenance Actions

One mechanism for the release of water into the Reactor Building is due to a combination of major maintenance on a system in the Reactor Building, coupled with an event that provides a flow path to the Reactor Building from a large water source. This subsection provides the event tree quantification for the following maintenance initiator event tree types:

(1) RCIC

(2) HPCI

- (3) Core Spray
- (4) LPCI
- (5) Service Water

The maintenance initiator event trees for these systems are presented in Figures 2 through 6. The following brief discussion of the functional events is provided for the understanding of the postulated sequences and their quantification. Additional details are presented in Appendix A.

INITIATING FREQUENCY Major Maintenance ($T_{FL1}-T_{FL5}$): Rare cases occur during reactor power operation when a safety system may require major maintenance. Here, major maintenance refers to those actions which would require disassembly of system components eliminating one barrier between large sources of water and the Reactor Building. The calculation of the frequency of such major maintenance actions is done for each system and is presented in Appendix A.

PROCEDURE (P): According to Shoreham procedures during maintenance actions the operator is required to remove power from the valves which isolate the maintenance items from potential water sources. Failure to remove power from the isolation valves could result in either automatic opening on an accident challenge (D) or accidental manual opening from the control room (E_C).

Local opening of the isolation valves (from the motor control center (MCC) or local manual) is judged to be negligible since there is no convenient way for the operator to de-isolate the system.

DEMAND (D): In the unlikely event that the operator fails to follow the maintenance procedure and remove power from the isolation valves, there is a possibility that a transient challenge for safe shutdown may occur during the major maintenance outage which also results in an automatic challenge to opening the system valves. The probability of the demand includes the automatic or manual action to open the isolation valves.

SOURCE (S): For some systems there is a possibility that suction can be taken from either the CST or the suppression pool. This branch point is an artifice used to distinguish these features for use in sorting the potential sequences.

OPERATOR MAINTAINS ISOLATION (E_C & E_L): Even with no real challenge for the safety system there is some small probability that an operator error may occur during major on-line maintenance which would result in inadvertent opening of the isolation valves.

FLOOD ANNUNCIATION (I): Control room annunciation of the fact that excessive water is present in the Reactor Building is based strictly on the estimated reliability of the water level instrumentation system.

OPERATION ACTION (A): The operator's ability to isolate the source of the water release into the elevation 8 is based upon an operator response model discussed in detail in Appendix A. This is a time-dependent function and is evaluated at the time for which operator response would prevent extensive environmental stress on the safety system operation, a flooding to a 3'-10" depth.

PLANT/REACTOR STATUS (R): Since the primary method of coolant injection and containment heat removal is the use of the power conversion system, the status of the power conversion system is a key parameter in assessing the mitigating capability of the plant given a flood induced in elevation 8. As described in Appendix A a value of 0.3 conservatively bounds the possibility of the flood inducing a transient condition in the reactor which results in a MSIV closure event (S).

INITIATOR EVENT TREE: Summary

One of the principal functions of the initiator event trees is to sort out similar sequences, collect them together, and then be able to evaluate the system response to these similar preconditioned events in the systemic event trees. As discussed above, "Entry Condition States" developed by examining the various types of potential flood initiators result in a matrix of plant states which are then combined and used as initiators in the systemic event trees in order to define the probability and distribution of potential core vulnerable states.

The five initiator event trees presented here have been quantified using the data and models of the event functions developed in Appendix A. The results are compiled in Table 3 according to the 4 possible discrete entry states discussed earlier.

Table 3

INITIATOR EVENT TREE SUMMARY FOR
 MAINTENANCE-INDUCED POSTULATE ACCIDENT SEQUENCES
 INVOLVING REACTOR BUILDING FLOODING

INITIATOR	DESIGNATOR	SEQUENCE TYPE				CORE VULNERABLE FREQUENCY PER REACTOR YEAR	
		T-C	T-O	S-C	S-O	CLASS I	CLASS II
RCIC in major maintenance	T _{FL1}	1.8E-8	1.8E-8	4.3E-8	7.7E-9	6.5E-9	9.5E-10
HPCI in major maintenance	T _{FL2}	5.5E-6	7.1E-7	5.4E-6	3.0E-7	7.5E-7	1.2E-7
CS in major maintenance	T _{FL3}	---	2.9E-8	---	1.2E-6	1.3E-7	1.8E-8
LPCI in major maintenance	T _{FL4}	---	5.6E-7	---	4.0E-6	4.4E-7	6.0E-8
RHR Heat Exchanger in major mainten- ance	T _{FL5}	---	3.6E-9	---	6.8E-9	7.6E-10	1.2E-10
Σ	--	5.5E-6	1.4E-6	5.4E-6	5.6E-6	1.3E-6	2.0E-7

Next, the processing of these frequencies through the Shoreham specific systemic event trees is performed.

1.3.2 Systemic Event Trees

Given the entry conditions derived from the above discussion, the systemic event trees are formulated to assess the likelihood of the progression of flooding accident sequence to core vulnerable conditions. The system event tree format is the same as that used in Section 3 of the Shoreham draft PRA.

Figures 7 through 10 are the systemic event trees which summarize the quantification of end states (frequency of core vulnerable Classes) resulting from manual turbine trips or MSIV closures.

The quantification of the conditional probabilities of system availability takes into account the plant status, the system environmental stress, the availability of water sources, and the systems involved in the initiator.

The functional event descriptions are similar to those presented earlier in Section 3. This section discusses any significant differences from the previous description emphasizing functional, spatial, and environmental dependencies induced by the postulated accident sequences.

INITIATOR (S,T): Table 3 summarizes the initiating frequencies which are determined via the initiator event trees and which are used to enter the systemic event trees.

SCRAM (C): See discussion for manual shutdown, turbine trip, and MSIV closure presented in Sections 3.4.1, 3.4.2, and 3.4.3, of the PRA. The principal difference in the system event trees presented here is that all failures to insert the control rods are treated as leading directly to a Class IV core vulnerable event. No credit is given for ATWS mitigation using the feedwater system and SLC. Note that the benefit from ARI and RPT in reducing common mode electrical failures has been accounted for in the choice of the conditional probabilities of scram system failure; that is, the reactor scram function is approximated for these cases to be only those mechanical common mode failures which may inhibit control rod insertion, since electrical common mode failures are approximately two orders of magnitude less likely due to the implementation of ARI and RPT design changes at Shoreham.

PRESSURE CONTROL (M,P): See the discussion of these events in Sections 3.4.1, 3.4.2, and 3.4.3.

FEEDWATER (Q): The availability of feedwater is preconditioned on the status of the plant. For MSIV closure events, virtually

no credit is given for feedwater as a useful coolant injection source within 30 minutes*. For operator induced turbine trip events, feedwater unavailability is calculated to be relatively low; this is based upon licensing basis analysis which indicates a small potential for feedwater trip and subsequent MSIV closure. Shoreham startup tests may show that this characterization is overly conservative and needs to be modified to more accurately assess the plant response under these conditions.

HIGH PRESSURE COOLANT INJECTION RCIC (U') and HPCI (U''): The response of HPCI and RCIC is directly affected by the postulated conditions of excessive water in the reactor building. Since control instrumentation for both systems is located at approximately the 2 foot level it is found that the postulated flooding sequences could compromise HPCI operability. Therefore, for unisolated floods HPCI is assigned a failure probability of 1.0. Similarly, RCIC has components which could be disabled by the postulated massive flooding reached the 2 foot height.

*Time available for feedwater to be restored may actually be longer for some identified flooding sequences, but no credit is taken for this additional time for operator action to reopen the MSIVs. This is judged to be a conservatism in the analysis. Shoreham emergency procedures provide instructions for re-opening MSIV's.

LOW PRESSURE COOLANT INJECTION (V): The release of excessive water into the reactor building results in two effects which can adversely impact the LPCI and CS pumps:

- (1) The water can create unacceptable environmental stress on the electrical connections for the pumps at the 3' 10" level..
- (2) The water source could be the suppression pool in which case the CS and LPCI pumps would cavitate due to loss of suction at approximately the same level as item (1).

In all of the low probability flooding accident sequences analyzed, the LPCI and CS pumps were assumed to be disabled due to one of the above causes.

The remaining low pressure system is the condensate system which is normally operating.

Event X Timely Reactor Depressurization: In the instance when the operator loses feedwater, depressurization is required. The primary contributor to the probability of Event X is the probability of the recognition by the operations team that they require the condensate system. This recognition is considered to be a cognitive task which has been conservatively assumed to be

required within 30 minutes minus the time required for depressurization. Since the depressurization time can be considered negligible, the probability of this event would be given by Table A-10 as 0.01. Since this table provides the probability of operator response to a secondary event, it could be argued that this is too conservative because the occurrence of the flood event would make the operations team aware of the necessity to depressurize if feedwater is unavailable. However, it could also be argued that with alarms present the decision-making may be made in a stressful atmosphere. Since the effects of stress differ depending on the level of training, to be conservative it is assumed that the event occurs within the first six months of operation and so the operators would be considered to be novices.

Since extremely high stress is reserved for life-threatening emergency situations (which is not the case here) moderately high stress is assumed in the performance of a dynamic task. In this case, the assigned probability should be increased by an order of magnitude as required by Table 20-23, Section 2, Item 3B on page 20-32 of NUREG/CR-1278. This would place the assigned probability at $10 \times 0.01 = 0.1$. This number would correspond to the extreme of the conservative error bounds assigned to the response of a cognitive task within 30 minutes from NUREG/CR-2815(G-14), and so is very conservative.

CONDENSATE: As for the case of CS and LPCI, the condensate pumps can be used for low pressure coolant makeup given that the reactor can be depressurized. The condensate system has a separate water source, i.e., the condenser hotwell, which affords sufficient water supply to maintain reactor coolant inventory and adequate core cooling. Since the condensate system does not depend on equipment in the elevation 8 compartment of the reactor building, the release of water into the reactor building will not adversely affect the use of the condensate system to initially supply coolant makeup to the reactor. Also, since the condensate system is running during operation; there is a high probability that it will continue to run for the duration of the postulated transient. If feedwater becomes unavailable, (e.g. due to MSIV closure) than the condensate system will continue to operate on recirculation to the condenser hotwell. When the reactor primary system pressure is lowered sufficiently, the discharge check valves in the FW/condensate system will open and inject coolant directly into the primary system automatically.

Operator action is required only for the following:

1. Control water level in the reactor.
2. Control flow to the reactor.

3. Minimize flow into the containment.

Under the isolation conditions there would not be coolant makeup from the reactor to the hotwell and makeup must come from the following within approximately 4 to 6 hours at decay heat levels:

- (1) Condensate transfer pumps from the CST to the hotwell. Since this is a normal operation it is judged to have a relatively high success rate.
- (2) Reopening the MSIVs or aligning alternate makeup paths to the condenser hotwell. In the event of the unavailability of water from the CST, operator action under stress may be required. For cases where hardware availability may also be in question, a low success rate is assigned to the operator response.

It is judged that the condensate system has a high conditional probability of success under these circumstances. A conservative estimate has been made to characterize the condensate system availability over short term and the extended period of recovery.*

CONTAINMENT HEAT REMOVAL: This event function is the same as discussed in Sections 3.4.1, 3.4.2 and 3.4.3 of draft PRA.

The availability to remove decay heat from containment needs to be established in order to ensure long term containment integrity. The principal means of removing heat from the containment and their limitations are as follows:

- RHR and RCIC in the Steam Condensing Mode: Essential components of these systems are located in elevation 8 of the reactor building. Therefore, adverse environmental stress in elevation 8 is assumed to compromise the long term heat removal capability of these systems.
- Power Conversion System: The normal heat removal path through the main condenser is not affected by the environmental effects in elevation 8 as long as the MSIVs can be maintained open. In any event, if the water level in the core can be restored, the MSIVs can be reopened per emergency operating procedure.

*The draft Shoreham PRA fault tree had assumed that use of the condensate system for injection to the reactor required a manual alignment of the system utilizing the startup bypass line around the feed pumps. A re-evaluation indicated that injection directly through the feed pumps was feasible without re-alignment.

1.4 Summary of the Probabilistic Evaluation of the Frequency of Core Vulnerable Conditions Due to Internal Flooding

Table 4 summarizes the results of the systemic event tree quantification for internal flood related sequences. The results are presented as a summation of the frequencies of various similar end states (i.e., core vulnerable) from the system event trees by accident class. The two classes to which internal floods contribute are summarized by the entry condition derived from the initiator event trees, i.e., turbine trips, or isolation events.

An examination of the dominant contributors to core vulnerable frequency from postulated internal flooding sequences indicates that isolation events involving releases of water to the reactor building through the HPCI, LPCI or CS are the primary contributors.

Table 4

SUMMARY OF RESULTS OF EVENT TREE
 QUANTIFICATION FOR MAINTENANCE-INDUCED
 INTERNAL FLOOD RELATED SEQUENCES IN TERMS
 OF CORE VULNERABLE FREQUENCY

Initiator Event Tree States	Class I Loss of Coolant Makeup	Class II Loss of Containment Heat Removal
Turbine Trips:		
T-C	1.4E-8	2.9E-8
T-O	3.1E-9	7.4E-9
MSIV Closures:		
S-C	7.0E-7	8.1E-8
S-O	6.2E-7	8.4E-8
TOTAL:	1.3E-6	2.0E-7
% of Total Core Vulnerable:	2.6%	.4%

In order to place the postulated flooding sequences in perspective, it should be recognized that:

- Large internal floods are unlikely.
- Safety grade level instrumentation alarms in the control room alert the operator to the potential hazard.
- The operator can isolate the identified flood sequences from the control room.
- Safe shutdown can be performed with equipment which is not affected by the postulated flood and which is the principal equipment virtually always used by the operator to reach safe shutdown.

The principal contributors of the identified sequences to risk are in the lower core melt consequence classes (i.e., Class I and Class II). Therefore, the potential public risk does not increase proportionally to the increase in frequency of these accident classes.

The results of the probabilistic analysis of the maintenance-induced internal flood sequences indicate that the calculated frequency of these postulated events taken together represent approximately 3.0%

of the best estimate core vulnerable frequency. Based upon this finding, the sequerces involving postulated large internal floods due to maintenance do not represent risk outliers at Shoreham.

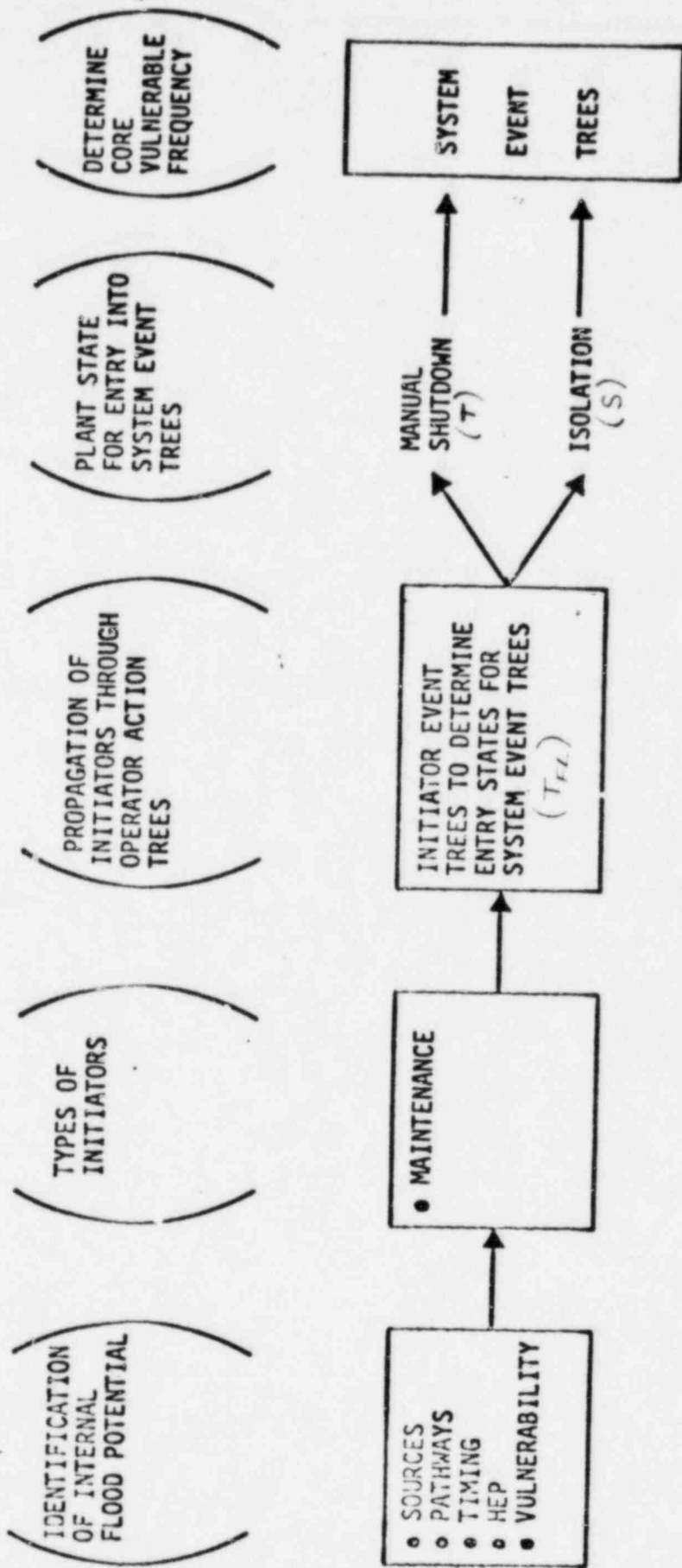
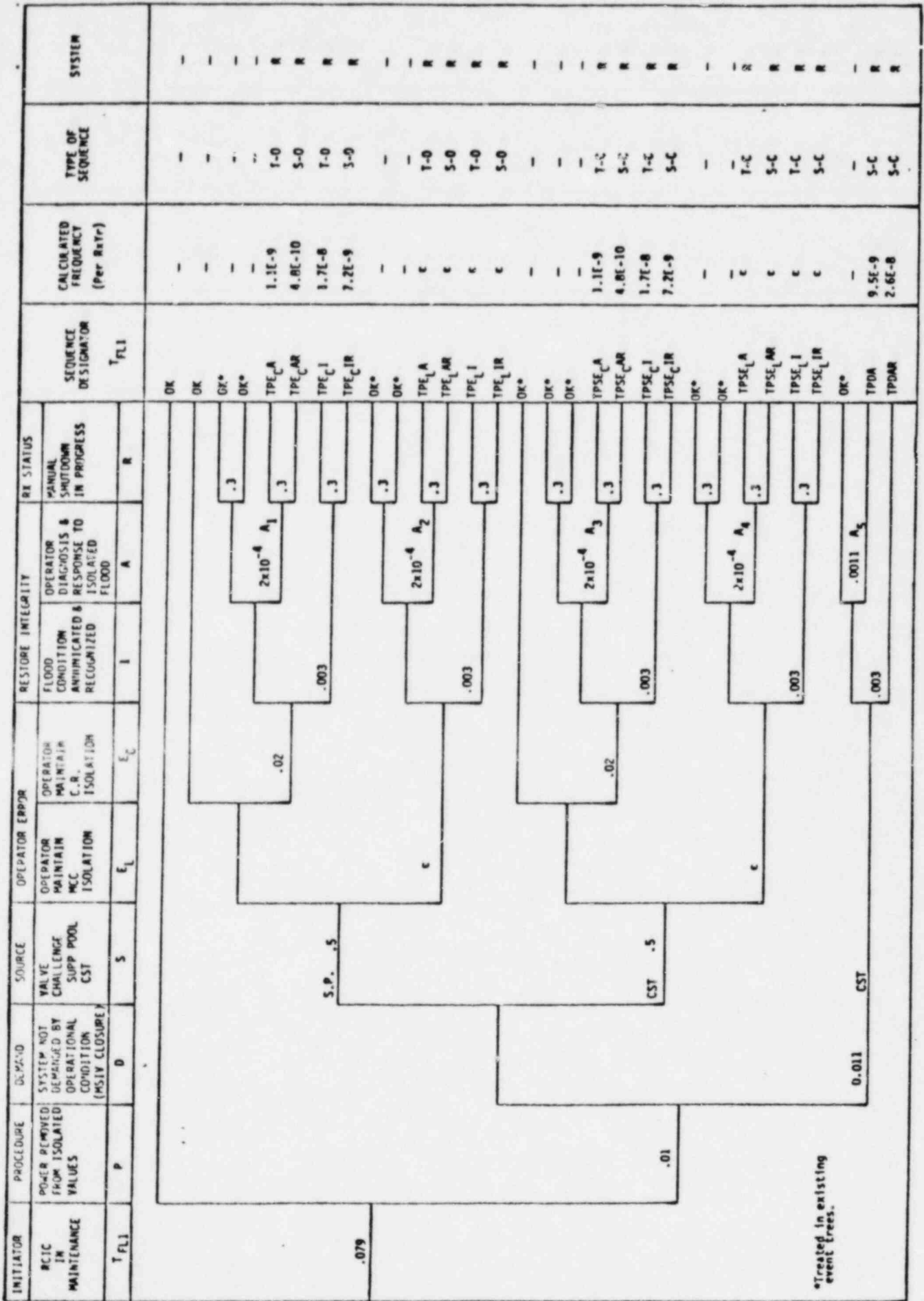


Figure 1 Flow Chart Describing the Progression of initiators from Identification Through Core Vulnerable for Postulated Internal Flood Cases.



*Treated in existing event trees.

Figure 2: T_{FL1}: Initiator Event Tree for Postulated Flooding Sequences Initiated During RCIC Maintenance.

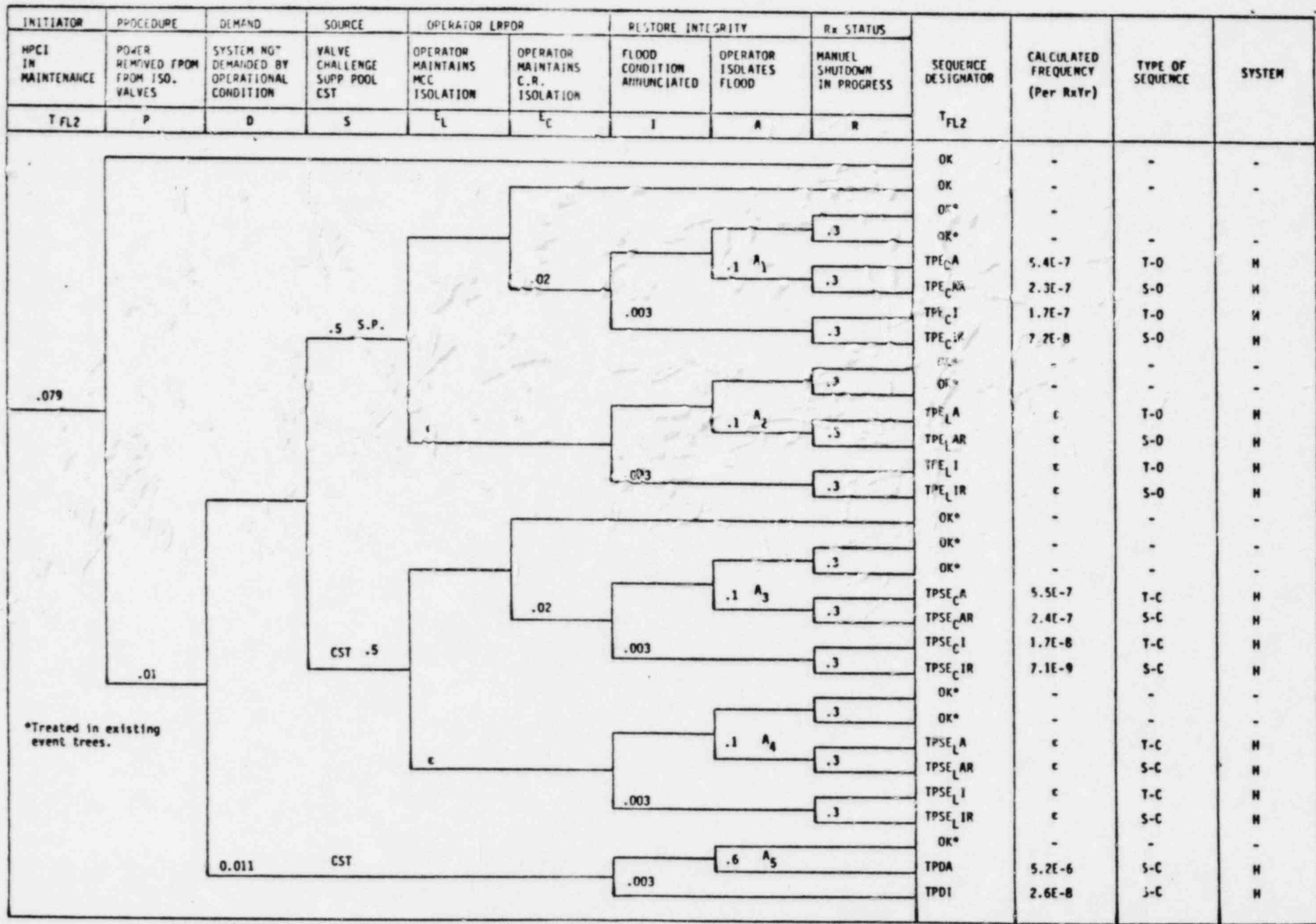


Figure 3: T_{FL2}: Initiator Event Tree for Postulated Flooding Sequences Initiated by an Error During HPCI Major Maintenance.

INITIATOR	PROCEDURE	DEMAND	OPERATOR ERROR		RESTORE INTEGRITY		REACTOR STATUS	SEQUENCE DESIGNATOR	CALCULATED FREQUENCY (Per Rx Yr)	TYPE OF SEQUENCE	SYSTEM
CS IN MAINTENANCE	POWER REMOVED FROM ISOLATION VALVES PER PROCEDURE	SYSTEM NOT DEMANDED BY OPERATIONAL CONDITION	OPERATOR MAINTAINS LOCAL ISOLATION	OPERATOR MAINTAINS CR ISOLATION	FLOOD CONDITION ANNUNCIATED AND RECOGNIZED	OPERATOR DIAGNOSIS AND RESPONSE TO ISOLATED FLOOD	MANUAL SHUTDOWN IN PROGRESS				
T_{FL3}	P	D	E_L	E_C	I	A	R	T_{FL3}			
								OK	-	-	-
								OK	-	-	-
								OK*	-	-	-
								OK*	-	-	-
								$TPE_{C,A}$	$2.8E-8$	T-0	L
								$TPE_{C,AR}$	$1.2E-8$	S-0	L
								$TPE_{C,I}$	$8.4E-10$	T-0	L
								$TPE_{C,IR}$	$3.6E-10$	S-0	L
								OK*	-	-	-
								OK*	-	-	-
								$TPE_{L,A}$	ϵ	T-0	L
								$TPE_{L,AR}$	ϵ	S-0	L
								$TPE_{L,I}$	ϵ	T-0	L
								$TPE_{L,IR}$	ϵ	S-0	L
								OK*	-	-	-
TPDA	$1.2E-6$	S-0	L								
TPDI	$5.8E-9$	S-0	L								

*Treated in existing event trees.

**Includes both CS pumps.

† Manual valve from CST is treated in human error probability section and found to contribute a negligible conditional probability to the potential for unmitigated flooding.

Figure 4: T_{FL3} : Initiator Event Tree for Postulated Flooding Sequences Initiated by an Error During Core Spray Major Maintenance

INITIATOR	PROCEDURE	DEMAND	OPERATOR ERROR		RESTORE INTEGRITY		REACTOR STATUS	SEQUENCE DESIGNATOR	CALCULATED FREQUENCY (Per Rx Yr)	TYPE OF SEQUENCE	SYSTEM
LPCI IN MAINTENANCE	POWER REMOVED FROM ISOLATION VALVES PER PROCEDURE	SYSTEM NOT DEMANDED BY OPERATIONAL CONDITION	OPERATOR MAINTAINS LOCAL ISOLATION	OPERATOR MAINTAINS CR ISOLATION	FLOOD CONDITION ANNUNCIATED AND RECOGNIZED	OPERATOR DIAGNOSIS AND RESPONSE TO ISOLATED FLOOD	MANUAL SHUTDOWN IN PROGRESS				
T _{FL4}	P	D	E _L	E _C	I	A	R	T _{FL4}			
.08 **	P	D	E _L	E _C	I	A	R	OK	-	-	-
								OK	-	-	-
								OK*	-	-	-
								OK*	-	-	-
								TPE _C A	5.6E-7	T-0	L
								TPE _C AR	2.4E-7	S-0	L
								TPE _C I	1.7E-9	T-0	L
								TPE _C IR	7.2E-10	S-0	L
								OK*	-	-	-
								OK*	-	-	-
								TPE _L A	ε	T-0	L
								TPE _L AR	ε	S-0	L
								TPE _L I	ε	T-0	L
								TPE _L IR	ε	S-0	L
								OK*	-	-	-
TPDA	3.0E-6	S-0	L								
TPDI	1.2E-6	S-0	L								

*Treated in existing event trees.
 **Includes four LPCI pumps.

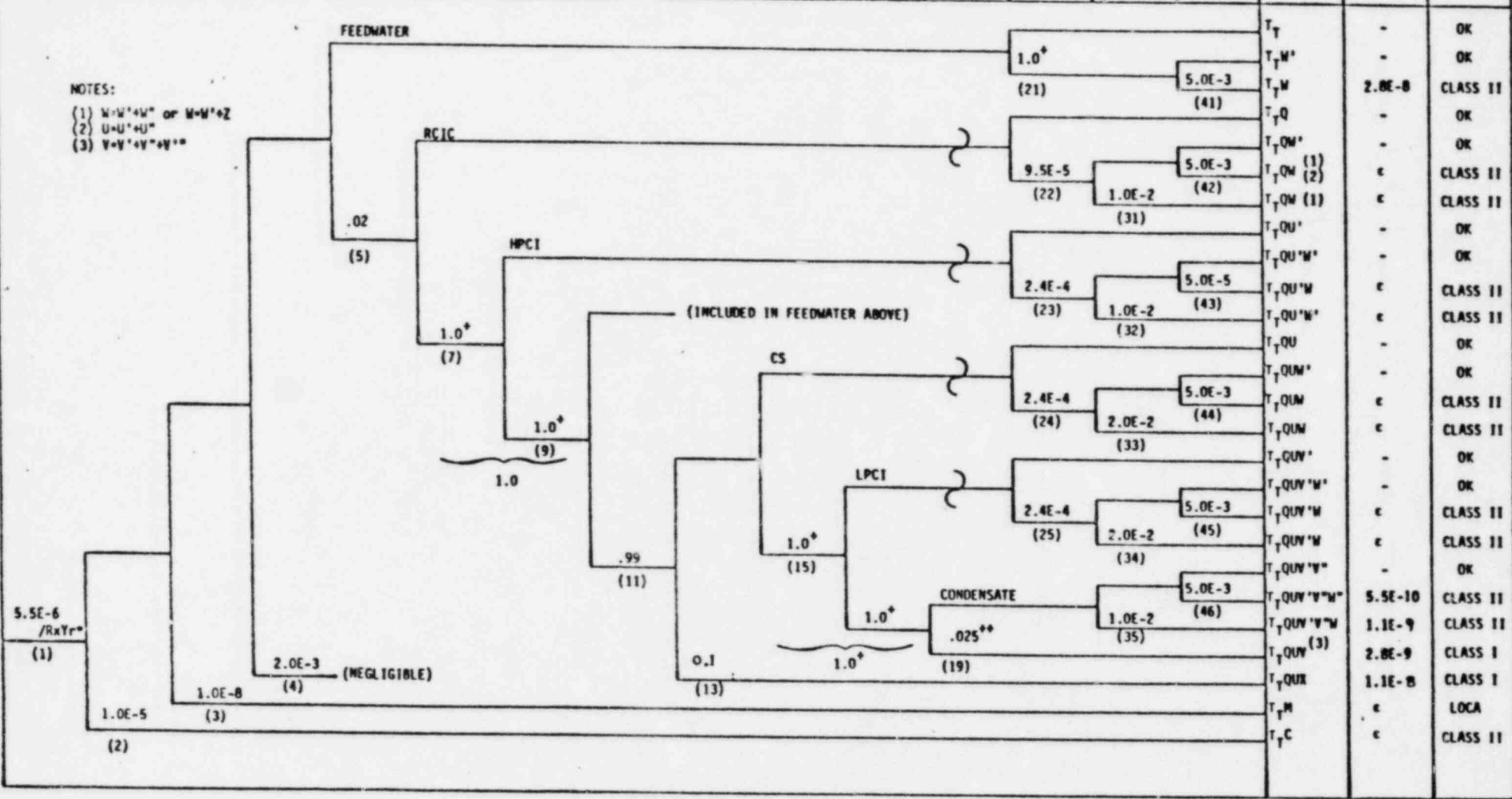
Figure 5: T_{FL4}: Initiator Event Tree for Postulated Flooding Sequences Initiated by an Error During LPCI Major Maintenance.

INITIATOR	PROCEDURE	DEMAND	OPERATOR ERROR		RESTORE INTEGRITY		REACTOR STATUS	SEQUENCE DESIGNATOR	CALCULATED FREQUENCY (Per Rx Yr)	TYPE OF SEQUENCE	SYSTEM
SERVICE WATER IN MAINTENANCE	POWER REMOVED FROM ISOLATION VALVES PER PROCEDURE	SYSTEM NOT DEMANDED BY OPERATIONAL CONDITION	OPERATOR MAINTAINS LOCAL ISOLATION	OPERATOR MAINTAINS CR ISOLATION	FLOOD CONDITION ANNUNCIATED AND RECOGNIZED	OPERATOR DIAGNOSIS AND RESPONSE TO ISOLATED FLOOD	MANUAL SHUTDOWN IN PROGRESS				
T _{FL5}	P	D	E _L	E _C	I	A	R	T _{FL5}			
								OK	-	-	-
								OK	-	-	-
								OK*	-	-	-
								OK*	-	-	-
								TPE _C A	2.8E-9	T-0	0
								TPE _C AR	1.2E-9	S-0	0
								TPE _C I	1.2E-9	T-0	0
								TPE _C IR	1.2E-9	S-0	0
								OK*	-	-	-
								OK*	-	-	-
								TPE _L A	ε	T-0	0
								TPE _L AR	ε	S-0	0
								TPE _L I	ε	T-0	0
								TPE _L IR	ε	S-0	0
								OK*	-	-	-
TPA	4.0E-9	S-0	0								
TPAI	1.2E-9	S-0	0								

*Included in existing event trees.
 **Includes both service water loops.

Figure 6: T_{FL5}: Initiator Event Tree for Postulated Flooding Sequences Initiated by an Error During Service Water Major Maintenance (i.e., Heat Exchangers)

INITIATOR T-C OPERATOR TRIPS TURBINE CST-SOURCE	CRITICALITY SCRAM	PRESSURE CONTROL		COOLANT INJECTION								CONTAINMENT HEAT REMOVAL			SEQUENCE DESIGNATOR	CALCULATED FREQUENCY (Per Kx Yr)	CLASS OF POSTULATED CORE DAMAGEABLE OR TRANSFER
		S/R VALVES OPEN	S/R VALVES RECLOSED	FEEDWATER	RCIC AVAILABLE	HPCI AVAILABLE	MSIV REOPENED AND FEEDWATER RECOVERED	TIMELY REACTOR DEPRES- SURIZATION	CS AVAILABLE	LPCI AVAILABLE	CONDENSATE PUMP INJECTION AVAILABLE	RHR OR RCIC IN STEAM CONL PLUS SW	MSIV REOPENED >10 HRS	PCS			
T	C	M	P	Q	U'	U''	Q	X	V'	V''	V'''	H'	Z	W''			



*Includes contribution due to control rod withdrawal.
 †In maintenance or flooded
 †† Requires the supply of makeup to the hotwell within approximately 5 hours by opening MSIV's or an alternate source (i.e., CST is unavailable)

Figure 7: System Event Tree for Turbine Trips with Greater Than 3' 10" of Water in the Reactor Building (Source = CST).

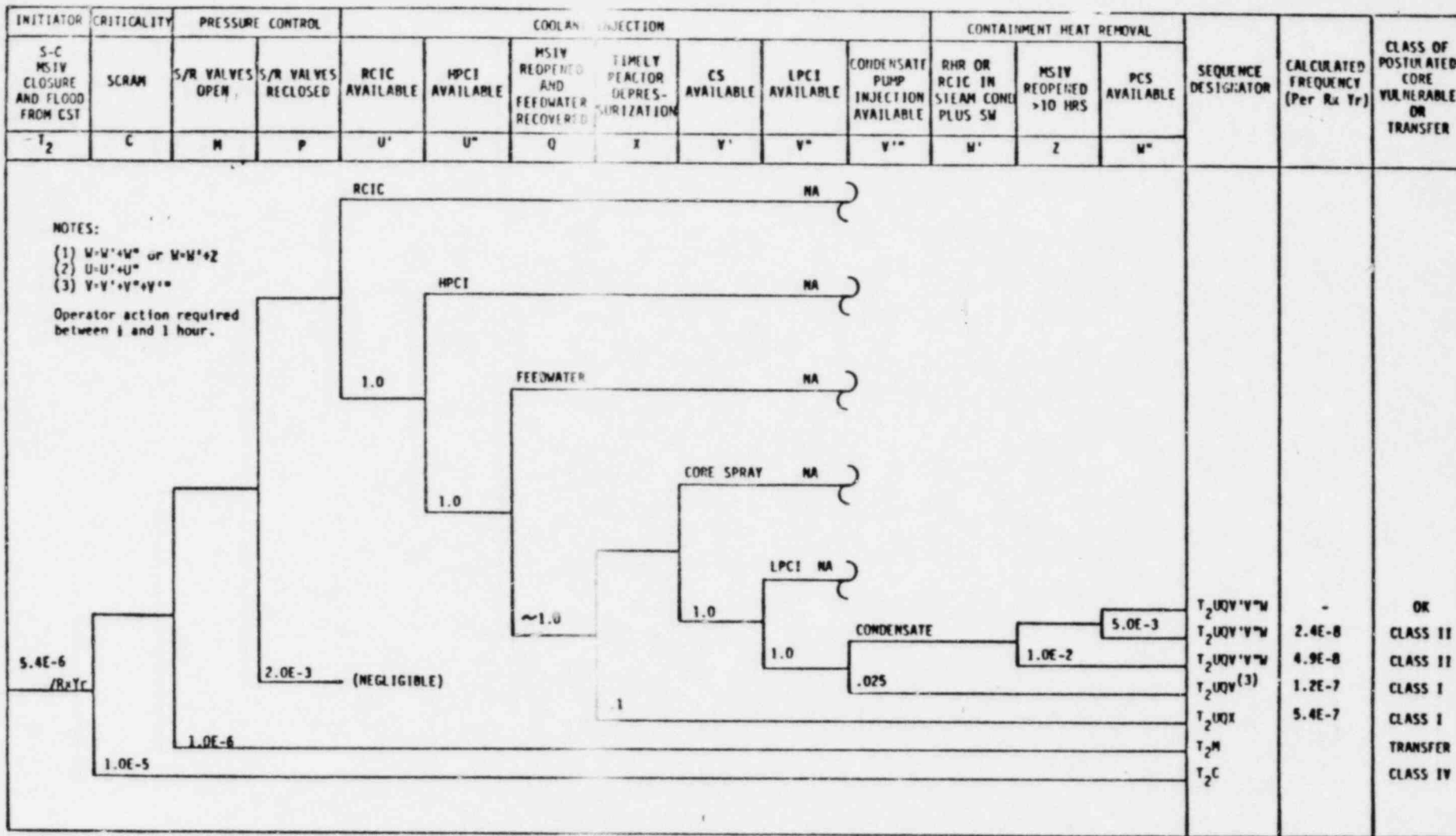
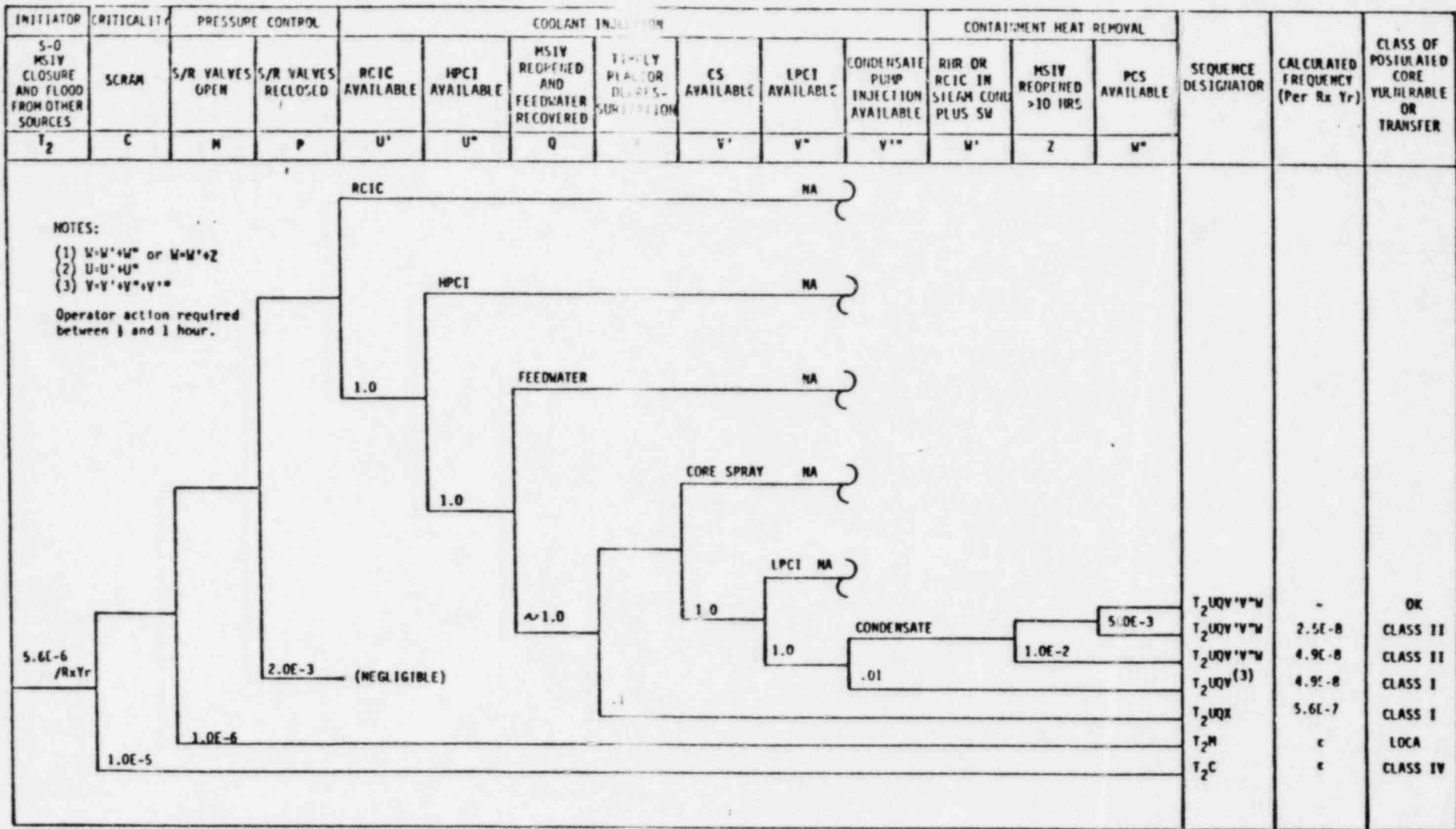


Figure 9: System Event Trees for MSIV Closure Cases with an Accumulation of Greater Than 3' 10" of Water in the Reactor Building (Source = CST via HPCI or RCIC).



* Requires supply of makeup to the hotwell within approximately 5 hours by opening MSIV's or insertion from alternate source (i.e., CST is unavailable)

Figure 10: System Event Tree for MSIV Closure Cases with an Accumulation of Greater Than 3' 10" of Water in the Reactor Building (Source = other than CST).

APPENDIX A

RELEASE OF WATER INTO ELEVATION 8 OF THE REACTOR BUILDING

APPENDIX A

RELEASE OF WATER INTO ELEVATION 8 OF THE REACTOR BUILDING

The Shoreham Reactor Building surrounds the Mark II containment structure. At its lowest elevation (referred to here as elevation 8), the building is an open cylindrical compartment: i.e., there are no barriers in the elevation 8 compartment, which would interfere with personnel access or room ventilation. However, this open area presents the possibility of adversely affecting the equipment in elevation 8, if excessive water were released into the compartment.

A release of water into elevation 8 of the Reactor Building, greater than the sump capacity, is not anticipated to occur during the life of the Shoreham plant. Nevertheless, sources of water exist which have the potential to overflow the sump capacity if one or more potential initiator types (defined as initiator types) are examined that have this potential, regardless of how small the probability of a release. The frequency of these potential initiator types are developed in this appendix. This frequency is used in Section 1.4 as the initiator for a set of the event trees which are used to evaluate the potential accident sequence outcomes from these initiators. Further, the following aspects of the evaluation of elevation 8 regarding the potential release of water into the Reactor Building are discussed:

- Sources of water and available sump pump capacity (Section A.1)
- Pathways of water into elevation 8 and corresponding flow rates (Section A.2).
- Vital system equipment in elevation 8 and vulnerability to high water level (Section A.3)
- Functional event quantification (Section A.4)

The spectrum of event sequences postulated to lead to the release of water into the elevation 8 compartment are evaluated by considering the largest releases possible and conservatively characterizing flow rates and operator response for these large releases.

A.1 SOURCES OF WATER AND AVAILABLE SUMP CAPACITY

As a starting point for determining the likelihood of various reactor building (RB) internal flooding scenarios, the sources and volume of water required to flood the critical RB locations, as well as the capacity of various drainage systems must be considered. These data make it possible to identify water inventories, which, if diverted into these regions such as the RB elevation 8 compartment could result in a flood.

The volume of water for each foot of depth required to flood the reactor building elevation 8 compartment with all equipment and piping installed has been conservatively estimated at 41600 gallons. Drainage systems which would receive the initial volume of flood water include:

- Reactor Building Floor Sumps
- Reactor Building Equipment Sumps
- Reactor Building Porous Concrete Sumps

These systems have sump capacities of 2490 gallons, 1660 gallons, and 500 gallons, respectively for a total sump capacity of 4650 gallons. The sump pump capacities for these systems are 400 gpm (which includes the excess leakage return pump with a capacity of approximately 100 gpm), 200 gpm, and 40 gpm, respectively, for a total sump pump capacity of 640 gpm.

These reactor building sump pumps are available, on the normal AC power buses, to successfully drain and control water leakage within the elevation 8 compartment. If the floor drain sump tank indicators register radioactive materials, the sump pumps will not be activated (pumping water out through the radioactive waste system). In this case, the leak detection pump can be activated manually, to pump leakage into the suppression pool.

A second case for using the leakage return system would be in the event of a loss-of-offsite power. All floor drain sump pumps would become inoperable. The leakage return pump is designed to remain operable under this condition.

For the purposes of this study, failures which produce leakage within the capability of the sump pumps are found to be negligible contributors to the overall frequency of unacceptable releases of water into the elevation 8 compartment. This is due to the relatively high reliability of the sump pump system to effectively mitigate small leaks. Therefore, those failures which will be quantified in this analysis are the spectrum of failures which are large enough to inundate the sump capacity. Since the PRA, of necessity, is an evaluation of discretized accidents rather than a continuum, it is necessary to treat these spectra together. Therefore, a set of conservative assumptions are made to discretize the continuum of possible leaks. These assumptions place all the potential leaks greater than the sump pump capacity in one group, characterizing it with the probability of a large release and the flow rate associated with a large release.

The capacity of these drainage systems and the volume of the elevation 8 compartment require that potential flooding initiators have a large water inventory and a flow path capable of delivering water at a rate greater than 640 gpm. Water sources of this size are summarized in Table A-1. Flow paths are considered in Section A.2.

A.2 INITIATOR TYPES

Based upon information found in Table A-1 defining the sources of water, a pathway investigation has been performed to define the potential failure modes (due to maintenance acts) from these water sources which may lead to the release of water into elevation 8. Table A-2 summarizes the initiator water sources (as evaluated for the Shoreham PRA).

Table A-1

SUMMARY OF POTENTIAL WATER SOURCES WHICH MAY
RELEASE EXCESSIVE WATER IN ELEVATION 8

SOURCE	QUANTITY (GAL.)
SUPPRESSION POOL	160,000*
CST	550,000
SCREEN WELL (Long Island Sound)	UNLIMITED
REACTOR PRIMARY SYSTEM**	a) 42,928 b) 152,928

* Total water volume in suppression pool is 608,500 gallons. However, only a portion of it can be drained through ECCS pump suction piping.

** Figure "a" includes water from the bottom of the core to normal water level in the reactor pressure vessel. Figure "b" includes "a" plus condenser hotwell water.

Table A-2

TYPES OF INITIATORS WHICH MAY LEAD TO THE RELEASE OF WATER INTO
THE ELEVATION 8 COMPARTMENT

Water Source	No. of Lines	Systems Involved	Characterization
SUPPRESSION POOL	8	CS, LPCI, RCIC, HPCI	NON-PRESSURIZED
CST	4	CS, HPCI, RCIC	NON-PRESSURIZED
SCREENWELL/LONG ISLAND SOUND	4	SERVICE WATER	PRESSURIZED (Service Water Discharge)

This section provides estimates of the time available between the initial release of water into the reactor building and when water level of 3 feet and 10 inches is reached for each initiator water source identified in Table A-2. These estimates then form the basis for determining the impact on equipment availability and operator response.

Each initiator has an associated flow rate which, together with the data supplied in Section A.1, determines the time frame for various flood levels.

A.2.1 Suppression Pool Source Initiator

Inadvertent opening of a flow path from the suppression pool to a pump in either the HPCI, RCIC, LPCI or Core Spray systems undergoing major maintenance could allow a portion of the contents of the suppression pool to drain into the reactor building. The calculations of flow rate were conservatively performed to estimate the flow rate from the suppression pool to the reactor building under these postulated conditions. These flow rates were based on the suppression pool water level being maintained at the high water level setpoint. This conservative assumption was made because the rate at which coolant makeup is discharged to the suppression pool cannot be determined for the general case. If there is no coolant discharge to the suppression pool, the suppression pool water level will drop, eventually uncovering the pump suction strainers which are located approximately 5 feet below the high water level mark.

A.2.2 CST Initiator Source

When major maintenance occurs on the pump in either of the HPCI, RCIC, or Core Spray systems, there is a possibility that a flow path to the pump from the condensate storage tank (CST) may be inadvertently opened allowing the contents of the CST to drain into the reactor building. Calculations were performed in order to estimate the flow rate from the CST into the reactor building under these postulated conditions.

A.2.3 Service Water Initiator Source

The RHR and RBCLCW heat exchangers are supplied by service water at flow rates that are high enough to be considered as possible flooding initiators. A maintenance act was assumed to result in design flow rates for each heat exchanger (8000 gpm for the RHR heat exchanger, 6400 gpm for the RBCLCW heat exchanger) leaking into the reactor building.

A.2.4 Summary of Initiator Sources: Flow Rates and Estimated Times to Reach 3'-10" depths

The data from Section A.1 implies that the time frame for a flood will be extended as long as drainage systems remain operable. In this analysis it is assumed that sump pump operation continues until the flood reaches a depth of 1 foot, after which the pumps are

inundated. Therefore the calculations of flood timing were carried out in two steps: below and above 1 foot of depth. The volume of water required to flood the reactor building, then, is 46250 gallons for the first foot of depth and 41600 gallons/foot above that level. The net flow rate into the reactor building is initially 640 gpm lower than the flow rate due to the initiator to account for sump pump operation. The results of this analysis for each initiator source and system are summarized in Table A-3.

Table A-3

SUMMARY OF INTERNAL FLOODING INITIATOR TYPES:
FLOW RATES AND FLOOD # TIMING

INITIATOR SOURCE	LOCATION	FLOW RATE gpm	ELEVATION 8 FLOODING TIME, MINUTES*
			3'-10" Depth
Suppression Pool	HPCI Pump Suction	9,600	17
	RCIC Pump Suction	1,500	110
	LPCI Pump Suction	17,000	9.4
	Core Spray Pump Suction	13,000	12
CST	HPCI Pump Suction	12,000	13
	RCIC Pump Suction	2,100	76
	Core Spray Pump Suction	12,000	13
Service Water	RHR Heat Exchanger	8,000	25

* These flood times were calculated based on a failure of the sump pumps to successfully operate, and a 41,600 gallons per foot of depth in the reactor building.

A.3 VULNERABILITY OF EQUIPMENT

The vulnerability of vital equipment with a potential to be disabled, by contact with water is assumed to be correlated to the height of potential flood level in the Elevation 8 compartment.

The quantity of water required to flood the elevation 8 compartment to various heights is tabulated in Table A-4 for a bare compartment, and for the compartment with all identified equipment and piping installed. Note that a 25% margin in equipment volume has been added to ensure that unidentified additional equipment will not invalidate this evaluation. The conclusions are relatively insensitive to the assumption including a 25% equipment margin.

Table A-4

HEIGHT OF WATER IN THE ELEVATION 8 COMPARTMENT VERSUS THE QUANTITY OF WATER REQUIRED TO ATTAIN THAT LEVEL

Water Height (Ft)	Calculated Quantity of Water (Gal) w/o Equipment	Conservative* Estimate
1	52,843	41,600
5	264,215	208,000
10	528,430	416,000

* Assumes 25% equipment volume.

Table A-5 lists the equipment in Elevation 8 and identifies the ECCS equipment.

Each piece of equipment has different vulnerability aspects. Some equipment, such as heat exchangers and tanks, are not judged to be adversely affected under the postulated high water level conditions. However, most pumps, turbines, electrical panels, and terminal box connections are assumed to be disabled if water comes in contact with any electrical features on the equipment.

For each piece of equipment the water level height, at which equipment may be subjected to adverse environmental stress, is an essential factor. The last column of Table A-5 gives the estimated height at which each individual piece is assumed to be disabled with a high probability, due to water coming in contact with essential controls or electrical components. The importance of the equipment's vulnerability is only a factor as it relates to the particular system it supports. The primary systems affected by water released into elevation 8 are the ECCS systems: HPCI, RCIC, LPCI and Core Spray (all of which have vital equipment at elevation 8). Table A-6 identifies the vital equipment, which if disabled, will disable the system it supports. Also listed in the last column are the heights of water that disable the equipment.

In the Shoreham analysis the critical flood level which is considered for reliable operation of ECCS equipment in the elevation 8

compartment is 3'-10". This level is chosen based upon the vulnerability of all ECCS equipment at this level, lower flood levels have been evaluated and shown not be significant contributors.

A.4 FUNCTIONAL EVENT QUANTIFICATION

The use of initiator event trees to sort out and bin similar plant states is the same as the concept used in WASH-1400 to limit the number of in-plant consequence calculations that were required. For the Shoreham analysis the initiator event trees are composed of five types. These types of event trees are derived directly from a knowledge of the initiator sources, the systems involved, and the type of postulated failure (i.e., maintenance coupled with an operator error).

Quantification of the functional events appearing in the event trees is performed in this section. Events that have identical derivations are grouped together. This section has been divided into subsections that correspond to similar portions of the initiator event trees as follows:

<u>Section</u>	<u>Functional Events</u>
A.4.1	Initiators due to Loss of System Integrity resulting from maintenance actions

Table A-5

MAJOR ELEVATION 8 EQUIPMENT LIST

EQUIP. TYPE	EQUIPMENT DESCRIPTION	PART NO.	POSTULATED DISABLED HEIGHT ¹ / ₂
PUMPS	FLOOR DRAIN SUMP PUMPS	1G11*P-035A-D 1G11*P-036A-F	1' - 0"
	DRY FLOOR DRAIN TANK PUMPS	1G11*P-161A,B	1' - 0"
	RADWASTE EQPT DRAIN SUMP & PUMP TO POROUS	1G11*P-224A,B	1' - 1"
**	HPCI PUMP	1E41*P-016	-----
	HPCI VAC PUMP	1E41*P-075	1' - 0"
	HPCI CON. PUMP	1E41*P-076	1' - 0"
**	RCIC PUMP	1E51*P-015	-----
	RCIC VAC PUMP	1E51*P-076	1' - 0"
	RCIC CON. PUMP	1E51*P-077	1' - 0"
**	RHR PUMP MOTORS	1E11*P-014A-D	5' - 4"
	LEAKAGE RETURN PUMP	G11-*P-270	3' - 9"
**	CORE SPRAY LOOP LEVEL PUMPS	1E21*P-049A,B	1' - 3"
**	CORE SPRAY PUMP MOTORS	1E21*P-013A,B	4' - 9"
	DRYWELL EQIP. DRAIN TANK PUMPS	1G11*P-0332A,B	1' - 2"
	RCIC LOOP LEVEL PUMP	1E51*P-051	1' - 4"
**	HPCI OIL PUMP	1E41*P-127	2' - 2"
	HPCI LOOP LEVEL PUMP	1E41*P-050	2' - 3"
<hr/>			
TURBINES			
**	HPCI TURBINE	1E41*-TU-002	6' - 0"
**	RCIC TURBINE	1E41*-TU-005	4' - 0"
<hr/>			
MOTOR	SUMP PUMPS AND COOLING	1R24-11D1	1' - 6"
CONTROL	WATER PUMPS TO RECIRC	1R24-12D1	1' - 6"
CENTERS	PUMP MG-SET FLUID COUPLER		

EQUIP. TYPE	EQUIPMENT DESCRIPTION	PART NO.	POSTULATED DISABLED HEIGHT ¹ /
TANKS	FLOOR DRAIN SUMP TANK	1G11*TK-050A,B 1G11*TK-056A-C	----- -----
	DRYWELL FLOOR DRAIN RECEIVER	1G11*TK-057	-----
	SALT WATER DRAIN TANK	1G11*TK-190	-----
	DRYWELL EQUIP. DRAIN RECEIVER	1G11*TK-049	-----
HEAT EXCHANGER	HPCI BAROMETRIC CON. VACUUM TANK	1E41*E-036	-----
	RCIC BAROMETRIC CON. TANK	1E51*E-038	-----
	RHR HEAT EXCHANGER	1E114*E-034A,B	-----
	RBCLCW HEAT EXCHANGERS	1P42*E-011A,B	-----
	DRYWELL EQUIP. DRAIN COOLER	1G11*E-094	-----
ELEC. PANELS	** RCIC INSTR. BACK	1H21*PNL-017	2' - 0"
	** RCIC INSTR. RACK	1H21*PNL-037	2' - 0"
	** CORE SPRAY RACK	1H21*PNL-01	3' - 10"
	** CORE SPRAY RACK	1H21*PNL-019	3' - 10"
	** RHR INST. RACK A	1H21*PNL-018	3' - 10"
	** RHR INST. RACK B	1H21*PNL-021	3' - 10"
	** HPCI INST. RACK A	1H21*PNL-036	1' - 10"
	** HPCI INST. RACK B	1H21*PNL-14	1' - 10"

** Vital Equipment required for system operation.

¹/Heights are taken from a physical survey measurement taken from bottom of component to floor level.

----- Non-electrical component

Table A-6

SUMMARY OF VITAL EQUIPMENT ASSOCIATED WITH SAFETY SYSTEMS
 LOCATED IN THE ELEVATION 8 COMPARTMENT AND THE POSTULATED
 HEIGHT AT WHICH VITAL EQUIPMENT COULD BE DISABLED

SYSTEM	ASSOCIATED VITAL EQUIPMENT	MINIMUM POSTULATED DISABLED HEIGHT (NOTE 2)	SYSTEM FAILURE MODE
HPCI	HPCI INST. (1E41*PS023A-D)	1' - 10"	HPCI ISOLATION
RCIC	RCIC INST. (1E51*PS026A, B)	2' - 0"	RCIC ISOLATION
LPCI	RHR INST. RACK A, B (1E11*PDS001A, B)	3' - 10"	RHR LOGIC DISABLED
CORE SPRAY	CORE SPRAY INST. RACK A, B (1E21*PDS033A, B)	3' - 10"	INJECTION VALVE CLOSURE
RECIRC PUMPS (MG-SET)	MOTOR CONTROL CENTERS (11D1, 12D1)	1' - 6"	COOLING WATER PUMP TRIP FOR FLUID COUPLER (NOTE 1)
CONDENSATE	NONE	NONE	NONE

NOTE 1: Due to fluid (oil) heatup, trip of recirculation pump MG-SET is calculated to occur in 7.5 minutes following loss of MCC. Emergency procedures require initiation of Emergency Shutdown on loss of cooling water.

NOTE 2: Based on physical survey of electric component position and associated electrical shorting effects

A.4.2 Human Error Probabilities

A.4.3 Other Initiator Event Tree
Functions

A.4.1 Quantification of System Maintenance Which May Lead to
the Release of Excessive Water Into the Elevation 8
Compartment

There is also the possibility that portions of a system could be disassembled to perform maintenance (e.g., pump impeller replacement). If during this maintenance, an error or set of errors occur which de-isolate the component undergoing maintenance, then the release of water through the opened system may occur.

Therefore, on-line maintenance of systems located in the reactor building which could result in the release of water into the reactor building when coupled with additional operator or maintenance errors are evaluated as potential sources of internal flood initiators. The method used in the quantification of the initiating frequency (i.e., the frequency of major on-line maintenance of the systems in the reactor building) is addressed here.

The conditional probability of the system being opened is based upon the following considerations:

- BWR operating experience data (A-1 to A-3) indicates that the unavailability of safety systems due to on-line maintenance is limited as shown in Appendix A.4, of the PRA. Table A-7 reproduces these best estimates.
- The unavailability of a system associated with major, on-line maintenance is judged to be significantly less than the overall system unavailability.
- Only a small fraction of the maintenance operations involve opening of the system to the Elevation 8 atmosphere; therefore, for most system maintenance operations, the system is not subjected to the failure mode of interest, i.e., internal flooding of the Elevation 8 compartment.
- A portion of the maintenance operation is assumed to be involved in disassembling and assembling the components; therefore, the system is not opened during this time of the Elevation 8 and also does not contribute to the potential for water release.

Table A-7
 MAINTENANCE UNAVAILABILITY

SYSTEM	TOTAL SYSTEM UNAVAILABILITY (APPENDIX A.4)
Core Spray	
Loop A	2×10^{-3}
Loop B	2×10^{-3}
LPCI	
Pump Leg A	
Pump Leg C	4×10^{-3}
Pump Leg B	
Pump Leg D	4×10^{-3}
HPCI	10^{-2}
RCIC	1.1×10^{-2}
EBCLCW	2×10^{-3} (est)

In order to identify the frequency of maintenance operations which could result in disassembling and opening the systems in elevation 8, a conservative approach is adopted. Specifically, the LER data base is reviewed to identify the frequency of turbine driven and motor driven pump failures. Using these failure frequencies, the approach used here is to identify each of these failures as a source of major maintenance which could, when coupled with an operator error, result in the release of water into elevation 8.

There are four failure modes for pumps in Reference A-4, i.e., leakage/rupture, does not start, loss of function, and does not continue to run. Table A-8 below shows the data used in the evaluation of the BWR standby pumps: motor driven and turbine driven. The hourly LER failure rates characterize the first failure mode, while demand failure rates are used for the other failure modes.

Table A-8

LER DATA* FOR BWR STANDBY PUMPS OVER THE PERIOD: JANUARY 1972 THROUGH APRIL 1978

STANDBY PUMPS	POPULATION		FAILURE EVENTS			
	(DEMANDS)	(STANDBY HOURS)	LEAKAGE/RUPTURE	DOES NOT START	LOSS OF FUNCTION	DOES NOT CONTINUE TO RUN
MOTOR DRIVEN	13,644	6,777,627	6	5	4	6
TURBINE DRIVEN	1,820	868,033	-	1	6	5

*Taken from Table 18 of Reference A-4.

Motor Driven Pumps

For motor driven standby pumps, the following LER rates are found for the four failure modes:

- o Leakage/Rupture: 6 events/6,777,627 hrs. = 8.0×10^{-7} /hr.

- o Does not start, loss of function, and does not continue to run: (5+4+6) events/13,644 demands = 1.1×10^{-3} /demand.

It is assumed that these pumps are in standby status nearly all of the time during a year and there are twelve* demands on the average per year. The annual maintenance frequency is then calculated directly from these LER rates:

$$(8 \times 10^{-7} / \text{hr}) \times (8760 \text{ hr/year}) + 1.1 \times 10^{-3} / \text{demand} \times 12 \text{ demand/year} = 2.0 \times 10^{-2} / \text{yr.}$$

In other words, the maintenance frequency is 2.0×10^{-2} per year for motor driven standby pumps.

Turbine Driven Pumps

Similarly, the annual maintenance frequency for turbine driven standby pumps can be calculated as follows:

$$(0/868.033\text{hr}) \times (8760\text{hr/yr}) + ((1+6+5)\text{failures}/1820\text{demands}) \times 12\text{demands/yr} = 7.9 \times 10^{-2}/\text{yr}$$

The maintenance frequency is 7.9×10^{-2} per year for turbine driven standby pumps.

Table A-9 summarizes the frequency associated with major maintenance operations based upon the above evaluation and a conservative estimate of heat exchanger on-line maintenance.

*The number of demands per year are conservatively estimated here to be four scheduled tests plus eight other occurrences.

Table A-9

FREQUENCY OF ON-LINE MAJOR MAINTENANCE,
OF SYSTEMS IN THE REACTOR BUILDING

SYSTEM	FREQUENCY (PER YEAR)	INITIATOR EVENT TREE
Core Spray	0.04	T _{FL3}
LPCI	0.08	T _{FL4}
HPCI	0.079	T _{FL2}
RCIC	0.079	T _{FL1}
Service Water	0.04	T _{FL5}

In addition to the maintenance frequency, another item required in assessing the length of plant vulnerability is the length of time that the major maintenance may require. This length of time is necessary to evaluate the likelihood of potential plant challenges (MSIV closure) during the major maintenance occurrence.

In WASH-1400 (A-3), maintenance summary reports from Millstone 1 and Dresden 1, 2, and 3 for 1972 were the data sources for the maintenance duration evaluation. The pump maintenance act duration ranges from 2 to 400 hours, with sample mean (based on raw data) 37 hours. It should be noted that these calculations included both on-line and off-line maintenance.

Taking into account the plant technical specifications which restrict the maintenance duration during the plant operation, bounds of $\frac{1}{2}$ hour and 72 hours are proposed for the log-normal distribution model for on-line maintenance by EG&G in Reference A-4. The main maintenance duration can be calculated by using these bounds as 5% and 95% percentile values. The calculated mean duration is 19 hours for the assumed bounds suggested by EG&G.

For the Shoreham Nuclear Generating Station, the plant technical specifications allow the turbine driven standby pumps to be unavailable for a maximum of 14 days* before the plant is placed in a "shutdown" configuration to complete the maintenance. Therefore, the maintenance duration evaluation for SNPS can be derived by increasing

the 95% percentile value to 336 hours (14 days). The median and mean of the log-normal model can be calculated as follows:

$$\text{Median:} \quad 1/2 \cdot 336 = 13\text{hrs}$$

$$\text{Mean:} \quad 13 \times \exp. \left[\frac{1}{2} \left(\frac{\ln 26}{1.64} \right)^2 \right] = 93 \text{ hrs.}$$

* HPCI and RCIC have technical specification allowable outage items of 14 days.

For motor driven standby pumps, the technical specification limit is 7 days instead of 14 days. By assigning a 95% percentile value to 168 hours (7 days) the median and mean are calculated as:

Median: $1/2 \cdot 168 = 9.2\text{hrs}$

Mean: $9.2 \times \exp. \left[\frac{1}{2} \left(\frac{\ln 18.4}{1.64} \right)^2 \right] = 44\text{hrs}$

A.4.2 Operator Action Interface Events Involved in Reactor Building Flood Sequences

A.4.2.1 Introduction

The systematic review of the operator interface with the sequences of the SNPS PRA which could potentially lead to Reactor Building flooding and consequent core vulnerable sequences has revealed operator related human error events which contribute to these sequences. The events of interest are:

1. Event P - Operator Removes Power from Boundary Valves
2. Event E_L - Operator Maintains motor control center (MCC) isolation of the Boundary Valves.
3. Event E_C - Operator Maintains Control Room Isolation of the Boundary Valves.
4. Event A - Operator Diagnoses and Isolates Flood in X minutes

The actual contribution of these events to a particular sequence is determined by the frequency and duration of other events such as maintenance on one of the systems which would be a potential

initiator, the frequency of automatic initiation commands and other events which are discussed in other sections. This section discusses the probability of individual events based upon a review of the design and procedures related material that has been acquired from LILCO and/or collected as a result of a walk-through inspection of both the SNPS control room, the Reactor Building Elevation 8 area, and interviews with SNPS operations and maintenance staff. Since this review was accomplished from a human reliability perspective many of the function distinctions important from other perspectives did not contribute to the human error probability whereas other distinctions which might not be functionally significant were of importance from a human reliability standpoint. For example, from a recovery standpoint the important consideration is whether the operating team is made aware of the flood, how long he has to respond to detect and isolate the flood, and whether or not his attention is totally available for this discovery and isolation problem. The individual valve which initiates the flood is of no consequence except as it affects these parameters.

A.4.2 Event P - Operator Removes Power from Boundary Valves

Event Background

The removal of power from equipment being maintained or inspected during a maintenance operation is a routine procedure followed in most industrial facilities. This procedure is common practice in

both fossil and nuclear stations and has become standard practice from a personnel safety standpoint. The removal of power is clearly called out in the LILCO "Rules of Safe Operation" dated 1 January 1980. The relevant paragraph states:

1.04.4 "Hold-off" type of "Equipment Clearance Permit" SHALL be used where ever it is necessary to perform maintenance on or inspect equipment. This type of "Equipment Clearance Permit" certifies to the persons to whom it is issued that the equipment specified is isolated from all sources of voltage, temperature, and pressure so that the work indicated on the "Equipment Clearance Request" form can be performed. This type of "Equipment Clearance Permit" can be issued to an unlimited number of authorized personnel at the same time.

Although the procedure refers to the maintained equipment alone and not the boundary equipment it is also common practice that power is removed from all boundary equipment as well (again to protect plant maintenance personnel). Interviews with LILCO personnel verified that this is in fact the LILCO practice, and a review of a sample SECP* for a relevant system (HPCI) indicated that the associated "Tagging Order" required isolation and then the electrical disablement of all boundary equipment. These valves are electrically disconnected from their associated 480 V supply by pulling and tagging the appropriate breaker at the motor control center (MCC).

The probability of missing an individual breaker is further reduced by the fact that each step in the tag sequence must be initialed by

*SECP - Station Equipment Clearance Permit

the individual performing the work. Also, routinely the sequence and its implementation are verified for safety related equipment. This is also indicated on Page 9 SPR.12.011.01 Rev. 5, 2/12/82 "Station Clearance Permits" the relevant section reads:

- 8.3.10 Step, 16,17 - If deemed necessary by the Watch Engineer, a secondary qualified person shall verify the correct implementation of the SECP tagging order and placement of the clearance tags.

Note: When a safety related system is affected independent verification should be provided to the extent necessary to assure that the proper system was removed from service. This may be accomplished by checking appropriate equipment and controls or indirectly by observation of indicators and status lights. Where significant radiation exposure could result, this equipment may be waived.

Event Human Error Probability (HEP) Alternatives:

This particular type of event could be assigned the HEP nominal values given in NUREG/CR-1278 for four recorded events. The recorded events and their corresponding probabilities are:

<u>NUREG/CR-1278 Events</u>	<u>Probability</u>	<u>Reference</u>
1. Failure to carry out plant policy when there is no check or person.	0.01(0.005 to 0.05)	p 20-31, Table 20-22, Item 1
2. Error of Omission in Use of Written Procedures in Non-passive Tasks with check-off. Long list 10 items.	0.003(0.001 to 0.01)	p 20-29, Table 20-22, Item 2
3. Failure to follow established procedures or policies in valve changes or restoration	0.01(0.005 to 0.01)	p 20-23, Table 20-15, Item 5

<u>NUREG/CR-1278 Events</u>	<u>Probability</u>	<u>Reference</u>
4. Change or restore wrong 110V switch or circuit breakers in a group of similar appearing items.	0.003(0.001 to 0.01)	p-20-21, Table 20-14, Item 7

Event 1 is clearly conservative when compared to the Event P defined here in the SNPS PRA since LILCO procedures call for a check and verification of the implementation of the tagging order. Event 3 is related to changes in the valves themselves rather than the restoration of power to the valve at the MCC. For these reasons it would appear that Event 2 or Event 4 is more analogous to Event P. Since each has the same HEP nominal value and range distinction need not be made between them.

Event Human Error Probability Selection and Justification:

The associated probability and bounds are then 0.003 (0.001 to 0.01) as given in NUREG/CR-1278. The extreme high value is known to be conservative since 0.01 is the nominal value to be assigned with no check, and LILCO procedures do call for a check. However total credit cannot be taken for the procedures as written because:

1. The tagging order requirement for checking is left to the discretion of the Watch Engineer, and he clearly has the option of not requiring verification, and
2. Even for safety systems the requirement is optional.

For these reasons the selected probability is judged to be between the nominal and high value (i.e., 0.003 to 0.01) and to be

conservative 0.01 is selected. If the procedures are amended so that a check is required for the boundary valves of concern, and if operating personnel are trained accordingly, then the probability could be reduced to 0.003. This value is consistent with the nominal probability of inadvertently not racking out a valve breaker. In a second meeting the operational staff agreed to consider changes to maintenance procedures.

Probability (Event P) = 0.01 per vulnerable maintenance occurrence is judged to be conservative.

A.4.2.3 Event E_C - Operator Maintains Isolation of the Boundary Valves

Event Background

The operator could fail to maintain the isolation of these valves either by manually opening one or more of them locally, or by remote opening. Of course remote opening is not possible for manual valves. Valves can be opened remotely either at the motor control center or in the control room. Due to the location of the manually operated isolation valves near the area where the flood would occur, it is judged to be very unlikely that an operator would open an isolation valve locally and fail to notice the flood and reclose the valve.

Operation of the valve at the MCC requires the presence of two things: power and command. Power at the MCC requires the failure of Event P. Command at the MCC requires the valve operation to be "jumped". Jumping of these valve controls is not likely to occur at Shoreham. Due to the low probability of this event, it is not considered in further calculations.

Inadvertent Operation of Panel Switch:

The other possibility is that the valve is opened from the control room. This operation would require that the valve auto function would be available and that appropriate panel switch is activated. The auto function would be active if the operator failed to remove power from the valve (EVENT P).

The panel switch could be activated if either the operator mistakenly operates the tagged out switch. A 0.001 (NUREG/CR 1278 p 20-21, Table 20-14, Item 4) high value is used to include the possibility for failure to tag and the use of multiple tags in the area. Two other considerations were evaluated: a command fault to the valve (less than 10^{-4} in the maintenance period), or if the operator inadvertently operates the panel switch. This final event requires further discussion.

Here a distinction is made between mistaken operation of a switch (i.e., the operator turns the wrong one) and inadvertent operation of

the switch (i.e., the operator turns the switch without knowing it). This second event is more probable in some instances due to design specific considerations of the SNPS control board. Two general types of switches are used in the control of the systems of interest, on the SNPS control board, round thumb knob two position switches and "L" handle switches. The thumb knob switches and "L" handle switches with key locks are not susceptible to inadvertent operation since they require an overt action directed specifically at their operation for actuation. The "L" handle switches without keys which are more than 6 inches from the edge of the panel are also not susceptible since the operators would have to actually sit on the panel to inadvertently actuate them. This is an unlikely occurrence for a trained operational staff. However, there are several "L" handle switches within one or two inches from the edge of the panel. Since the panel is approximately at hip height the potential for inadvertent actuation exists.

This possibility exists for the valve operator switches of interest for this sequence since many of them are on the edge of the panel and since they are momentary-contact spring-return-to-auto type which may be susceptible to inadvertent operation. The initiating mechanism is that of an operator walking by the panel and catching a belt loop, a flashlight, a wallet or anything else at hip height on the valve handle and activating the valve without his knowledge.

In the time required for some of the maintenance actions of interest and probability that someone inadvertently actuates a switch is estimated at 50% to be conservative. Assuming there are 50 valves switches on the edge and at most only one contributes to this sequence during a particular maintenance act the probability for each valve is estimated at 0.01 per vulnerable act, (HPCI and RCIC have two valves each associated with switches on the edge of the control panel) and 0.001 per vulnerable act for all others (LPCI, CS, SW).

A.4.2.4 Event A - Operator Diagnoses and Isolates Flood in X Minutes

The Operator Recovery Model Used for the SNPS PRA Flood Sequence

The evaluation of the probability of recovery (i.e., the operator isolating a flood which has occurred) is based upon the use of a response time versus human error probability relation. The suggestion that such a relation is the proper approach for recovery probability assignment has a long history. The work of W. Hannaman is also acknowledged in this area. Early work (A-5) provided experimental evidence for the validity of such a correlation for basic stimulus/response tasks in a NPP control room environment. Later work (A-6) suggested that the approach could have validity across a broad range of tasks. More recent work (A-7, A-8, A-9) provides correlational research to substantiate the suggestion, and provides quantitative indication of what conservative bounds for the relation would be when applied to operator responses to risk

significant cognitive tasks, as well as providing a more comprehensive reference set. The particular relation used in this analysis to assign Human Error Probabilities to the operator response to a singular flood occurrence will be contained in Chapter 12 of the 1982 revision of Reference A-12, and has been recently been published in Reference A-10. For multiple transients the singular occurrence value is assigned to the first transient diagnosed in and the more conservative screening values for the joint HEPs given in Reference A-11 are applied for all subsequent problems using the approach suggested in Reference A-10. In this analysis it has been assumed (for conservatism) that when multiple transients are present the flood will not be the first one diagnosed and so the more conservative values have been applied.

Event Background

The time available for flood response depends on the discharge rate from the flooding source through the active pathway. Since the times may change as a result of more definitive analysis the failure of this event has been developed parametrically using time of response as a parameter. The event A provides for recovery from all potential flood initiator sequences; automatic initiated opening of a boundary valve, or manually initiation of a valve. Although from a systems analysis standpoint each of these must be treated separately the human interface similarities allow the last two to be treated in a similar fashion. For the case of automatic initiated opening of a

boundary valve, it is assumed that multiple alarms of the same or higher priority will be occurring in the control room at the same time as the flood alarm, and the operators job will be to address multiple alarms until he gets to the flood alarm and then must proceed to identify the source of the flood, determine the isolation approach required, and implement it. In the case of a manually initiated opening of a boundary valve only the flood related alarms will be occurring and the operator need only address the isolation of the flooding source. For this reason the following two events are identified and discussed below:

1. Event A_A - Operator Isolates within X minutes after auto occurrence.
2. Event A_M - Operator Isolates Flood within X minutes after manual occurrence.

Event A_A

The operator can fail in Event A_A by either not being prompted to act to isolate the flood, or by acting but not being able to identify and isolate the flood in X minutes. The operator may not be prompted to act to isolate the flood either because the flood alarm does not activate, or because even though it activates he must deal with other alarms as well and may not be able to address and isolate the source of flooding in X minutes. The failure of the flood alarm is a component failure event and its probability is addressed in Event I. To be conservative alternative means of being alerted to the flood are not considered although they are available. When multiple

problems occur simultaneously the nominal response function needs to be modified to take into account the expected degradation in the function due to stress of multiple alarm occurrences. Recent research in this area has led to the development of the multiple occurrence time response table given below. The table is included in Chapter 12 of the 1982 Edition of NUREG/CR-1278. For the case when the flood is the second event the expected response probability performance reported is shown in Table A-10.

Table A-10
RESPONSE TIME PROBABILITY - 2ND EVENT

X (minutes)	P_x^1 (Probability of not successfully responding to the 2nd event in this case the flood by X minutes)
1.0	1.0
10	0.5
20	0.1
30	0.01
60	0.001
1500	10^{-4}

It should be noted that the times given here are times between the prompt (i.e., flood alarm), and the time a response is initiated. This does not include the operator action intervention time, (i.e., time required to activate the relevant controls) but does include the time required to identify the source of flooding and to determine what isolation response is required. The times listed (and also the times with other Table A-10) here are based upon the response of Control Room Operators who are trained in the specific flood alarm

response procedures, and recognize the time priorities required to be considered for isolation. That is what are the primary sources of water and the most probable pathways, and which require the quickest action. This training is considered to include work on this specific sequence response, and that the training is renewed on a regular basis.

If the operator is prompted to act immediately upon the occurrence of the flood alarm he might still be unable to identify and isolate the source of the flood. The time response situation is similar to the previous situation except that the flood is now his primary concern and therefore the first event numbers from Chapter 12 of NUREG/CR-1278 are used, as shown in Table A-11.

Table A-11

RESPONSE TIME PROBABILITY - 1ST EVENT

X (minutes)	P_x^1 (Probability of not successfully responding to the 2nd event in this case the flood by X minutes)
1.0	1.0
10	0.1
20	0.01
30	0.001
60	10^{-4}
1500	10^{-5}

Event A Probability: Operator Error Within X Minutes Following An Automatic Plant Action

The probability for failure to isolate the flood that occurs due to an isolation event is the sum of the values in the previous two tables. These results are displayed in Table A-12.

Table A-12

PROBABILITY THAT FLOOD REMAINS UNISOLATED FOR X MINUTES AFTER AUTOMATIC PLANT ACTION; e.g., MSIV CLOSURE INITIATES FLOOD

X	$P_{AA}(X)$
1	1
10	0.6
20	0.11
30	0.011
60	0.0011
1500	1.1×10^{-4}

Event A_M

The operator can fail Event A_M by either not being prompted to act to isolate the flood, or by acting but not being able to identify and isolate the flood in X minutes. The operator may not be prompted to act to isolate the flood either because the flood alarm does not activate, or because he does not respond to it properly. In the case of manual initiation the failure to respond properly is just the probability that he fails to respond to an annunciated alarm light. The probability is given in NUREG/CR-1278 (P20-9, Table 20-3, Item 1) as 10^{-4} per occurrence. The nominal value has been used since in this instance the flood is a singular occurrence. The failure of the alarm to activate is a hardware failure probability, which is again not addressed here. If the operator is prompted to the flood when the probability that he fails to respond to isolate it in X minutes is the same as the probabilities given in Table A-13.

Event A_M Probability

Based upon the above analyses the event A_M probability can be given (again neglecting the alarm failure probability) by Table A-13.

Table A-13

PROBABILITY THAT FLOOD REMAINS UNISOLATED
FOR X MINUTES DURING CONTROLLED MANUAL SHUTDOWN

X	P _A (X) M
1	1
10	0.1
20	0.01
30	1.1x10 ⁻³
60	2.0x10 ⁻⁴
1500	1.1x10 ⁻⁴

In summary the values used in the SNPS PRA for HEP are compiled in Table A-14 along with the initiator branch point, the source of the water, the time available, and the human error probability.

A.4.4 Other Initiator Event Tree Functions

There are two remaining categories of event tree functions which are discussed below:

- (1) Plant status which includes predisposition to the availability of the feedwater system.
- (2) The control room annunciation given that a flood is in progress.

A.4.4.1 Plant Status

First, consider the characterization of plant status. For the flood initiator trees associated with major maintenance the plant status is sorted based upon the use of two event functions, D and R.

System not demanded by operational condition (D): This event function sorts out those cases for which an MSIV closure occurs coincident with a potential flood initiator due to major maintenance.

Table A-14

SUMMARY OF THE HEP QUANTIFICATION FOR EVENT A

SYSTEM	INITIATOR POINT	BRANCH	REACTOR* STATUS	SOURCE/TIME AVAILABLE**	HUMAN ERROR PROBABILITY (HEP)
Maintenance RCIC (suction)	T _{FL1}	A ₁	P	Supp/110	2.0E-4
		A ₂	P	Supp/110	2.0E-4
		A ₃	P	CST/76	2.0E-4
		A ₄	P	CST/76	2.0E-4
		A ₅	S	CST/76	0.0011 (1 hr)
Maintenance HPCI (suction)	T _{FL2}	A ₁	P	Supp/17	0.1
		A ₂	P	Supp/17	0.1
		A ₃	P	CST/13	0.1
		A ₄	P	CST/13	0.1
		A ₅	S	CST/13	0.6
Maintenance CS (suction)	T _{FL3}	A ₁	P	Supp/12	0.1
		A ₂	P	Supp/12	0.1
		A ₃	S	Supp/12	0.6
Maintenance LPCI (suction)	T _{FL4}	A ₁	P	Supp/9.4	1.0
		A ₂	P	Supp/9.4	1.0
		A ₃	S	Supp/9.4	1.0
Service Water	TFL5	A1	P	SW/28	0.1

The hourly probability of an MSIV closure event is derived from an estimated/event per year divided by the number of hours in a year, (8760) to give

$$\frac{1}{8760} = 1.1 \times 10^{-4}/\text{hr.}$$

The probability of an MSIV closure during maintenance of RCIC or HPCI is

$$P (D/T_{FL1}, T_{FL2}) = 93 \times 1.1 \times 10^{-4} = 0.011$$

The probability of an MSIV closure during maintenance of either LPC1 or CS pumps is conservatively assumed to automatically activate this system

$$P (D/T_{FL3}, T_{FL4}) = 43 \times 1.1 \times 10^{-4} = 0.0048$$

Reactor Status: (R) - This event function distinguishes between the possibility of a controlled operator response that preserves feedwater (T), and a response that results in an MSIV closure and loss of feedwater (S). The LILCO Emergency Procedures such as that related to loss of reactor building closed loop cooling water to recirculation pump MG-Set (SP#29.017.01 Revision 2 - 9/24/82) clearly require that the reactor operator immediately reduce Recirc pump speed to minimum, trip Recirc MG-Set, and initiate the emergency shutdown procedure (SP#29.010.01). If this is accomplished, the feedwater system will continue to operate. On the other hand, if the

operator allows the reactor to remain at full power, a delayed recirculation pump trip (approximately 7.5 minutes from the time at which the flood reaches Motor Control Centers at the 18" level) will occur. A recirc pump trip is caused by a postulated flood-induced failure of cooling water pumps to the recirc pump MG-set fluid coupler which is annunciated in the control room. If both recirc pumps trip simultaneously at full reactor power, it is possible that the feedwater system will not be capable of a runback to prevent a reactor water level 8 feedwater trip which is followed by an MSIV closure. It is conservatively assumed that an MSIV closure will also occur even for events that do not occur with the reactor at full power.

Since LILCO procedures (such as that referenced above) establish an operational requirement for manual shutdown via the emergency shutdown procedure, it is judged that a substantial majority of events will occur without loss of feedwater. It is also conceivable that the operator has initiated shutdown prior to the loss of MCC 11D1 and 12D1 at 18". If this is the case, the trip of the recirculation pumps will have no effect on reactor status. A proposed LILCO secondary containment control procedure will address this. However, the probability of failure of the operator to manually shutdown the reactor is estimated to be .3. This upper bound is assigned to take into account the possibility of operator error due to a large number of alarms occurring at the time necessary for this decision to be made. This value is consistent with the .25

value given by NUREG/CR 1278 for human error probability assigned to an error on the part of novice operators carrying out a task under extremely high (life-threatening) stress conditions, and is therefore very conservative when applied to experienced operators or to the stress conditions which are to be expected.

A.4.3.2 Control Room Annunciation (I):

The probability that the flooding conditions is not annunciated or recognized is dominated by two events - failure to recognize a flood event/given that it is annunciated, and failure of the annunciators. The flood annunciator is a safety grade system with an alarm appearing on the dedicated panel in the control room. The alarm is served by an acknowledge switch on the panel so that it is very likely that this alarm will be noticed. Failure to recognize the flood alarm is assessed to be 0.001. Failure of the flood annunciator is dominated by a common-mode miscalibration error assessed to be 2×10^{-3} . Therefore, the event I is assessed at 3×10^{-3} per challenge.

REFERENCES

- A-1 Limerick Generating Station Probabilistic Risk Assessment, Docket Nos. 50-352, 50-353, September 1982.
- A-2 "Probabilistic Analysis of the Reliability of BWR-4 Systems for Small LOCA Events", General Electric, NEDO 24809, April 1980.
- A-3 WASH-1400, "Reactor Safety Study: An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants", U.S. Nuclear Regulatory Commission, October 1975.
- A-4 NUREG/CR 1205, "Data Summaries of Licensee Event Reports of Pumps at U.S. Commercial Nuclear Power Plants: January 1, 1977 to April 30, 1978", U.S. Nuclear Regulatory Commission, January 1980.
- A-5 A.E. Green, "Safety Assessment of Automatic and Manual Protective Systems for Reactors", AHSB(s), R-172, Authority Health and Safety Branch, UK, Risely England, 1979.
- A-6 R.R. Fullwood and A.A. Hussiemy, "Human Performance Response Time", 1979 ANS Winter Meeting.
- A-7 J.R. Fragola, "Human Error Probability for the Cognitive Mode of Behavior", SAI/NY R82-7-3 (3), July 27, 1982.
- A-8 J. Wreathall, "Operation Action Trees, An Approach to Quantifying Operator Error Probability During Accident Sequences", NUS Report 4655, NUS, July 1982.
- A-9 R.E. Hall, J.R. Fragola, and J. Wreathall, "Post Event Decision Errors: Operation Action Tree/Trim-Reliability Correlation", NUREG/CR 1605, BNL, August 1982.
- A-10 A.D. Swain, "Modeling of Response to Nuclear Power Plant Transients for Probabilistic Risk Assessment", in K. Noro (ed.), Proceedings of the 8th Congress of the International Economics Association, August 23-27, 1982, Tokyo, JAPAN.
- A-11 R.A. Bari, et. al., "National Reliability Evaluation Program (NREP) Procedures Guide", NUREG/CR 2815, Final Draft, September 9, 1982.
- A-12 A.D. Swain and H.E. Guttman, Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications, NUREG/CR 1278, pg. 13-4, April 1980.